## Palo Alto Networks vs. Check Point

Clarifying the differences between Palo Alto Networks next-generation firewall and Check Point’s Application Control Blade; a port-based firewall add-on.

### CP Fiction:
Stateful inspection + Application Blade will do what Palo Alto Networks does.

### Fact:
Check Point’s port-based stateful inspection FW with UTM-style add-on blades will not deliver the safe application enablement that Palo Alto Networks does.

### Additional supporting details:
- Application Blade is an IPS engine with application signatures; it uses a negative control model to only block recognized applications on standard ports.
- With Application Blade, there will be two completely separate policy tables (and management tabs) for application controls – one for the firewall and one for the Application Blade. This means that the application and user control is NOT part of the firewall policy.
- Administrators will need to configure the Application Blade to look for applications (it is not enabled by default); expanding classification to non-standard ports is an added configuration step.
- The add-on Blade approach and tab-based integration means there is no way to positively enable applications (e.g., allow and apply QoS, allow and scan for viruses, allow at specific times).
- Application Blade cannot inspect SSL traffic; it does not include common protocols and is unable to enable key application functions such as file transfer within an application.

Palo Alto Networks App-ID is THE traffic classification mechanism; it classifies all traffic, on all ports, all the time – by application. The resulting application information is used as the basis for all firewall security policy decisions – allow, deny, inspect, shape, schedule, etc.

### Questions to ask:

| Q | Which traffic classification mechanism will the Application Blade execute first – stateful inspection, or L7 (application) classification? |
|   | App-ID is THE Palo Alto Networks traffic classification mechanism; it looks at all ports, all traffic to FIRST determine the application identity. |
| Q | Are all of the Application Blade identification techniques across all ports enabled by default? |
|   | All four of the mechanisms in Palo Alto Networks App-ID are always on, always looking across all ports, at all traffic to identify applications. |
| Q | If the Application Blade classifies traffic AFTER the FW, where is policy enforcement determined and executed – in the FW or the Blade? |
|   | App-ID is the basis of Palo Alto Networks FW and the application identity is determined first and is then used as the basis of all policies – allow, deny, allow and scan, allow and shape, etc. |
| Q | What makes this different from previous attempts at Application Control? |
|   | This will be Check Point’s third attempt at the application identification issue – AI, SmartDefense, and now an OEM database from Facetime – why will this effort succeed? |

### About Check Point:
- Large, well known security vendor; first to market with a stateful inspection port-based firewall.
- Broad line of FW UTM add-ons ("Blade Architecture") sourced from a combination of development and acquisitions.
- Thousands of loyal customers, publically traded with consistent earnings. Solid UI and management.

### About Palo Alto Networks:
- First to market with a next-generation firewall that classifies traffic based on the application, first and foremost.
- Safe-application-enablement approach to FW security is described as visionary and disruptive by Gartner. All other vendors forced to follow.
- Young, rapidly growing company with 2,500 customers worldwide.
- Cash flow positive the last 2 consecutive quarters; on a $100 M annual sales run rate (WSJ, 10/29/2010).

**Key Palo Alto Networks Differentiators:**
- App-ID: Traffic classification that delivers application visibility and control, irrespective of port, protocol, SSL or evasive tactic, as the basis of firewall classification, not an add-on.
- User-ID: Integration with every major directory service: Active Directory, Open LDAP, and eDirectory; as well as with Citrix, and Microsoft Terminal Servers.
- Content-ID: the only firewall to achieve NSS rated 94% effectiveness in IPS testing; gateway-based malware prevention; comprehensive URL filtering database; all integrated into a single pass engine to maximize performance.
- Purpose-built platform that uses four dedicated banks of function-specific processing to perform application identification, inspection and control.
## Palo Alto Networks vs. Check Point

Clarifying the differences between Palo Alto Networks next-generation firewall and Check Point’s Application Control Blade; a port-based firewall add-on.

### CP Fiction: Stateful inspection + Application Blade = Next Generation Firewall (NGFW)

Gartner defines a NGFW as a firewall with full stack visibility – not a port-based FW with UTM-style add-ons. More importantly, port-based classification cannot accurately ID the application traffic, making reliable control over those applications impossible.

Check Point’s application signature database is the largest in the world.

### Fact:

More is not better. More, in the network security world, is inefficient and risky. More creates management and performance headaches. Many of the 50,000 are widgets (45,000+), and many “core applications” are specific client and OS variants, making control efforts a management nightmare.

### Additional supporting details:

- Application control needs to be done in the FW, the heart of your security infrastructure. Control over what goes in and out of your network is what a FW is designed to do. Attempting to accomplish this goal with a UTM-style add-on is ineffective.
- App-ID is how Palo Alto Networks classifies traffic. App-ID uses as many as four mechanisms to determine the identity of the application, irrespective of port, protocol, SSL or evasive tactic.
- App-ID is always enabled, and is automatically applied to all traffic, across all ports.
- Positive enforcement model firewall policies are based on the application identity, not the port.
- App-ID is how Palo Alto Networks classifies traffic. App-ID uses as many as four mechanisms to monitor how an application and user interact.
- App-ID is client and OS agnostic, which means one App-ID is equal to many, many signatures used in other offerings.
- A single App-ID can “identify” more application variants than a single CP signature.
- Example: the single BitTorrent App-ID will see the equivalent to 40+ CP BitTorrent signatures.

### Questions to ask:

**Q)** How will CP identify an application that has already been (mis)classified by the port it came in on?

The VERY first task Palo Alto Networks executes with App-ID is the identification of the application, which becomes the basis of all security policy decisions.

**Q)** Did Check Point re-write their FW with the Application Blade or is it an add-on to their existing FW?

Palo Alto Networks is the only FW to deliver full stack visibility through our FW traffic classification mechanism; Check Point still uses port-based stateful inspection to perform its initial traffic classification, which eliminates the ability to securely enable applications.

**Q)** What is the most efficient use of your administrator’s time – managing signatures for widgets and obscure client applications, or enabling application usage for your user community?

Visibility into all applications, across all ports is automatic. Enabling applications, irrespective of port, protocol, SSL, client version, OS or rev level is done through a unified, easy-to-use policy editor.

**Q)** Can the Application Blade inspect inbound and outbound SSL?

Palo Alto Networks is the only FW to identify and control inbound and outbound SSL – traffic can be decrypted, inspected, re-encrypted and forwarded.

**Q)** How will your internal, custom applications be identified and managed?

Palo Alto Networks enables you to address custom applications in two ways (1) an application override; (2) by writing your own custom application signature.

**Q)** How are application false positives and application updates managed?

An OEM relationship + well-known internal bureaucracy will hinder responses to application false positives and application updates. And what about evasive applications like UltraSurf that change every week? Palo Alto Networks understands these challenges and has a proven team and infrastructure in place to address them.
## Palo Alto Networks vs. Check Point

Clarifying the differences between Palo Alto Networks next-generation firewall and Check Point’s Application Control Blade; a port-based firewall add-on.

### CP Fiction: Palo Alto Networks User-ID requires an agent on every desktop, our user control is agentless.

### Fact: CP User control requires a significant client on the network for management (SmartCenter) with ties directly into AD. Check Point UserCheck will require an agent on every desktop for “user involvement”.

### Additional supporting details:

- Palo Alto Networks User-ID requires a **single** agent deployed on the network, talking to Active Directory, Open LDAP, and eDirectory; as well as with Citrix, and Microsoft Terminal Servers.
- User-ID does not rely on centralized management infrastructure.
- Palo Alto Networks “user involvement” is accomplished through flexible and customizable comfort (block) pages for all elements, applications, URLs, file downloads and more. User involvement does not require an agent deployed to individual desktops.

### Questions to ask:

**Q)** Can Check Point see and control applications for LDAP, eDirectory, Citrix, TSE users as well as Active Directory?

Now in its 4th iteration, Palo Alto Networks User-ID integrates with the widest range of directory services in the FW market. In addition, it also supports an XML API for custom integration with other user repositories.

**Q)** Can Check Point present the user with comfort pages when something is blocked or violates policy – without requiring agent deployment?

Palo Alto Networks allows administrators to present the user with fully customizable block pages for all elements (applications, URLs, files, etc) without a desktop agent, to inform, warn or coach a user about policy violations.

**Q)** Think seriously about this question: what will happen to the performance of your existing gateway when you enable all 50,000 application signatures for all traffic?

Remember what happened when you enabled AI on Check Point? Or IPS on some other FW platform? L7 inspection is processing intensive – Palo Alto Networks recognized that and built a platform to address the requirements. Our performance is measured with App-ID (application inspection) enabled, on all ports, for all traffic, for all 1,100+ App-IDs. Our performance is proven. Check Point’s Application Blade is unproven.

**Q)** Has the platform been built specifically to perform port-based classification or application-based classification?

The Palo Alto Networks platform has been developed with the express purpose of identifying applications (L7) on all ports, for all traffic, all of the time.

**Q)** What performance metrics do they have when application control is enabled on all traffic?

The Palo Alto Networks performance metrics are based on application identification, not port-based classification.

### Application Blade will run on any gateway.

The Application Blade may run on every gateway, but the performance impact will be significant and may require unplanned (and un-budgeted) platform upgrades.

- CP platforms are optimized for stateful inspection fast-path, a mechanism where, once traffic is classified it is untouched until it changes.
- CP platforms are NOT optimized for level classification for all traffic on all ports.
- The impact of enabling all 50,000 signatures for all traffic, on all ports will result in IPS-level or worse performance.

Palo Alto Networks platforms utilize dedicated, high performance processing for networking, security, threat prevention, and management to delivers multi-Gbs throughput of application level inspection across all ports, on all traffic.
### Palo Alto Networks vs. Check Point

Clarifying the differences between Palo Alto Networks next-generation firewall and Check Point’s Application Control Blade; a port-based firewall add-on.

<table>
<thead>
<tr>
<th>CP Fiction:</th>
<th>Palo Alto Networks is an unproven, niche’ vendor with limited customers.</th>
<th>Palo Alto Networks cannot support a large scale deployment.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fact:</strong></td>
<td>Our experience, a rapidly growing customer base and recognition by Gartner indicate Palo Alto Networks is more than a ‘niche” player. No other vendor has deployed more NGFWs as defined by Garner, than Palo Alto Networks.</td>
<td>Palo Alto Networks has a full line of support, education, and professional services delivered by a worldwide network of partners. Large scale references available on request.</td>
</tr>
</tbody>
</table>
| **Additional Supporting Details:** | • First customer ship in June of 2007; 2,500+ customers to date growing at 25% Qtr-over-Qtr.  
• Palo Alto Networks is approaching the 4th major release and the 9th feature release of PAN-OS.  
• *Every* customer is using the application visibility and control in our NGFW – it is the core of what Palo Alto Networks does.  
• Recognized as “disruptive” and a “visionary” vendor by Gartner in most recent Enterprise FW Magic Quadrant.  
• Cash flow positive the last 2 consecutive quarters; on a $100 M annual sales run rate (*WSJ, 10/29/2010*). | Palo Alto Networks is already supporting many, many large scale deployments with the following key elements.  
• Support: In-seat level 3 engineers 24/7 in the US, EMEA and APAC; 1,000s of trained (ACE) SEs - partner and Palo Alto Networks – around the world.  
• Education: Basic and advanced accreditation training (ACE) delivered by a worldwide network of partners.  
• Services: Design and planning best practices based on thousands of deployments, and automated policy migration tools for Check Point, Juniper and Cisco – all delivered by Palo Alto Networks and a worldwide network of partners. |
| **Questions to ask:** | Q) How long have they been shipping their Application Blade?  
*Check Point has had zero releases! WHY WAIT?*  
Q) How many customers do they have using application control?  
*Palo Alto Networks has more than 2,500; growing on average at 25% QoQ. Why Wait?*  
Q) How many application control references do they have?  
*EVERY customer using our firewall uses App-ID, our traffic classification mechanism. It is the core of our firewall, just as port-based classification is the core of Check Point’s FW.*  
Q) How confident are you that Check Point will execute successfully?  
*The Check Point track record for FW add-ons has been poor (AI, SmartDefense, IPS, SSL VPN).*  
Q) How many CP FW add-ons have you bought, and implemented, only to be disappointed in the functions, performance or stability?  
*Palo Alto Networks has many references you can speak with regarding any functionality, performance, reliability, or support concerns you may have.* | Q) How many customers do they have using application control?  
*Palo Alto Networks has more than 2,500; growing on average at 25% Qtr-over-Qtr. Many are WW deployments with many, many devices.*  
Q) How many application control references do they have?  
*EVERY customer using our solution uses App-ID, our traffic classification to identify and control the applications on the network.*  
Q) How many CP FW add-ons have you bought, and implemented, only to be disappointed in their functionality, performance or stability?  
*Palo Alto Networks has many references you can speak with regarding any functionality, performance, reliability, or support concerns you may have.* |

Competitive data is generated from public information sources.