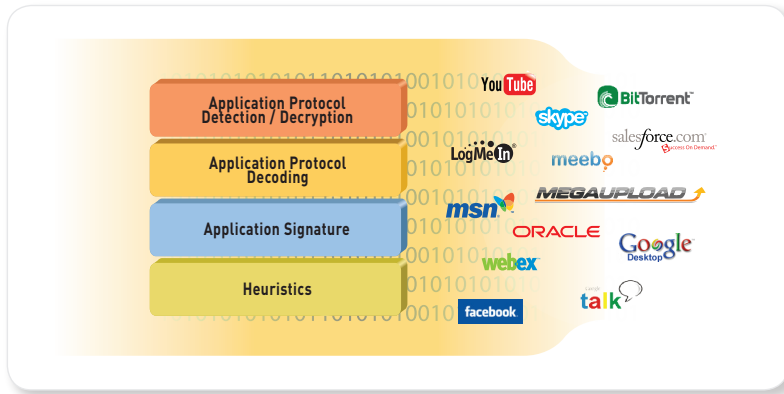


# App-ID



App-ID is a patent-pending traffic classification technology that identifies more than 950 applications, irrespective of port, protocol, SSL encryption or evasive characteristic.

- Facilitates more complete understanding of the business value and associated risk of the applications traversing the network.
- Enables creation and enforcement of appropriate application usage policies.
- Brings application visibility and control back to the firewall where it belongs.

App-ID uses as many as four identification techniques to determine the exact identity of applications traversing the network—irrespective of port, protocol, evasive tactic, or SSL encryption. Identifying the application is the very first task that is performed by Palo Alto Networks next-generation firewalls, providing administrators with the greatest amount of application knowledge and the only true opportunity for policy control.

As the foundational element of the Palo Alto Networks next-generation firewall, App-ID provides visibility and control over work-related and non-work-related applications that can evade detection by masquerading as legitimate traffic, hopping ports or sneaking through the firewall using SSL.

In the past, unapproved or non-work-related applications on the corporate network were summarily removed or blocked. However, in today's business environment, the response options are not nearly as clear because many of the same applications are helping employees get their jobs done.

App-ID enables administrators to see the applications on the network and learn how they work, their behavioral characteristics, and their relative risk. When used in conjunction with User-ID, administrators can see exactly who is using the application based on their identity, not just an IP address. Armed with this information, administrators can use positive security model rules to block known bad applications, while enabling, inspecting and shaping those that are allowed.

**App-ID Traffic Classification Technology**

The first task that a Palo Alto Networks next-generation firewall executes is the identification of the applications traversing the network using App-ID. Using as many as four different techniques, App-ID determines what the application is, irrespective of port, protocol, SSL encryption or other evasive tactic employed. The number of identification mechanisms used to identify the application will vary depending on the application. The order in which the identification mechanisms are applied may vary from application to application, the general flow is as follows:

- **Application Signatures:** Context-based signatures are used first to look for unique application properties and related transaction characteristics to correctly identify the application regardless of the protocol and port being used. The signature also determines if the application is being used on its default port or it is using a non-standard port (for example, RDP across port 80 instead of port 3389, its standard port).
- **SSL Decryption:** If App-ID determines that SSL encryption is in use (and a decryption policy is in place), the traffic is decrypted and then passed to other identification mechanisms as needed. If no policy is in place, then SSL decryption is not employed. Once the application is identified, and deemed acceptable by policy, threat prevention profiles are applied and the traffic is then re-encrypted and delivered to its destination.
- **Application Protocol Decoding:** If needed, protocol decoders are then employed to determine whether the application is using a protocol as its normal transport (such as HTTP for web browsing applications), or if it is only using the protocol as an obfuscation technique to hide the real application (for example, Yahoo! Instant Messenger used across HTTP). Protocol decoders also help narrow the range of possible applications, providing valuable context when applying signatures and they identify files and other content that should be scanned for threats or sensitive data.
- **Heuristics:** In certain cases, evasive applications still cannot be detected even through advanced signature and protocol analysis. In those situations, it is necessary to apply additional heuristic, or behavioral analysis to identify certain applications such as peer-to-peer or VoIP applications that use proprietary encryption. Heuristic analysis is used as needed, with the other App-ID techniques discussed here, to provide visibility into applications that might otherwise elude positive identification.

With App-ID as the foundational element for every Palo Alto Networks next-generation firewall, administrators can regain visibility into, and control over, the applications traversing the network.

**How App-ID Works: Identifying WebEx**

When a user initiates a WebEx session, the initial connection is an SSL-based communication. With App-ID, the device sees the traffic and the signatures determine that it is using SSL. The decryption engine and protocol decoders are then initiated to decrypt the SSL and detect that it is HTTP traffic. Once the decoder has the HTTP stream, the system can apply contextual signatures and detect that the application in use is WebEx. WebEx is then displayed within ACC and can be controlled via a security policy.

If the end user were to initiate the WebEx Desktop Sharing feature, WebEx undergoes a “mode-shift” to where the session has been altered from a conferencing application to a remote access application. In this scenario, the characteristics of WebEx have changed and application signatures detect this with the results (WebEx Desktop Sharing) being displayed in ACC. Using a security policy, administrators can control the use of this WebEx application function separately from general WebEx use.

**Firewall Traffic Classification: Applications, not Ports**

Identifying the application as soon as the firewall sees it provides the greatest amount of application knowledge and the only true opportunity for policy control. The application identity, how it works, who is using it, bandwidth consumed and associated threats are just a few of the key data points that App-ID provides the administrator, which in turn, enables more effective decision making on how to treat the application. When coupled with the directory services integration (Active Directory, LDAP, eDirectory), the firewall policy control options can incorporate users and groups, in addition to IP addresses.

Palo Alto Networks recognized that applications had evolved to where they can easily slip through the firewall and chose to develop App-ID, a new method of firewall traffic classification that does not rely on any one single element like port or protocol. Instead, App-ID uses multiple mechanisms to determine what the application is, first and foremost, and the application identity then becomes the basis for the firewall policy. App-ID has been created to be highly adaptable. As applications continue to evolve, application signatures can be added to App-ID or updated as a means of keeping pace with the ever-changing application landscape.

Stateful inspection, the basis for most of today’s firewalls, was created at a time when applications could be controlled using ports and source/destination IPs. The strict adherence to port-based classification and control methodology is the primary policy element, it is hard-coded into the foundation and cannot be turned off. This means that many of today’s

applications cannot be identified, much less controlled by the firewall and no amount of “after the fact” traffic classification by firewall helpers can correct the firewall port-based classification.

App-ID enables administrators to build positive enforcement firewall rules that are based on the application, not the port, resulting in policies that are more flexible than the basic allow or deny.

### **Application Identity: The Heart of Policy Control**

Identifying the application is the first step in learning more about the traffic traversing the network. Learning what the application does, the ports it uses, its underlying technology, and its behavioral characteristics is the next step towards making a more informed decision about how to treat the application. Once a complete picture of usage is gained, organizations can apply policies with a range of responses that are more fine-grained than allow or deny. Examples include:

- Allow or deny
- Allow but scan for exploits, viruses and other threats
- Allow based on schedule, users or groups
- Decrypt and inspect
- Apply traffic shaping through QoS
- Apply policy-based forwarding
- Allow certain application functions
- Any combination of the above

With App-ID as the foundational element, Palo Alto Networks’ next-generation firewalls are restoring visibility and control over the applications traversing the network to the firewall, the most strategic security component in the network security infrastructure.

### **Application Knowledge Means Better Decision Making**

Knowing more about how the application operates, what it does, and its underlying technology enables more effective and flexible policy creation. The Palo Alto Networks application database is broken into five main categories and 25 sub-categories, which can be used as filters to create policy groups. In addition to the category and subcategory breakdowns, the behavioral characteristics and the underlying technology for each application can be used as filters or to learn more about the application and make more informed policy control decisions. The category, sub-category, characteristics and underlying technology are shown below.

- **Category and Subcategory**
  - **Business:** Authentication services, database, ERP, general management, office programs, software updates, storage/ backup
  - **General Internet:** File sharing, Internet utilities (web-browsing, toolbars, etc)
  - **Collaboration:** Email, instant messaging, Internet conferencing, social networking, VoIP-video, web-posting
  - **Media:** Audio-streaming, gaming, photo-video
  - **Networking:** Encrypted tunnel, infrastructure, IP-protocol, proxy, remote-access, routing
- **Application Characteristics**
  - Able to transfer files from one network to another
  - Used to propagate malware
  - Consumes 1 Mbps or more regularly through normal use
  - Evades detection using a port or protocol for something other than its intended purpose
  - Has been widely deployed
  - Application has had known vulnerabilities
  - Prone to misuse or is easily configured to expose more than intended
  - Tunnels other applications
- **Underlying Application Technology**
  - Client-server based
  - Browser-based
  - Peer-to-peer based
  - Network protocol

**Applopedia**

Browse up-to-date application research and analysis at the Palo Alto Networks Application and Threat Research Center.

**APPLICATION & THREAT Research Center**

BLOG APPLIPEDIA THREAT VAULT TOOLS REPORTS ABOUT

Search:  950 matching applications (Clear filters)

Category	Subcategory	Technology	Risk	Characteristic
173 business-systems	29 audio-streaming	339 browser-based	266 1	372 Evasive
253 collaboration	10 auth-service	328 client-server	159 2	290 Excessive Bandwidth
123 general-internet	16 database	181 network-protocol	233 3	223 Prone to Misuse
132 media	47 email	102 peer-to-peer	191 4	469 Transfers Files
268 networking	23 encrypted-tunnel		101 5	205 Tunnels Other Apps
	15 erp-crm			203 Used by Malware
	94 file-sharing			512 Vulnerabilities
	31 gaming			597 Widely Used

Name	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	6	peer-to-peer
2ch	collaboration	social-networking	2	browser-based
2ch-posting	collaboration	web-posting	2	browser-based
3pc	networking	ip-protocol	1	network-protocol
4shared	general-internet	file-sharing	4	browser-based
acronis-snapdeploy	business-systems	management	2	client-server
active-directory	business-systems	auth-service	2	client-server
activenet	networking	ip-protocol	1	network-protocol
activesync	business-systems	general-business	4	client-server
adnstream	media	photo-video	3	browser-based
adobe-connect	collaboration	internet-conferencing	4	browser-based
adobe-update	business-systems	software-update	4	client-server
adrive	general-internet	file-sharing	4	browser-based
adrive-internal	general-internet	file-sharing	2	browser-based
atp	business-systems	storage-backup	3	client-server
aim	collaboration	instant-messaging	4	client-server
aim-audio	collaboration	voip-video	5	peer-to-peer
aim-express	collaboration	instant-messaging	4	browser-based
aim-file-transfer	collaboration	instant-messaging	4	peer-to-peer
aim-mail	collaboration	email	4	browser-based
aim-video	collaboration	voip-video	3	peer-to-peer
airaim	collaboration	instant-messaging	2	browser-based
alisoft	business-systems	management	3	browser-based

Copyright ©2007-2010 Palo Alto Networks. All rights Reserved. | [Privacy](#) | [Contact Us](#)

**Expanding the List of Applications**

The list of applications that App-ID detects is growing rapidly with 3-5 new applications added weekly based on input from customers, partners, and market trends. Customers that find unidentified applications on their network can capture the traffic and then send the information back to Palo Alto Networks for signature development. Once a new signature is assembled and tested, it is added to the list as part of the weekly content updates. If the application is internal or proprietary, an application override can be used to rename the application for visibility and control purposes. For additional flexibility in identifying HTTP applications or those that use SSL, customers can create custom application identification signatures.



**Palo Alto Networks**  
 232 E. Java Drive  
 Sunnyvale, CA. 94089  
 Sales 866.320.4788  
 408.738.7700  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

Copyright ©2010, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN-OS 3.1, March 2010.