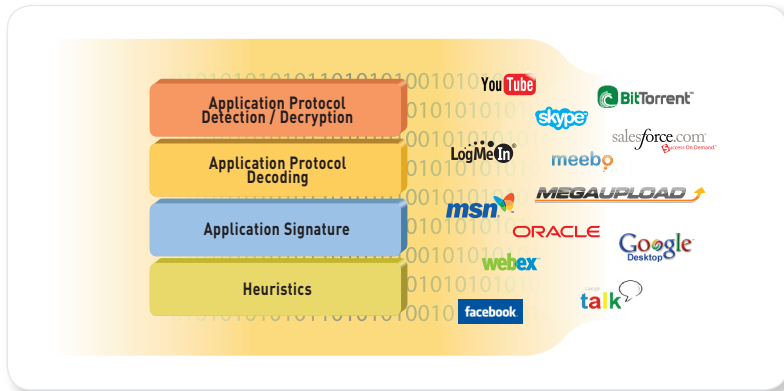


# App-ID



App-ID uses as many as four identification techniques to determine the exact identity of applications flowing in and out of the network—irrespective of port, protocol, evasive tactic, or SSL encryption. With App-ID delivering the identity of the application, administrators are able to define policies that help regain visibility into, and control over inbound and outbound applications traffic.

Enterprise networks are populated with applications, both work-related and non-work-related, that can evade detection. Some will masquerade as legitimate traffic, others will hop ports or sneak through the firewall using encrypted SSL tunnels. In the past, unapproved or non-work-related applications on the corporate network were summarily removed or blocked but the evasive nature of today's applications means that the security team cannot see the application, much less control them.

Even if the identity of the application was readily available, the remove or block as the default response may not be appropriate due to the widespread use (often at the executive level) of these applications and their potential business benefits. App-ID enables administrators to see which applications are traversing the network, learning more about how the application works, its relative risk and when used in conjunction with User-ID, who is using the application. Armed with this information, administrators can make a more informed decision on how to treat the application via policy.

App-ID is a patent-pending traffic classification technology that identifies more than 800 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 Traffic Classification Technology

The first task that a Palo Alto Networks next-generation firewall executes is the classification of traffic using App-ID, a patent-pending technology unique to Palo Alto Networks next-generation firewalls. App-ID includes as many as four different techniques to determine which applications are traversing the network—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. In some cases, an application is detected using only one mechanism while in others multiple mechanisms are used. While 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 the signature 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.

The breadth of applications in use by employees of all levels means that they cannot be treated as threats – it is not a question of good versus bad. It is a determination of the business value to the user. The ideal place to identify the applications is at the firewall, the most strategic point in the security infrastructure. Palo Alto Networks next-generation firewalls use App-ID to identify the applications, irrespective of port, protocol, evasive technique or SSL encryption. Armed with the knowledge of what the application is, and who is using it, administrators can then apply policies with a range of responses that are more fine-grained than allow or deny. Examples include:

- Allow and scan for threats
- Allow based on schedule
- Decrypt SSL and inspect
- Allow and apply traffic shaping
- Allow for certain users or groups
- Allow key application functions
- Any combination

The bottom line is that identifying the application, first and foremost, and using it as the basis of the firewall policy is the only effective way to restore visibility and control.

### 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 using 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 and ACC will begin displaying the WebEx Desktop Sharing feature. Using the policy editor, administrators can allow or deny the use of this application feature.

### 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 an 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, customers can create custom signatures to identify an application.

### Application Identity: Only Part of the Application Control Puzzle

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. Palo Alto Networks provides fingertip access to all of this information for more than 800 applications, allowing an administrator to filter applications based on category, subcategory, underlying technology, and behavioral characteristic. Once a complete picture of the usage is gained, organizations can apply policy controls that can be tied to a specific set of users and groups via Palo Alto Networks' Active Directory integration.

#### Application Browser

To view more than 800 applications and their respective characteristics, please visit the Palo Alto Networks Application Research Center at [www.paloaltonetworks.com/arc](http://www.paloaltonetworks.com/arc).

829 matching applications (Clear filters)

Category	Subcategory	Technology	Risk	Characteristic
152 business-systems	22 audio-streaming	286 browser-based	243 1	319 Evasive
209 collaboration	9 auth-service	267 client-server	147 2	238 Excessive Bandwidth
108 general-internet	16 database	176 network-protocol	184 3	206 Prone to Misuse
107 media	42 email	100 peer-to-peer	157 4	404 Transfers Files
253 networking	21 encrypted-tunnel		98 5	164 Tunnels Other Apps
	15 erp-crm			191 Used by Malware
	82 file-sharing			416 Vulnerabilities
	23 gaming			536 Widely Used

Name	Category	Subcategory	Risk	Technology
100bao	general-internet	file-sharing	5	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
adobe-connect	collaboration	internet-conferencing	3	browser-based
adobe-update	business-systems	software-update	4	client-server
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	5	peer-to-peer
airsim	collaboration	instant-messaging	2	browser-based
allpeers	general-internet	file-sharing	5	peer-to-peer
altiris	business-systems	management	1	client-server

## Application Categories and Subcategories

To enable efficient research and policy creation, all of the 800+ applications are separated into categories and subcategories, enabling the administrator to filter the application list to create dynamic groups of applications that can be used for policy-control.

CATEGORY	SUBCATEGORIES
Business	Authentication services, database, ERP, general management, office programs, software updates, storage/backup
General Internet	File sharing, Internet utilities
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

Information on each of the more than 800 applications identified includes eight different behavioral characteristics which serves two purposes. First, they provide administrators with more information on how the application operates and the potential risks. Secondly, they can be used as a filter in policy creation. For example, using the Instant Messaging subcategory and the file transfer characteristic, an administrator can create a policy to block IM applications that can transfer files.

### APPLICATION CHARACTERISTIC

**Transfers files:** Able to transfer files from one network to another.

**Used by malware:** Has been used to propagate malware, initiate an attack or steal data.

**Excessive bandwidth:** Application consumes 1 Mbps or more regularly through normal use.

**Evasive:** Uses a port or protocol for something other than its intended purpose to ease deployment or hide from security controls.

**Widely used:** Has seen widespread deployment.

**Vulnerabilities:** Application has had known vulnerabilities.

**Prone to misuse:** Used for nefarious purposes or is easily configured to expose more than intended.

**Tunnels other applications:** Able to transport other applications.

## Underlying Application Technology

The final element that is provided for every application is its underlying technology. Knowing whether the underlying technology is peer-to-peer, browser-based, client-server or networking protocol provides an additional data point that can be used in making the decision on how to treat an application.

## Using Category, Subcategory And Technology For Policy Control

Some examples of how an administrator can use the filter elements to create and enforce dynamic policies are described below.

- Block the use of any IM that transfers files by selecting *instant messaging subcategory* and *transfers files* characteristic.
- Allow the use of webmail but scan for threats by selecting *webmail subcategory* and *browser-based technology* and then apply an appropriate threat prevention profile.
- Allow the use of media applications but apply QoS by selecting *photo-video subcategory* and then apply an appropriate traffic shaping profile.



Palo Alto Networks

232 E. Java Drive  
Sunnyvale, CA. 94089  
Sales 866.207.0077

www.paloaltonetworks.com

Copyright ©2009, 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 3.0, June 2009.