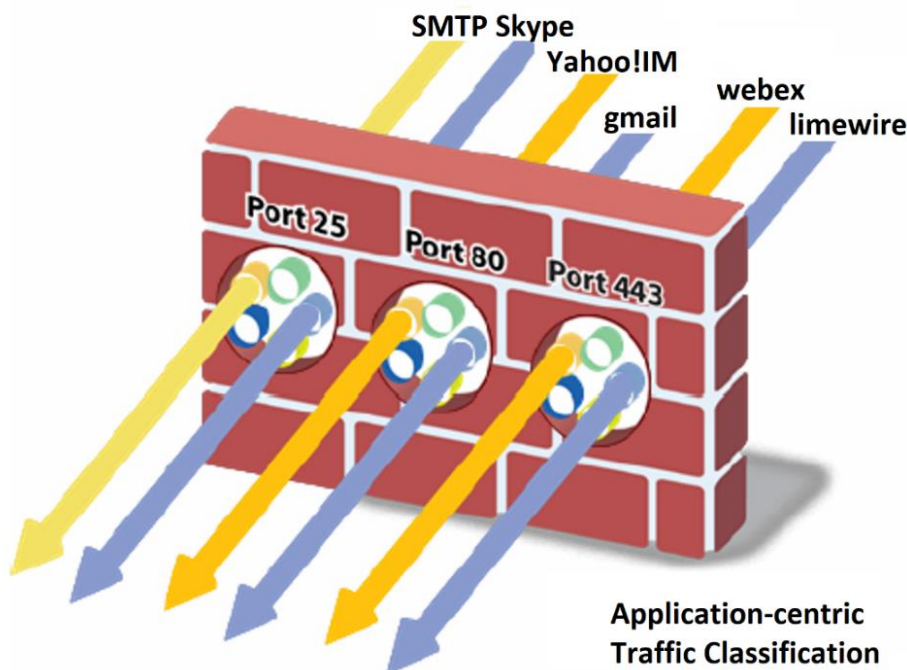# Application identification

Stateful packet inspection technology – the basis for most of today's legacy firewalls – was created more than 25 years ago, at a time when applications could be controlled using ports and source/destination IP addresses. 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. As a result, 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.

Establishing port and protocol information is a first step in application identification, but it is insufficient by itself. Robust application identification and inspection in a next-generation firewall enables granular control of the flow of sessions through the firewall. Identification is based on the specific applications (such as Skype, Gmail, and WebEx) that are being used, instead of just relying on the underlying set of often indistinguishable network communication services (see Figure 2-6).

Figure 2-6

Application-centric traffic classification identifies specific applications on the network, irrespective of the port and protocol in use.

Application identification provides visibility and control over work-related and non-work-related applications that can evade detection by legacy port-based firewalls, for example, by masquerading as legitimate traffic, hopping ports, or using encryption to slip past the firewall.

Application identification (App-ID) technology in a Palo Alto Networks next-generation firewall does not rely on a single element, such as 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 that is applied to the session. App-ID is highly extensible, and, as applications continue to evolve, application detection mechanisms can be added or updated as a means of keeping pace with the ever-changing application landscape.

Many organizations are not fully aware of the number of applications in use, how heavily they are used, or by whom. This lack of visibility forces organizations to implement negative (blacklist) enforcement approaches where they selectively block traffic and destinations known to be a risk to the organization. The next-generation firewall also allows you to implement a positive (whitelist) enforcement policy where you selectively allow the applications required to run your organization. This significantly reduces the number of ways cybercriminals can attack your organization. A key to positive enforcement is App-ID. App-ID identifies the applications traversing the firewall – regardless of port or protocol – even if the traffic is tunneled in Generic Routing Encapsulation (GRE) tunnels, uses evasive tactics, or is encrypted. App-ID can determine the difference between base applications and application functions. This level of visibility brings a complete understanding of the applications on your network and their value and risk to your organization.

App-ID traffic classification technology

The first task that a Palo Alto Networks next-generation firewall executes is using App-ID to identify the applications traversing the network. App-ID uses a multifaceted approach to determine the application, irrespective of port, protocol, encryption (SSL and SSH), or other evasive tactics employed. The number and order of identification mechanisms used to identify the application vary depending on the application. The application identification techniques (see Figure 2-7) used include:

- **Application signatures.** To identify an application, App-ID first uses signatures to look for unique application properties and related transaction characteristics. The signature also determines whether the application is using its default port or a non-standard port. Context-based signatures look for unique properties and transaction characteristics to correctly identify the application regardless of the port and protocol being used. These signatures include the ability to detect specific functions within applications (such as file transfers within SaaS applications). If the security policy allows the identified application, App-ID further analyzes the traffic in order to identify more granular applications and scan for threats.

- **TLS/SSL and SSH decryption.** If App-ID determines that TLS/SSL encryption is in use, it can decrypt and reevaluate the traffic. App-ID uses a similar approach with SSH in order to determine whether port forwarding is being used to tunnel traffic over SSH.

- **Application and protocol decoding.** For known protocols, decoders apply additional context-based signatures to detect applications tunneling inside the protocols. Decoders validate that traffic conforms to the protocol specification, and they support network address translation (NAT) traversal and opening dynamic pinholes for applications such as Voice over IP (VoIP) or File Transfer Protocol (FTP). Decoders for popular applications also identify the individual functions within the application. In addition to identifying applications, decoders identify files and other content to be scanned for threats or sensitive data.

- **Heuristics.** In certain cases, evasive applications cannot be detected by using advanced signature and protocol decoding. In those cases, App-ID uses heuristic or behavioral analysis to identify applications that use proprietary encryption, such as peer-to-peer (P2P) file sharing. Heuristic analysis, with the other App-ID techniques, provides visibility into applications that might otherwise elude identification. The heuristics are specific to each application and include checks based on information such as the packet length, session rate, and packet source.

Figure 2-7

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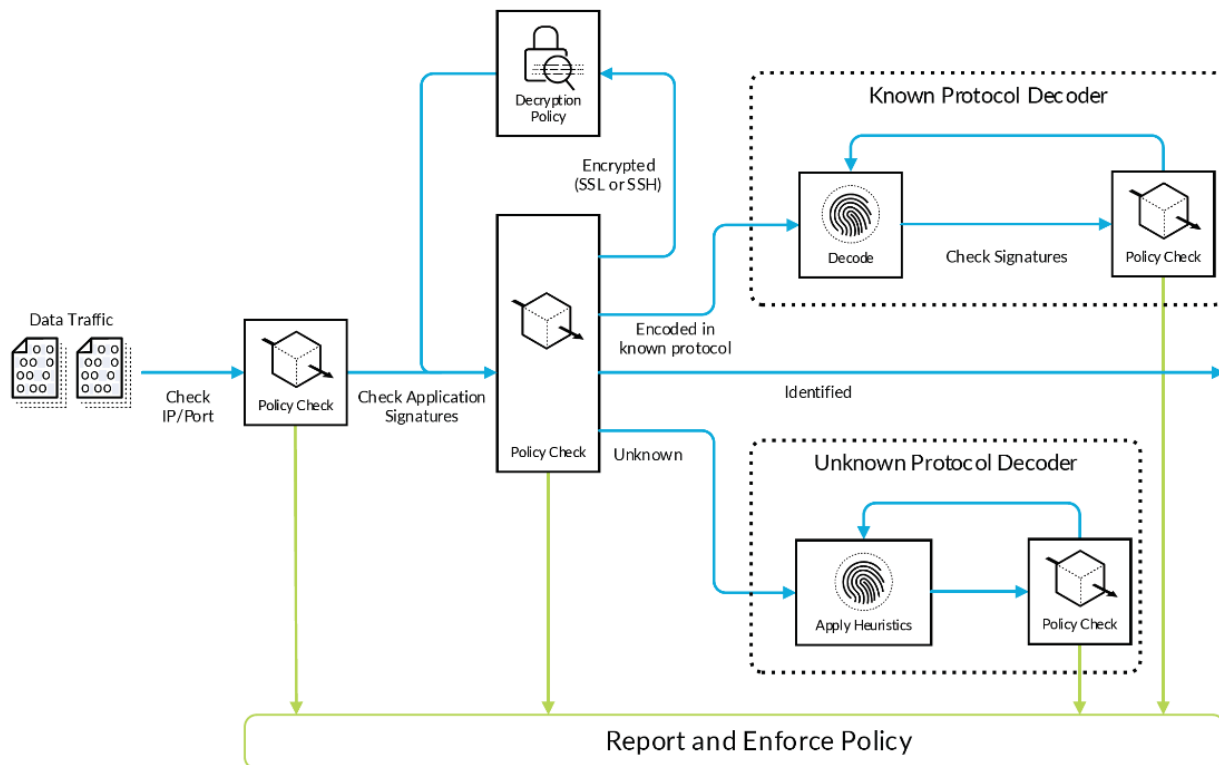
With App-ID as the foundational element for every Palo Alto Networks next-generation firewall, administrators can regain visibility into, and control over, the applications traversing the network.

App-ID: Addressing custom or unknown applications

Using the Application Command Center (ACC), you can see the applications in use across your organization. After you've determined the value of an application to your organization, App-ID controls the security policy for that application. The security policy can include a number of different actions, such as:

- Allowing or denying

- Allowing but scanning the content for exploits, viruses, and other threats

- Allowing based on schedule, users, or groups

- Controlling file or sensitive data transfer

- Allowing or denying a subset of application functions

While you are compiling the list of the applications you want to support, tolerate, or block, App-ID can restrict applications that behave in undesirable ways. You can use application categories, technologies, and risk ratings to define a security policy to block any applications that match those characteristics.

Often, safe application enablement means striking an appropriate security policy balance between allowing some application functions and denying others. Examples include:

Allowing Facebook but denying Facebook mail, chat, posting, and apps, effectively allowing users only to browse Facebook.

Allowing the use of SaaS applications such as Dropbox but denying file uploads. This technique grants internal users access to personal file shares but prevents intentional or unintended corporate information leaks.

The list of App-IDs is updated monthly, with new applications added based on input from the Palo Alto Networks community (customers, partners) and market trends. All App-IDs are classified by category, subcategory, technology, and risk rating. The security policy can use these classifications to automatically support new applications as the App-ID list expands. Alternatively, you can specify that you want to review new applications and determine how they are treated before the new list is installed.

Despite regular updates, unknown application traffic will inevitably still be detected on the network, such as:

- **Unknown commercial applications.** Administrators can use the ACC and the log viewer to quickly determine whether an unknown application is a commercial application. Administrators can use the packet capture (pcap) feature on the Palo Alto Networks next-generation firewall, to record the traffic and submit it for App-ID development. The new App-ID is developed, tested with the organization, and then added to the global database for all users.

- **Internal or custom applications.** Administrators can use the ACC and the log viewer to quickly determine whether an unknown application is an internal or custom application. You can develop a custom App-ID for the application, using the exposed protocol decoders. The protocol decoders that have been exposed include:

  - FTP (File Transfer Protocol)

  - HTTP (Hypertext Transfer Protocol) and HTTPS (HTTP Secure, or HTTP over SSL)

  - IMAP (Internet Message Access Protocol) and SMTP (Simple Mail Transfer Protocol)

  - RTSP (Real Time Streaming Protocol)

  - Telnet

  - unknown-TCP, unknown-UDP, and file body (for html/pdf/flv/swf/riff/mov)

After the custom App-ID is developed, traffic identified by it is treated in the same manner as the previously classified traffic: It can be enabled via policy, inspected for threats, shaped using quality of service (QoS), etc. Alternatively, an application override can be created and applied, which effectively renames the application. Custom App-ID entries are managed in a separate database on the next-generation firewall to ensure that they are not impacted by weekly App-ID updates.

An important point to highlight is that Palo Alto Networks next-generation firewalls use a positive enforcement model, which means that all traffic can be denied except those applications that are expressly allowed via policy. This positive enforcement model means that in some cases the unknown traffic can be easily blocked or tightly controlled. Alternative offerings that are based on IPS will allow unknown traffic to pass through without providing any semblance of visibility or control.

App-ID in action: 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 determines that it is using SSL. If there is a matching decryption policy rule, then the decryption engine and protocol decoders are initiated to decrypt the SSL and detect that it is HTTP traffic. After the decoder has the HTTP stream, App-ID can apply contextual signatures and detect that the application in use is WebEx.

WebEx is then displayed in the ACC and can be controlled via a security policy. If the end user initiates the WebEx Desktop Sharing feature, WebEx undergoes a "mode-shift": The session has been altered from a conferencing application to a remote access application. In this scenario, the characteristics of WebEx have changed, and App-ID detects the WebEx Desktop Sharing feature, which is then displayed in the ACC. At this stage, an administrator has learned more about the application use and can exert policy control over the use of the WebEx Desktop Sharing feature separately from general WebEx use.

Application identification and policy control

Application identification enables administrators to see the applications on the network, learn how they work, and analyze their behavioral characteristics and relative risk. When application identification is used in conjunction with user identification, administrators can see exactly who is using the application based on their identity, not just an IP address. With this information, administrators can use granular rules – based on a positive security model – to block unknown applications, while enabling, inspecting, and shaping those applications that are allowed.

After an application has been identified and a complete picture of its usage is gained, organizations can apply policies with a range of responses that are far more granular than the "allow" or "deny" actions available in legacy firewalls. 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

Application function control
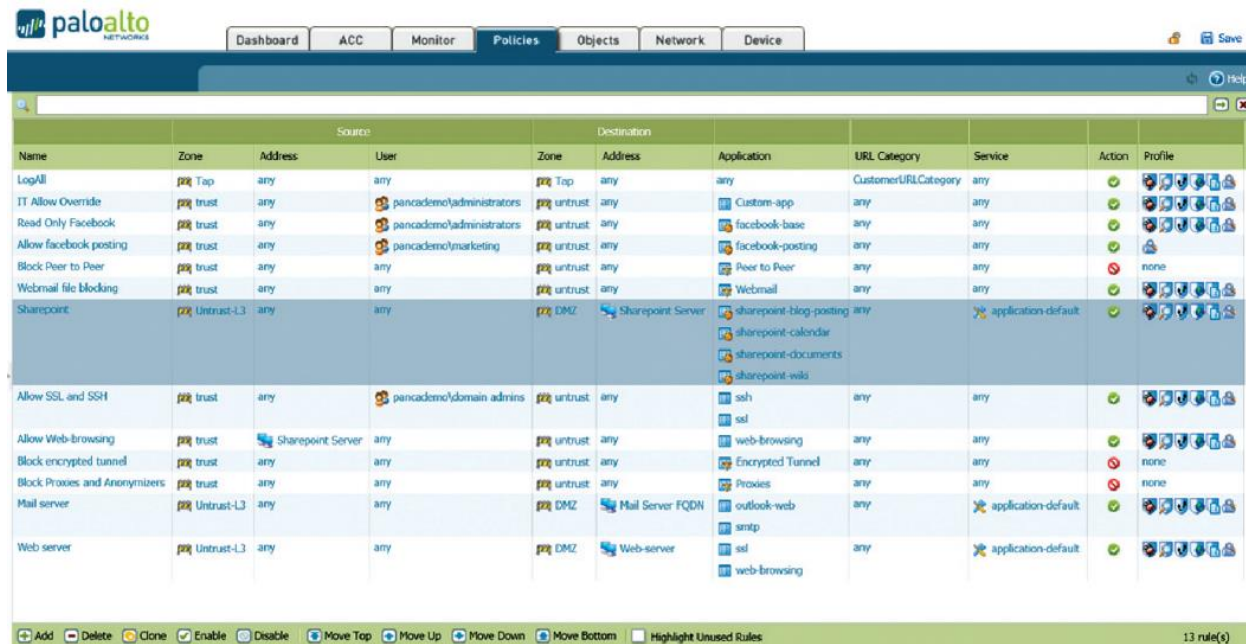
For many organizations, secure application enablement means striking an appropriate security policy balance by enabling individual application functionality while blocking other functions within the same application. Examples may include:

- Allowing SharePoint documents but blocking the use of SharePoint administration

- Blocking Facebook mail, chat, posting, and applications but allowing Facebook itself, effectively allowing users only to browse Facebook

App-ID uses an application hierarchy that follows a "container and supporting function" model to help administrators easily choose which applications to allow, while blocking or controlling functions within the application. Figure 2-8 shows SharePoint as the container application and the individual functions within it.

Figure 2-8

Application function control maximizes productivity by safely enabling the application itself (Microsoft SharePoint) or individual functions.

Controlling multiple applications: Dynamic filters and groups

In some cases, organizations may want to control applications in bulk, as opposed to controlling them individually. The two mechanisms in the Palo Alto Networks next-generation firewall that address this need are application groups and dynamic filters:

- **Application groups.** A group of applications is a static list of applications that can be used to allow their use for certain users, while blocking their use for others. For example, remote management applications such as Remote Desktop Protocol (RDP), Telnet, and Secure Shell (SSH) are commonly used by IT support personnel, yet employees who fall outside of these groups also use these tools to access their home networks. A group of applications can be created and assigned to IT support through User-ID, binding the groups to the policy. New employees only need to be added to the directory group; no updates are needed to the policy itself.

- **Dynamic filters.** A dynamic filter is a set of applications that is created based on any combination of the filter criteria: category, subcategory, behavioral characteristic, underlying technology, or risk factor. After the desired filter is created, a policy that blocks or enables and scans the traffic can be applied. As new App-ID files are added that fulfill the filter criteria, the filter is automatically updated as soon as the device is updated, thereby minimizing the administrative effort associated with policy management.