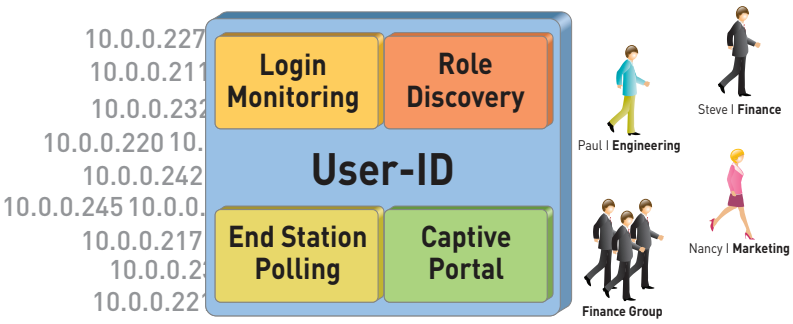
User-ID



User-ID seamlessly integrates Palo Alto Networks firewalls with a range of enterprise directory and terminal services offerings, enabling administrators to tie application activity and security policies to users and groups – not just IP addresses. When used in conjunction with App-ID™ and Content-ID™, IT organizations can leverage user and group information for visibility, policy creation, forensic investigation and reporting on application, threat, web surfing and data transfer activity.

User-ID addresses the challenge of using IP addresses to monitor and control the activity of specific network users – something that was once a fairly simple task, but has become difficult as enterprises moved to an Internet- and web-centric model.

Compounding the visibility problem in an increasingly mobile enterprise, where employees access the network from virtually anywhere around the world, internal wireless networks re-assign IP addresses as users move from zone to zone, and network users are not always company employees. The result is that the IP address is now an inadequate mechanism for monitoring and controlling user activity.

User-ID™ enables policy control over applications and content based on the employee and group identity through seamless integration with the widest range of directory services in the firewall market.

- Extends user-based application enablement polices across Microsoft Windows, Mac OS X, Apple iOS and UNIX users.
- Analyzes application, threat and web surfing activity based on individual users and groups of users, as opposed to just IP addresses.
- Enables user information harvesting from enterprise directories (Microsoft Active Directory, eDirectory, Open LDAP) and terminal services offerings (Citrix, Microsoft Terminal Services).
- Integrates with Microsoft Exchange, a captive portal and an XML API enable organizations to extend policies to Mac OS X, Apple iOS and UNIX users that typically reside outside of the domain.

paloalto NETWORKS
the network security company™

Integrating User Information into Security Policies

The ability to connect integrate user information with network security policies enables organizations to reap several significant benefits.

- Visibility: Improved visibility into application usage based on user and group information can help organizations maintain a more accurate picture of network activity.
- Policy control: Tying user information to the security policy can enable more granular control over application activity and reduces the administrative effort associated with employee moves, adds and changes.
- Logging and reporting: In the event that a security incident occurs, forensics analysis and reporting can include user information, again, providing a more complete picture of the incident.

How User-ID Works

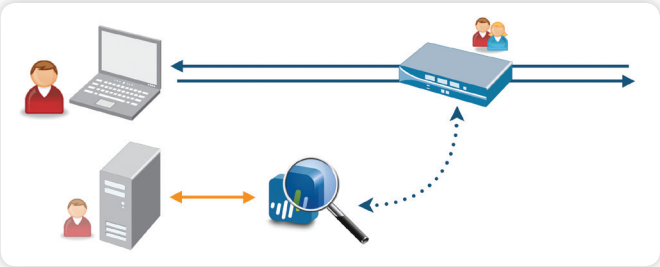
User-ID seamlessly integrates Palo Alto Networks next-generation firewalls through an agent that is installed on the network, communicating with the domain controller, mapping the user information to the IP address that is assigned to the user at a given time. On a configurable basis, the User-ID Agent uses multiple techniques to verify and maintain the user to IP address relationship.

Active Directory

In Active Directory environments, three techniques are used to collect user information: event log monitoring, server session monitoring and host probing.

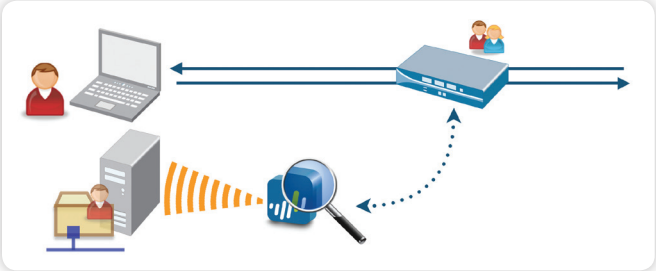
- **Event log monitoring:** Palo Alto Networks User-ID agent constantly monitors Microsoft Active Directory Domain Controllers for user logon events. Once a new user logon, Kerberos ticket grant or renewal has been identified, the user name in the log event is being associated with the origin IP address.

  In environments with Microsoft Exchange Server deployed, the User-ID Agent can be configured to constantly monitor the logon events produced by clients accessing their Microsoft Exchange mailbox. Using this technique, even Mac OS X, Apple iOS, Linux/UNIX client systems that don't directly authenticate to Microsoft Active Directory can be discovered and identified.



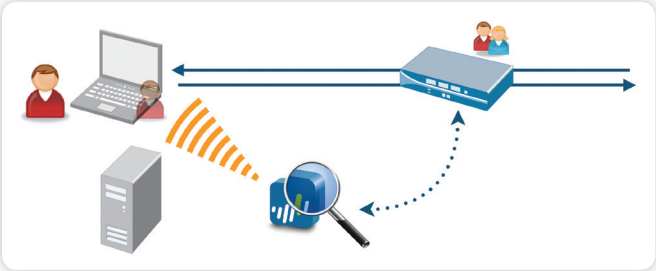
User-ID Agent monitors Domain Controller event logs.

- **Server active session monitoring:** User-ID agent can be configured to monitor active network sessions of a Microsoft Windows Server. As soon as a user accesses a network share on the server, the agent identifies the origin IP address and maps it to the user name provided to establish the session.



User-ID Agent monitors server file sharing sessions.

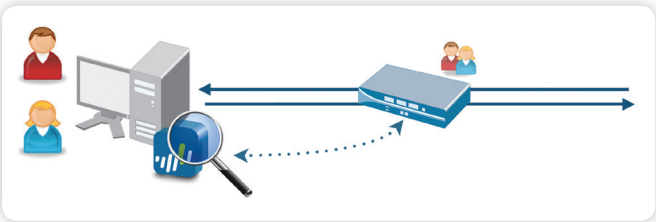
- **Host probing:** In order to ensure the accuracy and status of a user IP relation, User-ID agent can be configured to periodically probe Microsoft Windows Clients remotely for logged on users through Windows Management Instrumentation (WMI) or NetBios protocol.



User-ID Agent probes client machines for user information.

Terminal Services Environments

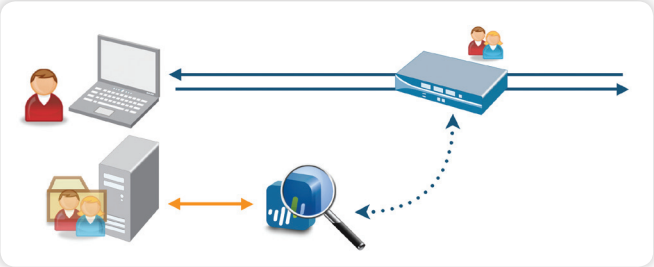
In environments were the user identity is obfuscated by a Terminal Services deployment (Citrix or Microsof), User-ID can be deployed to determine which applications users are accessing. Users sharing IP addresses working on Microsoft Windows Terminal Services or Citrix can be identified. Completely transparent to the user, every user session is assigned a certain port range on the server, which allows the firewall to associate network connections with users and groups sharing one host on the network. Once the applications and users are identified, full visibility and control within ACC, policy editing, logging and reporting is available.



Terminal Services Agent allocates port ranges for logged on users.

Novell eDirectory

In Novell eDirectory environments, User-ID can query and monitor existing information to identify users and group memberships via standard LDAP queries on the Novell eDirectory servers.

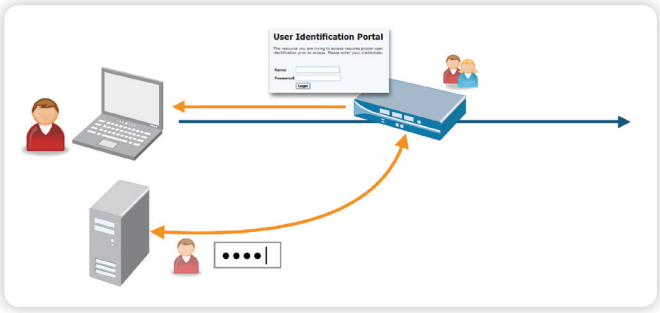


User-ID Agent monitors user eDirectory logon events and resolves group membership.

Other LDAP Directories

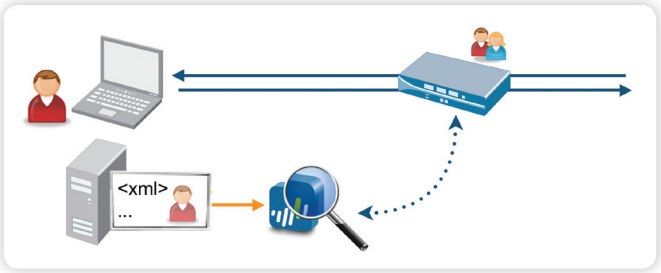
In other non Active Directory environments, the firewall can retrieve user and group information via standard LDAP from most LDAP based directory servers. The association of users to computers can be achieved through other means, for example Captive Portal or XML API.

- **Captive Portal:** In cases where administrators need to establish rules under which users are required to authenticate to the firewall prior to accessing the internet, a captive portal can be deployed. Captive portal is used in cases where the user cannot be identified using other mechanisms, or a User-ID Agent is not deployed. In addition to an explicit username and password prompt, captive portal can also be configured to send a NTLM authentication request to the web browser in order to make the authentication process transparent to the user.



Captive portal provides users with a challenge/response mechanism.

- **XML API:** In some cases, organizations may already have a user repository or an application that is used to store information on users and their current IP address. For example an in-house developed application, which requires authentication and keeps track of the users' computer. In these scenarios, an XML API within the User-ID Agent enables rapid integration of user information with security policies.

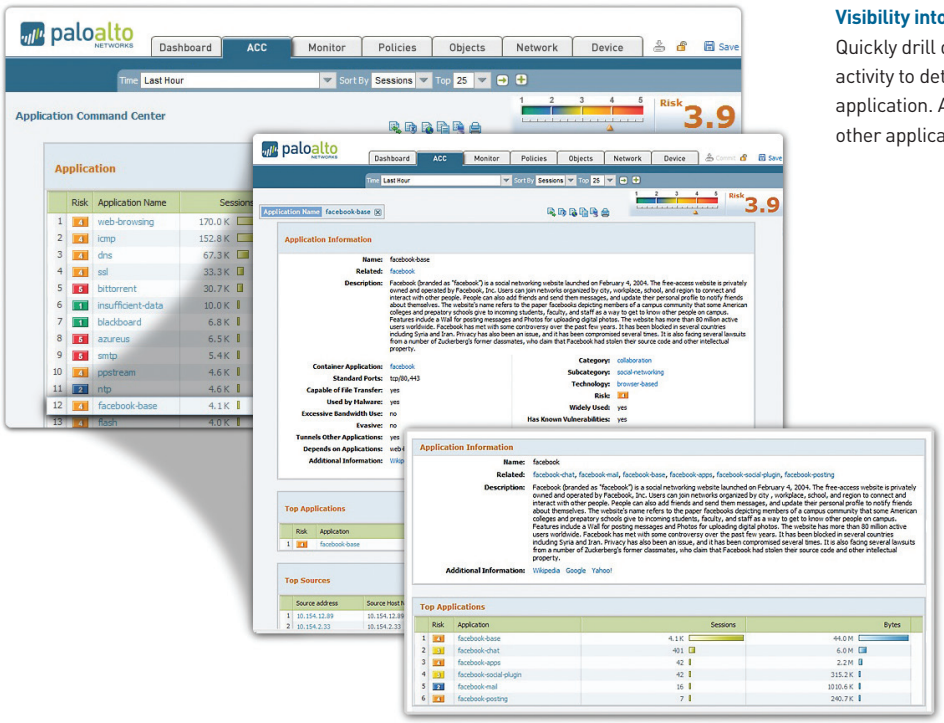


XML API enables organizations to integrate with custom or 3rd party repositories.

Visibility into User's Application Activity

The power of User-ID becomes evident when a strange or unfamiliar application is fond on the network by App-ID. Using Application Command Center (ACC), an administrator can discern what the application is, and who is using the application. Investigating the other applications that an individual user may be accessing is as easy as selecting their user name with a mouse click. The administrator can then see the different applications used, the bandwidth and sessions consumed, as well as threats. Flexible drill down features in ACC enable the administrator to not only see all the users of the individual application, but also the bandwidth and session consumption, the sources and destinations of the application traffic as well as any associated threats.

Visibility into the application activity at a user level, not just an IP address level, is a required step in regaining control over the applications traversing the network. Administrators can align application usage with the business unit requirements and if appropriate, can chose to inform the user that they are in violation of corporate policy, or take a more direct approach of blocking the user's application usage outright.



Visibility into a User's Application Activity
Quickly drill down into unusual application activity to determine who is using the application. Additional drill down shows other applications for individual users.

User-based Policy Control

The increased visibility into the application usage that is generated by App-ID means the security team can quickly analyze the role and risk of applications, who is using them, then easily translate that information into user-based application control policies. The ability to control applications based on users and groups, as opposed to IP addresses is a key differentiator for Palo Alto Networks. User-based policy controls can be assembled based on the application, which category and subcategory it belongs in, its underlying technology or what the application characteristics are. Policies can be used to control application access for specific users or groups in either an outbound or an inbound direction. Examples of user-based policies might include:

- Enable only the IT department to use tools such as SSH, telnet, and FTP on the standard port.
- Allow the Help Desk Services group to use Yahoo Messenger.
- Block the use of Facebook-apps for all users, allow Facebook for all users, yet allow only marketing to use Facebook-posting.

User-based Analysis, Reporting and Forensics

Access to the user and group information for visibility and control over application and threat activity is pervasive throughout the Palo Alto Networks next generation firewalls. Application Command Center provides an initial view into users application activity while the log viewer provides more fine-grained forensic analysis.

Informative reports on user activities can be generated using any one of the many pre-defined reports or by creating a custom report. Custom reports can be quickly created from scratch or by modifying a pre-defined report. Any of the reports – predefined or custom – can be exported to either CSV or PDF, or emailed on a scheduled basis to an interested manager or an HR group.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com