USER-ID

Strengthen Security Posture and Improve Visibility by Mapping Network Traffic to Users

User-ID is a standard feature of our next-generation security platform that enables visibility, security policies, reporting, and forensics based on users and groups – not just IP addresses. When used in conjunction with App-ID™ and Content-ID™, your visibility and security policies are based on IT-relevant context.

User-ID™ allows you to safely enable applications and content based on user identity information from a wide range of sources

- Enables user-based application enablement and security policies across Microsoft® Windows®, Apple® iOS and Mac® OS X®, Android™, and Linux®/UNIX users
- Enables analysis of application, threat and web surfing activity in terms of individual users, and groups of users

In support of business flexibility, many organizations have the need to support multiple types of end users across a variety of locations and access technologies. In these environments, IP addresses are no longer an effective proxy for end users. Instead, user and group information must be directly integrated into the technology platforms that secure modern organizations.

User-ID: Integrating User Information into Your Security Infrastructure

The user identity, as opposed to an IP address, is an integral component of an effective security infrastructure. Knowing who is using each of the applications on your network, and who may have transmitted a threat or is transferring files, can strengthen security policies and reduce incident response times. User-ID enables you to leverage user information stored in a wide range of repositories for the following uses:

- **Visibility:** Improved visibility into application usage based on users gives you a more relevant picture of network activity.
- **Policy control:** Tying user information to the security policies safely enables applications while reducing the administrative effort associated with end-user moves, adds and changes.
- **Logging, reporting, forensics:** If a security incident occurs, forensics analysis and reporting based on user information provides a more complete picture of the incident.

How User-ID Works

User-ID integrates our next-generation firewall functionality with a wide range of user repositories and terminal services environments. Depending on your environment, multiple techniques can be configured for user and group mapping. Once the applications, users, and groups are identified, full visibility and control within the application command center (ACC), policy editing, logging and reporting is available.

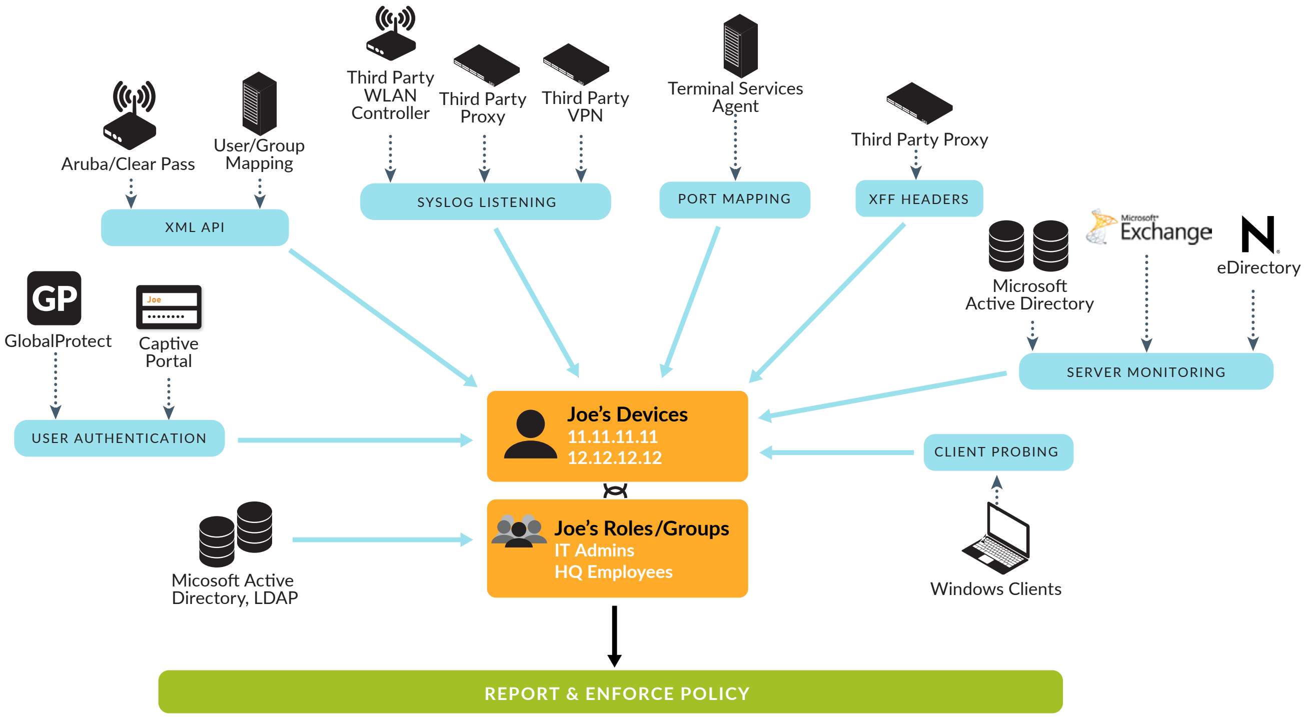

Figure 1: How User-ID Works

User-ID can use a combination of the following techniques for user mapping (group mapping will be addressed in a later section).

User Authentication: User-ID can get usernames when users authenticate themselves on a GlobalProtect client or on a captive portal in the browser.

- **GlobalProtect™:** The GlobalProtect client provides user and host information to the firewall that, in turn, can be used for policy control. GlobalProtect applies to both remote and on-premises devices, and is available for Windows, OS X, iOS, and Android.
- **Captive Portal:** Captive portal is used in cases where the user cannot be identified using other mechanisms. In addition to an explicit username and password prompt, captive portal can be configured to send a Kerberos authentication request to the web browser in order to make the authentication process transparent to the user.

XML API: Finally, the User-ID XML API is a powerful augment to the previous techniques, providing a programmatic way to map users from a variety of environments. Current integrations with partner technologies, such as Aruba ClearPass and Mobility Controller, use the XML API for seamless exchange of IP address to user mapping.

Syslog Listening: In environments with existing network services that authenticate users, (e.g., wireless controllers, 802.1X, or NAC products), User-ID can monitor syslog messages for user mapping. Extensible "syslog filters" control the parsing of syslog messages. Syslog filters can be user-defined, but there are several pre-defined filters including those for Blue Coat proxy, WLANs and Pulse Policy Secure.

Port Mapping: In Citrix® XenApp® or Microsoft Terminal Services environments, multiple users may be using the same IP address. The User-ID Terminal Services Agent enables organizations to differentiate users and the applications they are using. Each 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.

XFF Headers: User-ID can read the IPv4 or IPv6 addresses of users from the X-Forwarded-For (XFF) header in HTTP client requests when the firewall is deployed between the Internet and a proxy server that would otherwise hide the user IP addresses. User-ID matches the true user IP addresses with usernames.

Server Monitoring: User-ID can be configured to monitor authentication events for Microsoft Active Directory®, Microsoft Exchange and Novell® eDirectory™ environments. Monitoring of the authentication events on a network allows User-ID to associate a user with the IP address of the device from which the user logs in.

- **Microsoft Active Directory:** User-ID can be configured to constantly monitor domain log-on events (from either an agent running on the firewall a Windows server).
- **Microsoft Exchange Server:** User-ID can be configured to constantly monitor the Microsoft Exchange log-on events produced by clients accessing their email. Using this technique, even OS X, Apple iOS, Android, and Linux/UNIX client systems that don't directly authenticate to Microsoft Active Directory can be discovered and identified.

- **Novell eDirectory:** User-ID can be configured to monitor log-on events to identify users from Novell eDirectory servers.

Client Probing: User-ID can be configured to actively probe Microsoft Windows clients for user information.

Extending Control to Groups

In addition to user mapping, User-ID integrates with the "directory services" of many environments to accomplish group mapping. LDAP is used to integrate with a variety of directory servers including, once again, Active Directory.

Also, as in the case of user mapping, the XML API can be used as a programmatic interface for flexible group mapping capability.

With User-ID group mapping, security policies can be expressed in terms of groups, allowing existing policies to function even as users are added or removed from groups.

Visibility into a User's Application Activity

The power of User-ID becomes evident when a strange or unfamiliar application is found on your network by App-ID. Using either ACC or the log viewer, your security team can discern what the application is, who the user is, the bandwidth and session consumption, along with the source and destination 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, allows you to more effectively enable the applications traversing the network. You can align application usage with business requirements and, if appropriate, inform users that they are in violation of policy, or even block their application usage outright.

User-Based Policy Control

User-based policy controls can also include application information (including which category and subcategory it belongs in, its underlying technology, or what the application characteristics are). Policies can be defined to safely enable applications based on users or groups of users, in either outbound or inbound directions. Examples of user-based policies include:

- Enable only the IT department to use tools such as SSH, telnet, and FTP on standard ports.
- Allow the Help Desk Services group to use Slack.
- Allow all users to read Facebook, but block the use of Facebook apps, and restrict posting to employees in marketing.

User-Based Analysis, Reporting and Forensics

Informative reports on user activities can be generated using any one of the pre-defined reports or by creating a custom report. Examples of pre-defined reports are User/Group Activity report that summarizes the web activity of individual users or user groups, and SaaS Application Usage 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.

Summary

User-ID brings knowledge of users and groups to the visibility and enforcement capabilities of Palo Alto Networks Next-Generation Firewalls. Along with the context provided by App-ID and Content-ID, it is a powerful foundation for improving your organization's security posture.

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com