User identification

As you define security policies based on application use, a key component of that policy is who should be able to use those applications. IP addresses are ineffective identifiers of the user or the role of the server within the network. With the User-ID and dynamic address group (DAG) features, you can dynamically associate an IP address with a user or the role of a server in the data center. Afterward, you can define security policies that adapt dynamically to changing environments.

In environments that support multiple types of end users (for example, Marketing or Human Resources) across a variety of locations and access technologies, it is unrealistic to guarantee physical segmentation of each type of user. Visibility into the application activity at a user level, not just at an IP address level, allows you to more effectively enable the applications traversing the network. You can define both inbound and outbound policies to safely enable applications based on users or groups of users. Examples of user-based policies include:

- Enabling the IT department to use SSH, Telnet, and FTP on standard ports
- Allowing the Help Desk Services group to use Slack
- Allowing all users to read Facebook but blocking the use of Facebook apps and restricting posting to only employees in Marketing

User-ID: Integrating user information and security policies

Creating and managing security policies on an next-generation firewall, based on the application and the identity of the user regardless of device or location, is a more effective means of protecting the network than relying solely on port and IP address information in legacy, port-based firewalls. User-ID enables organizations to leverage user information stored in a wide range of repositories for the following purposes:

- **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.** Binding user information to the security policy helps organizations to safely enable applications or specific application functions, while reducing the administrative effort associated with employee moves, adds, and changes.
- **Logging and reporting.** If a security incident occurs, forensics analysis and reporting can include user information, which provides a more complete picture of the incident.

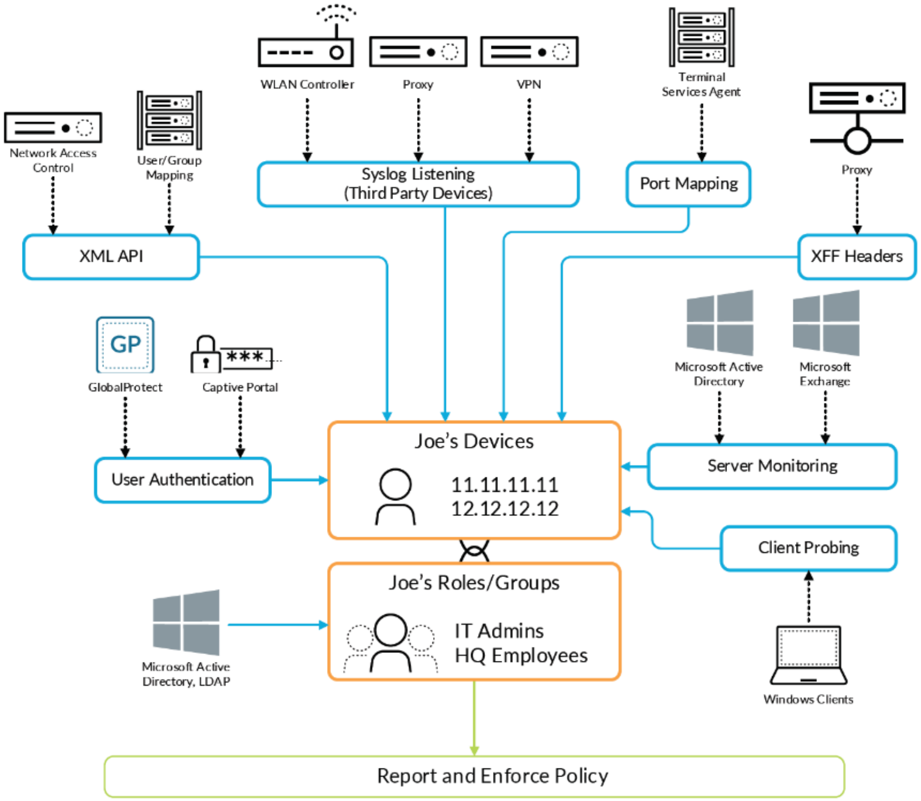
Palo Alto Networks Cybersecurity Academy

User-ID in action

User-ID seamlessly integrates Palo Alto Networks next-generation firewalls with a wide range of user repositories and terminal services environments. Depending on the network environment, multiple techniques can be configured to accurately map the user identity to an IP address. Events include authentication events, user authentication, terminal services monitoring, client probing, directory services integration, and a powerful XML API (see Figure 2-9).

Figure 2-9

User-ID integrates enterprise directories for user-based policies, reporting, and forensics.



After the applications and users are identified, full visibility and control within the Application Command Center (ACC), policy editing, and logging and reporting are available. User-ID tools and techniques include:

- **User authentication.** This technique allows organizations to configure a challenge-response authentication sequence to collect user and IP address information, using the following tools:
  - **Authentication Portal.** In cases where administrators need to establish rules under which users are required to authenticate to the firewall before accessing the internet, Authentication Portal can be deployed. Authentication Portal is used in cases where the user cannot be identified using other mechanisms. In addition to an explicit username and password prompt, Authentication Portal can also be configured to send an NT LAN Manager (NTLM) authentication request to the web browser to make the authentication process transparent to the user.

    - **Prisma Access.** Users logging in to the network with Prisma Access (discussed in Section 3.5.2) provide user and host information to the next-generation firewall, which, in turn, can be used for policy control.

- **Server monitoring.** 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 to enforce policy on the firewall. User-ID can be configured to monitor authentication events for:

    - **Microsoft Active Directory.** User-ID constantly monitors domain controller event logs to identify users when they log in to the domain. When a user logs in to the Windows domain, a new authentication event is recorded on the corresponding Windows domain controller. By remotely monitoring the authentication events on Windows domain controllers, User-ID can recognize authentication events to identify users on the network for creation and enforcement of policy.

    - **Microsoft Exchange Server.** User-ID can be configured to constantly monitor Microsoft Exchange login events produced by clients accessing their email. Using this technique, even macOS, Apple iOS, and Linux/Unix client systems that don't directly authenticate to Active Directory can be discovered and identified.

    - **Novell eDirectory.** User-ID can query and monitor login information to identify users and group memberships via standard Lightweight Directory Access Protocol (LDAP) queries on eDirectory servers.

- **Client probing and terminal services.** This technique enables organizations to configure User-ID to monitor Windows clients or hosts to collect the identity and map it to the IP address. In environments where the user identity is obfuscated by Citrix XenApp or Microsoft Terminal Services, the User-ID Terminal Services agent can be deployed to determine which applications are being accessed by users. The following techniques are available:

    - **Client probing.** If a user cannot be identified via monitoring of authentication events, User-ID actively probes Microsoft Windows clients on the network for information about the currently logged-on user. With client probing, laptop users who often switch from wired to wireless networks can be reliably identified.

    - **Host probing.** User-ID can also be configured to probe Windows servers for active network sessions of a user. As soon as a user accesses a network share on the server, User-ID identifies the origin IP address and maps it to the username provided to establish the session.

    - **Terminal services.** Users sharing IP addresses while working on Microsoft Terminal Services or Citrix can be identified. Every user session is assigned a certain port range on the server, which is completely transparent to the user and allows the next-generation firewall to associate network connections with users and groups sharing one host on the network.

Palo Alto Networks Cybersecurity Academy

- **XML API.** In some cases, organizations may already have a user repository or an application that is used to store information about users and their current IP address. In these scenarios, the XML API within User-ID enables rapid integration of user information with security policies. The XML API provides a programmatic way to map users to IP addresses through integrations with partner technologies, such as Aruba ClearPass and Aruba Mobility Controllers. Use of the XML API to collect user and IP address information includes:
  - **Wireless environments.** Organizations using 802.1*x* to secure corporate wireless networks can leverage a syslog-based integration with the User-ID XML API, to identify users as they authenticate to the wireless infrastructure.
  - **Proxies.** Authentication prompted by a proxy server can be provided to User-ID via its XML API, by parsing the authentication log file for user and IP address information.
  - **Network access control (NAC).** The XML API enables organizations to harvest user information from NAC environments. As an example, Bradford Networks, a NAC solution provider, uses the User-ID XML API to populate user logins and logouts of its 802.1*x* solution. This integration enables organizations to identify users as soon as they connect to the network and set user-based enablement policies.
- **Syslog listener.** In environments with existing network services that authenticate users – for example, wireless controllers, 802.1*x*, 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 several predefined filters are available, including those for Blue Coat proxy, wireless local-area networks (WLANs), and Pulse Policy Secure.

To enable organizations to specify security rules based on user groups and resolve the group members automatically, User-ID integrates with directory servers by using a standards-based protocol and a flexible configuration. After integration with the directory server is configured, the firewall automatically retrieves user and user group information and keeps the information updated to automatically adjust to changes in the user base or organization.

After User-ID gathers the user information, the next-generation firewall uses LDAP to obtain group information for that user. Also, as in the case of user mapping, the XML API can serve as a programmatic interface for a flexible group mapping ability. With group mapping, User-ID can express security policies in terms of groups, enabling existing policies to update dynamically as User-ID adds or removes users from groups.

User-ID gives you only half the picture when tying IP addresses to specific users. Servers and many other devices cannot use a user to identify their security access requirements. Dynamic address groups (DAGs) enable you to create policy that automatically adapts to server additions, moves, or deletions. They also enable the flexibility to apply security policy to the device based on its role on the network.

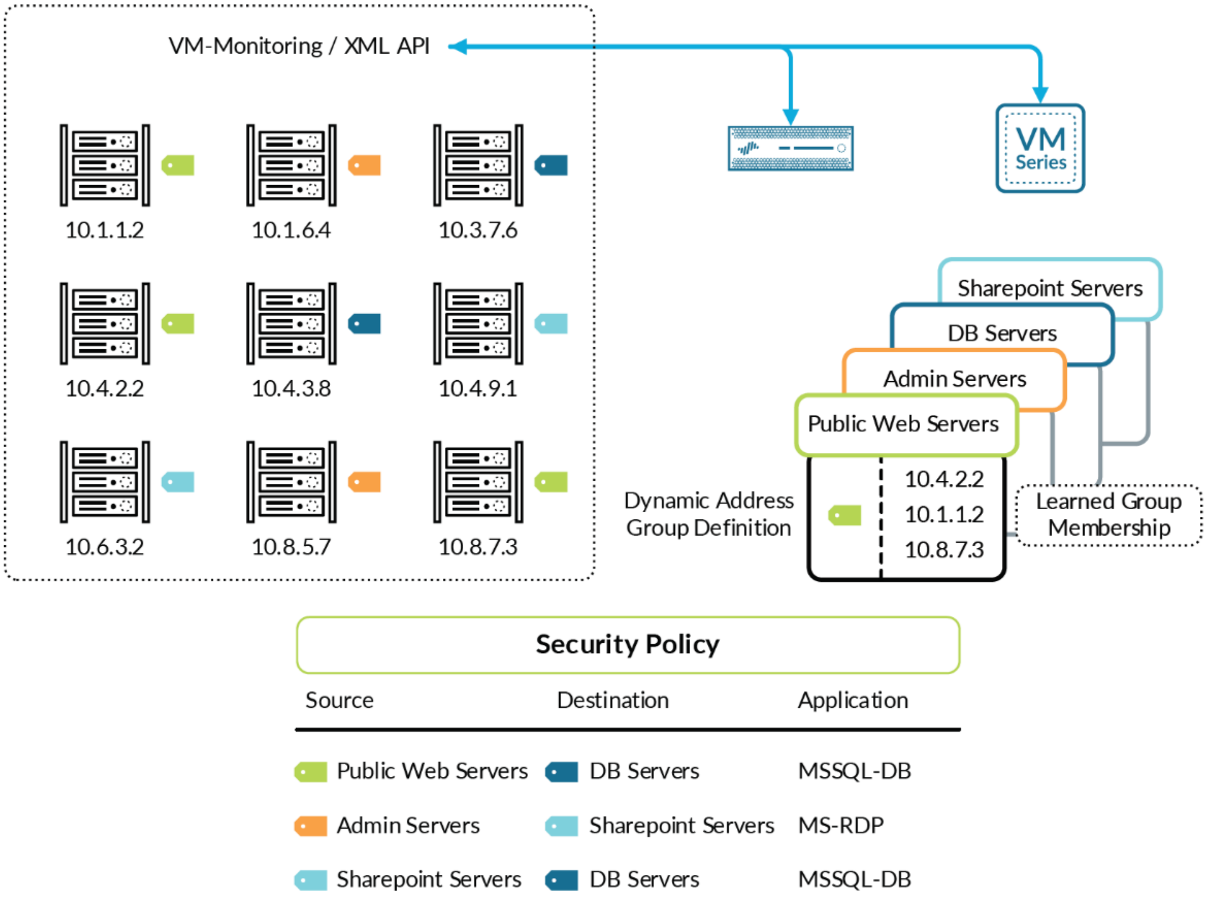
Palo Alto Networks Cybersecurity Academy

A DAG uses tags as a filtering criterion in order to determine its members. You can define tags statically or register them dynamically. You can dynamically register the IP address and associated tags for a device on the firewall by using the XML API or the VM Monitoring agent on the firewall; each registered IP address can have multiple tags. Within 60 seconds of the API call, the firewall registers the IP address and associated tags and automatically updates the membership information for the DAGs.

Because the members of a DAG are automatically updated, you can use address groups to adapt to changes in your environment without relying on a system administrator to make policy changes and committing them (see Figure 2-10).

Figure 2-10

Dynamic address groups (DAGs)



Security Policy

Source	Destination	Application
Public Web Servers	DB Servers	MSSQL-DB
Admin Servers	Sharepoint Servers	MS-RDP
Sharepoint Servers	DB Servers	MSSQL-DB

Visibility into a user’s activity

The power of User-ID becomes evident when App-ID finds a strange or unfamiliar application on the network. An administrator can use either the ACC or the log viewer to identify the application, who is using the application, the bandwidth and session consumption, the sources and destinations of the application traffic, and any associated threats.

Visibility into the application activity at a user level, not just at an IP address level, allows organizations to more effectively enable the applications traversing the network. Administrators can align application usage with business unit requirements and, if appropriate, can choose to inform the user that they are in violation of policy, or they can take the more direct approach of blocking the user’s application usage outright.

User-based policy control

User-based policy controls can be created based on the application, category and subcategory, underlying technology, or application characteristics. Policies can be used to safely enable applications based on users or groups, in either an outbound or an inbound direction.

User-based policies might include:

- Enable only the IT department to use tools such as SSH, Telnet, and FTP on their standard ports.
- Allow the Help Desk Services group to use Yahoo Messenger.
- Allow Facebook for all users, allow only the Marketing group to use Facebook-posting, and block the use of Facebook applications for all users.

Policy Optimizer

Policy Optimizer can help organizations migrate from legacy firewall rule configurations to application-based rules through App-ID. This capability strengthens the security posture by using App-ID to close any security gaps and minimizes configuration errors – a leading cause of breaches. Policy Optimizer analyzes application use and recommends policy rules that reduce exposure and risk.

Policy Optimizer identifies port-based rules so that they can be converted to application-based rules. Converting from port-based to application-based rules improves the overall security posture because you can whitelist the applications you want to permit and then deny all other applications. Policy Optimizer makes it simple for you to prioritize which of the port-based rules to migrate first, identify application-based rules that allow applications you don’t use, and analyze each of the rules’ usage characteristics, such as hit count.

Palo Alto Networks Cybersecurity Academy