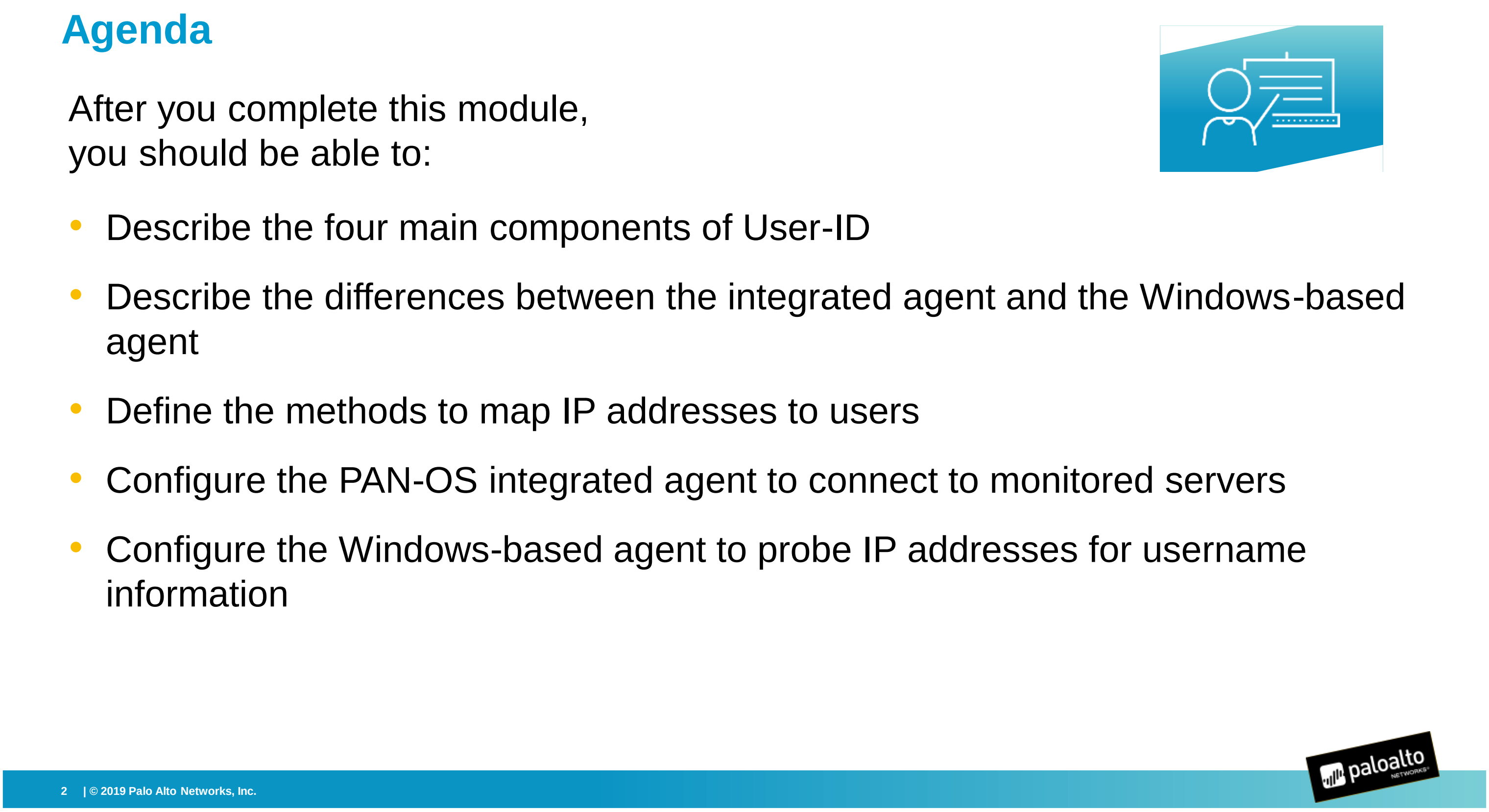
USER-ID

EDU-210 Version A
PAN-OS® 9.0

KNOW THE WHO; CONTROL THE WHO

- User-ID overview
- User mapping methods overview
- Configuring User-ID
- PAN-OS® integrated agent configuration
- Windows-based agent configuration
- Configuring group mapping
- User-ID and security policy



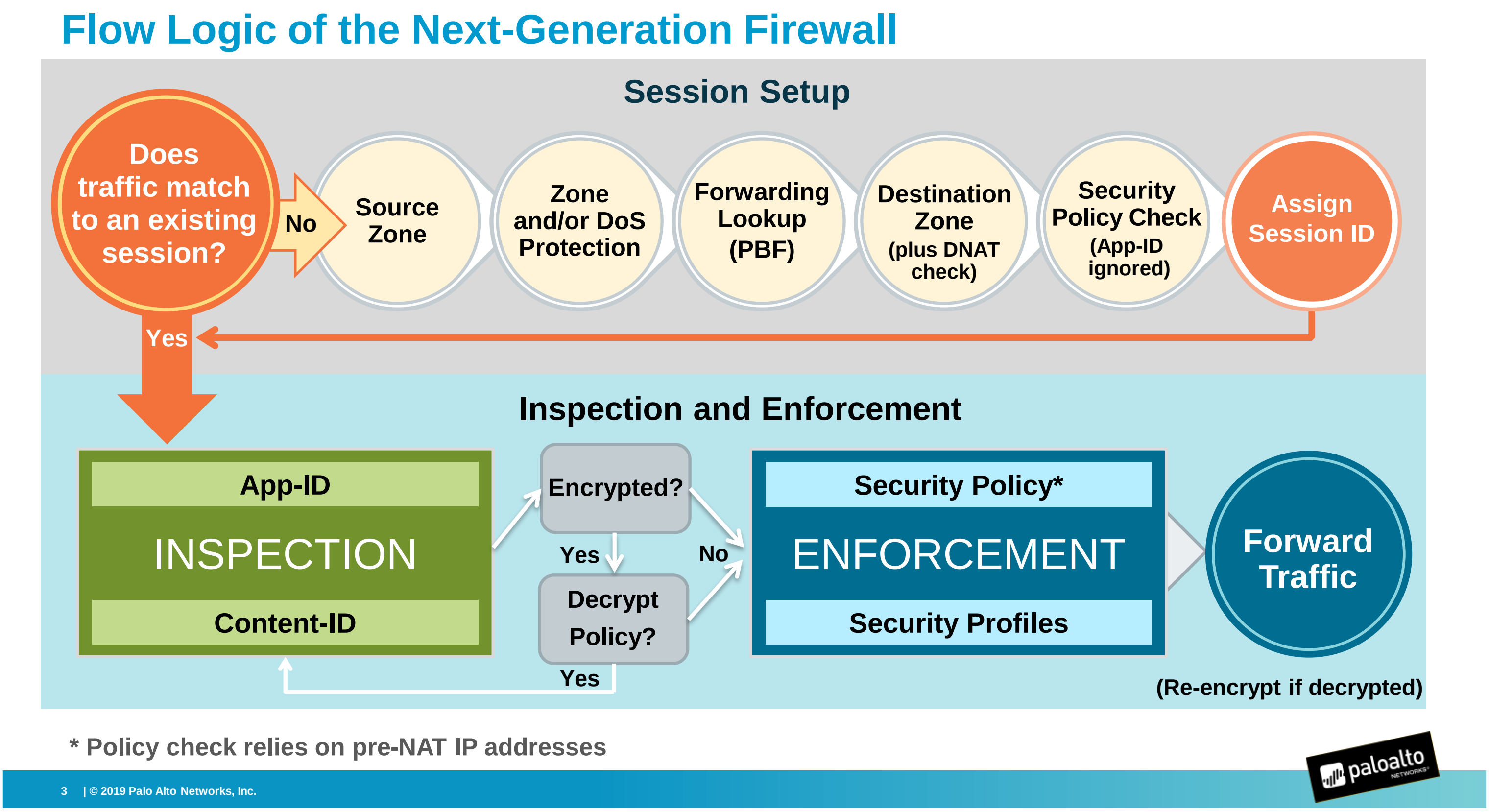
Agenda

After you complete this module,
you should be able to:

- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information

After you complete this module, you should be able to:

- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information



Flow Logic of the Next-Generation Firewall

Session Setup

Does traffic match to an existing session?

No

Source Zone

Zone and/or DoS Protection

Forwarding Lookup (PBF)

Destination Zone (plus DNAT check)

Security Policy Check (App-ID ignored)

Assign Session ID

Yes

Inspection and Enforcement

App-ID

INSPECTION

Content-ID

Encrypted?

Yes

No

Decrypt Policy?

Yes

Security Policy*

ENFORCEMENT

Security Profiles

Forward Traffic

(Re-encrypt if decrypted)

* Policy check relies on pre-NAT IP addresses

3 | © 2019 Palo Alto Networks, Inc.

This diagram is a simplified version of the flow logic of a packet traveling through a Palo Alto Networks firewall. The course will reference this diagram to address where specific concepts fit into the packet processing sequence.

For more information about the packet handling sequence inside of a PAN-OS device, see the *Packet Flow Sequence in PAN-OS* document available on the Palo Alto Networks Support website at https://live.paloaltonetworks.com/docs/DOC-1628.

User-ID overview

User mapping methods overview

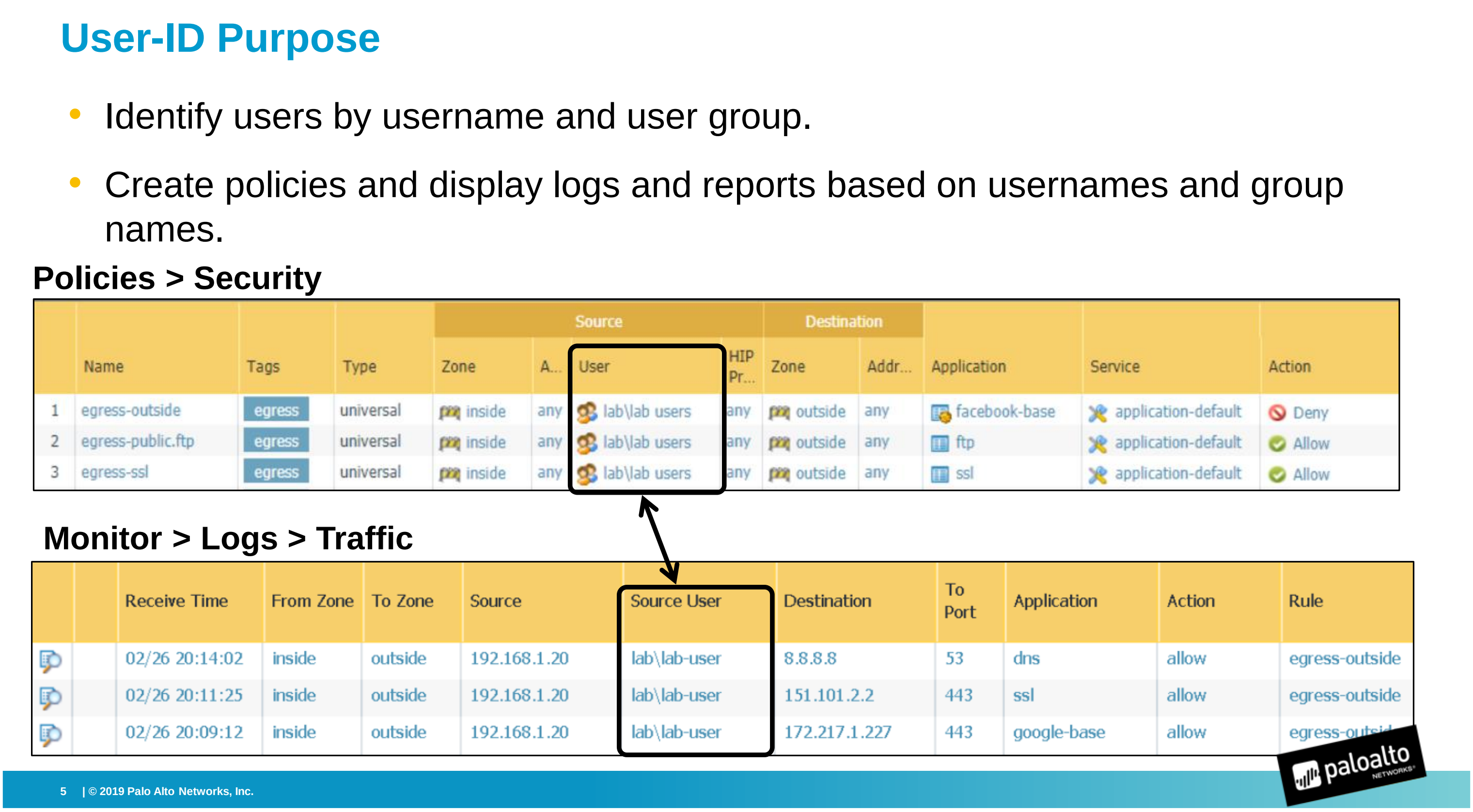
Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy



User-ID Purpose

- Identify users by username and user group.
- Create policies and display logs and reports based on usernames and group names.

Policies > Security

				Source				Destination				
	Name	Tags	Type	Zone	A...	User	HIP Pr...	Zone	Addr...	Application	Service	Action
1	egress-outside	egress	universal	inside	any	lab\lab users	any	outside	any	facebook-base	application-default	Deny
2	egress-public.ftp	egress	universal	inside	any	lab\lab users	any	outside	any	ftp	application-default	Allow
3	egress-ssl	egress	universal	inside	any	lab\lab users	any	outside	any	ssl	application-default	Allow

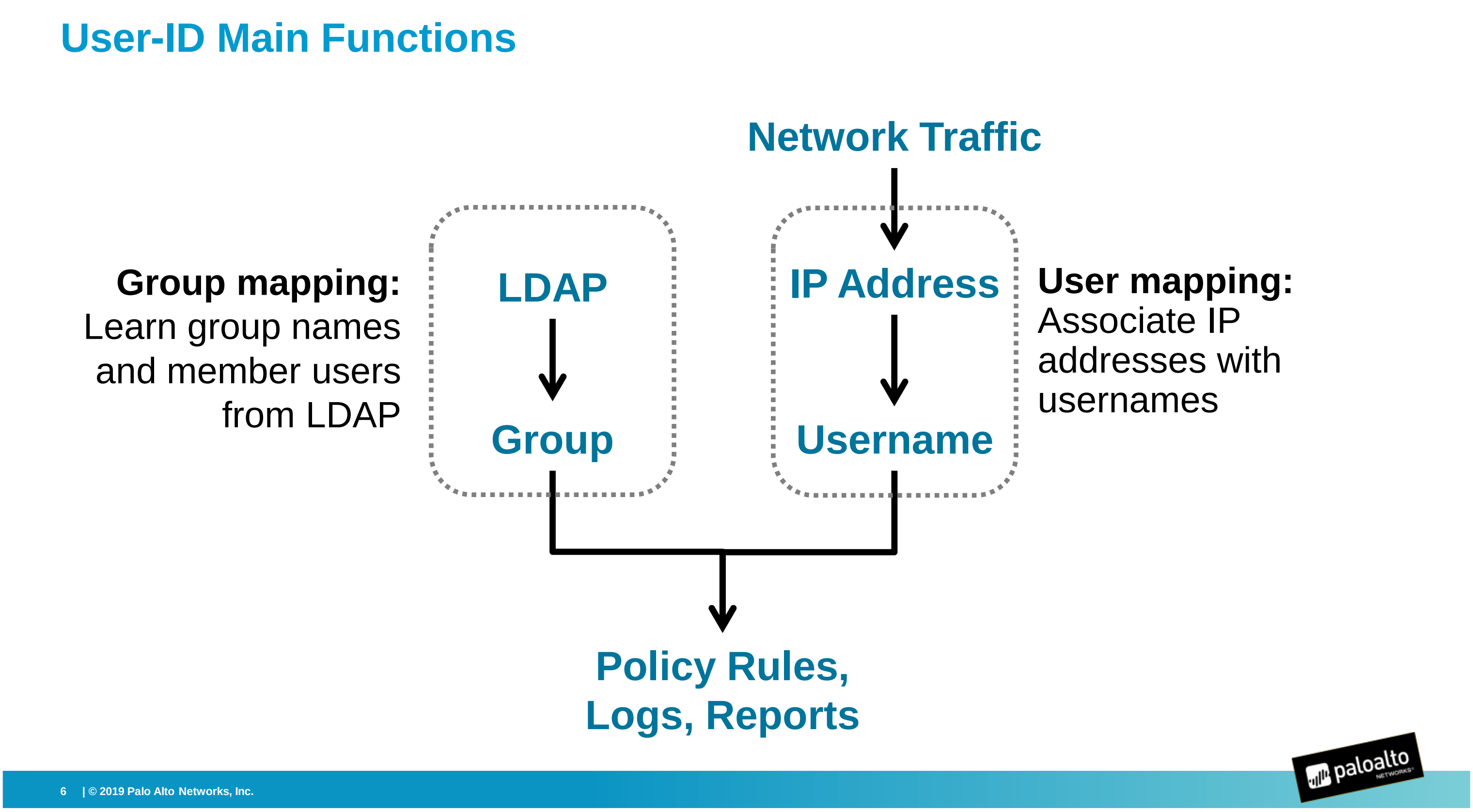
Monitor > Logs > Traffic

		Receive Time	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
		02/26 20:14:02	inside	outside	192.168.1.20	lab\lab-user	8.8.8.8	53	dns	allow	egress-outside
		02/26 20:11:25	inside	outside	192.168.1.20	lab\lab-user	151.101.2.2	443	ssl	allow	egress-outside
		02/26 20:09:12	inside	outside	192.168.1.20	lab\lab-user	172.217.1.227	443	google-base	allow	egress-outsid

The increasingly dynamic nature of users and applications means that IP addresses alone have become less effective as a mechanism for monitoring and controlling user activity. User-ID technology identifies the user on the network and the IP addresses of the computers the user is logged in to. User-ID also retrieves user group information from a connected LDAP directory.

The ultimate purpose of User-ID is to give you the ability to write policy, display logs, and display reports using usernames instead of using just IP addresses and port numbers. User-ID combined with App-ID technology provides you with very granular control over which users or user groups may access which applications from which network segments. For example, unknown users can be treated differently from known users to accommodate network guests.

Multiple policy types support User-ID. You can use usernames or group names as matching criteria in Authentication policies, Decryption policies, DoS Protection policies, Policy-Based Forwarding policies, QoS policies, Security policies, and Tunnel Inspection policies.



User-ID Main Functions

Network Traffic

Group mapping: Learn group names and member users from LDAP

LDAP → Group

IP Address → Username

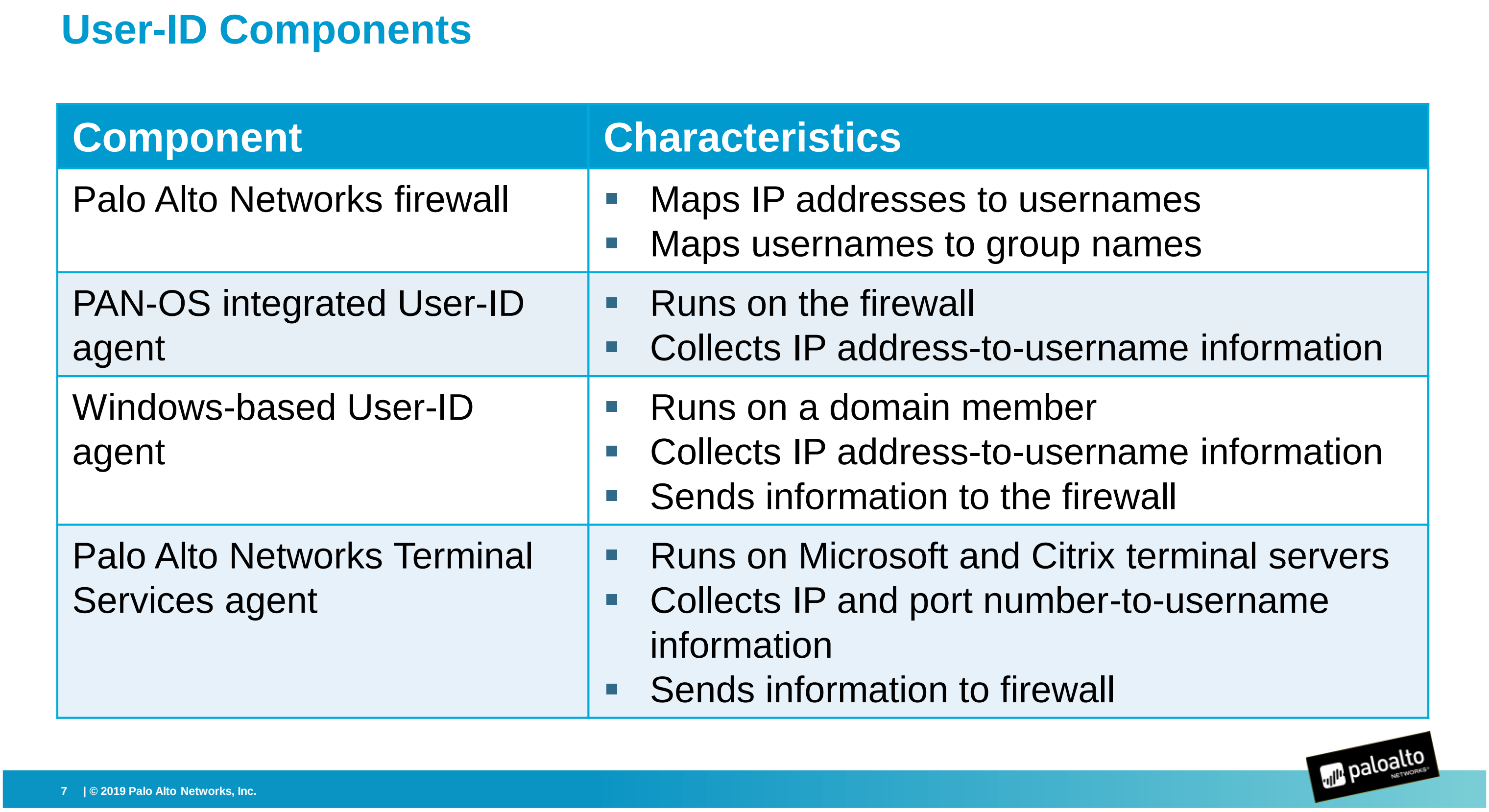
User mapping: Associate IP addresses with usernames

Policy Rules, Logs, Reports

6 | © 2019 Palo Alto Networks, Inc.

Before you can create user-based and group-based policy rules, the firewall requires a list of all available users and their corresponding group mappings. The firewall uses group mapping and user mapping to collect this information.

The firewall collects group mapping information by reading group information directly from your LDAP directory server. User-ID technology includes many methods to collect IP address-to-username mapping information. You can choose which user mapping methods to use to suit your environment, and even use different methods at different sites.



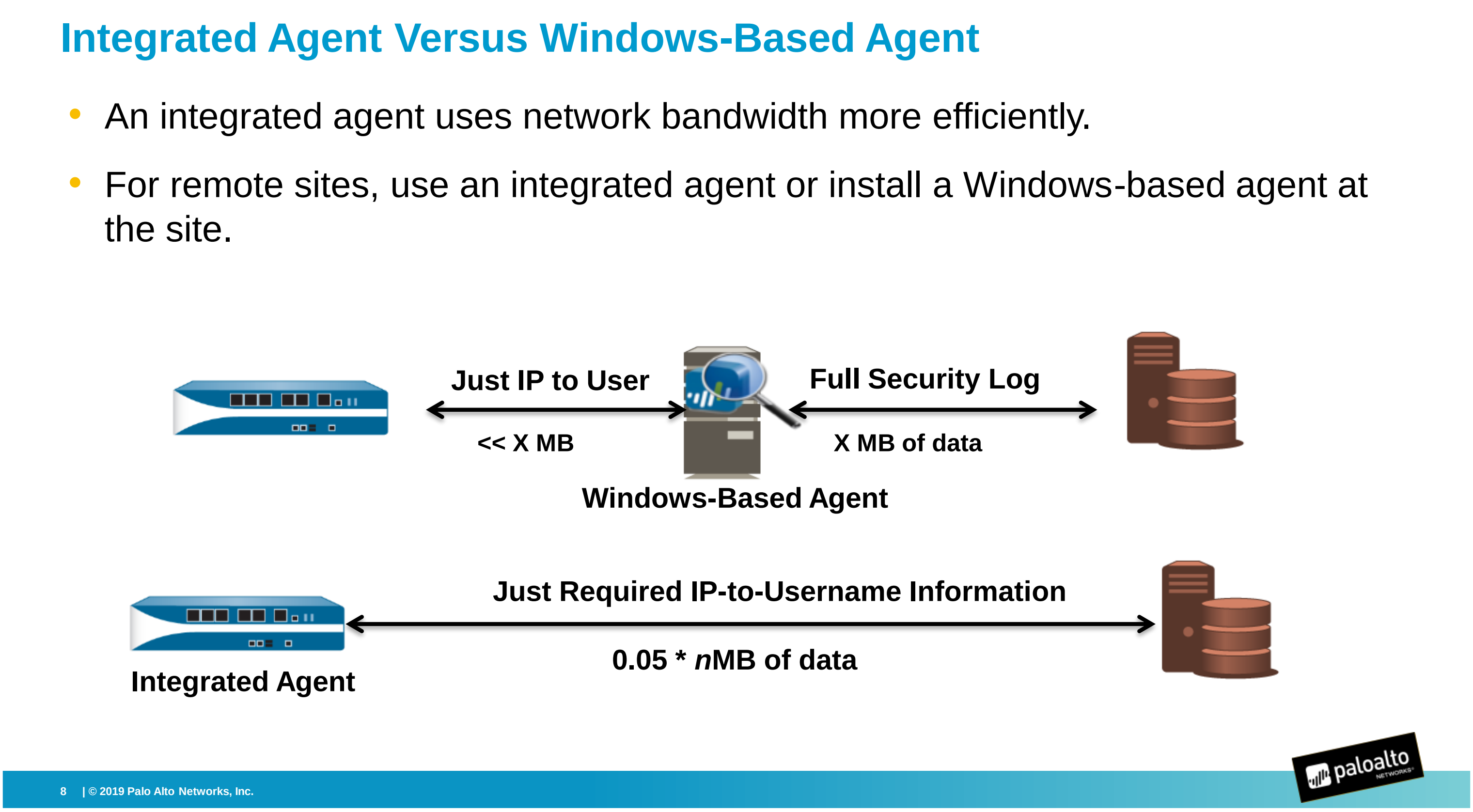
User-ID Components

Component	Characteristics
Palo Alto Networks firewall	▪ Maps IP addresses to usernames ▪ Maps usernames to group names
PAN-OS integrated User-ID agent	▪ Runs on the firewall ▪ Collects IP address-to-username information
Windows-based User-ID agent	▪ Runs on a domain member ▪ Collects IP address-to-username information ▪ Sends information to the firewall
Palo Alto Networks Terminal Services agent	▪ Runs on Microsoft and Citrix terminal servers ▪ Collects IP and port number-to-username information ▪ Sends information to firewall

User-ID technology has four main components. The table lists each component’s name and primary characteristics.

The User-ID agent comes in two forms: an integrated agent resident on the firewall or a Windows-based agent:

- The PAN-OS integrated agent is included with PAN-OS software.
- The Windows-based agent is available for download from Palo Alto Networks and can be installed on one or more Windows systems.
- A firewall can communicate with both agent types at the same time.
- Both agent types monitor up to 100 Domain Controllers or Exchange Servers.
- Both agent types can monitor users and Domain Controllers only from a single Active Directory, or AD, domain.
- The integrated agent is designed for small and midsize deployments such as small remote offices or lab environments.
- Multiple Windows-based agents can be deployed to handle larger environments or multiforest domains.



Integrated Agent Versus Windows-Based Agent

- An integrated agent uses network bandwidth more efficiently.
- For remote sites, use an integrated agent or install a Windows-based agent at the site.

Just IP to User

<< X MB

Full Security Log

X MB of data

Windows-Based Agent

Just Required IP-to-Username Information

0.05 * *n*MB of data

Integrated Agent

8 | © 2019 Palo Alto Networks, Inc.

Although the Windows-based agent and the PAN-OS integrated agent perform the same basic tasks, they use different underlying communication protocols. This difference makes each agent more appropriate for different environments.

The Windows-based agent uses MS-RPC, which requires the full Windows Security logs to be sent to the agent, where they are filtered for the relevant User-ID information.

The PAN-OS integrated agent uses either the Windows Management Instrumentation, or WMI, or the Windows Remote Management Protocol, or WinRM, which enables the agent to retrieve only the relevant User-ID information from the Windows security logs.

The result is that, in an infrastructure with remote networks separated by WAN links, the integrated agent is more appropriate for reading remote logs and the Windows-based agent is more appropriate for reading local logs. However, use of the integrated agent is not without cost: It consumes more of the firewall’s management plane resources. For this reason, deployment of the Windows agent at remote sites and having them forward the relevant User-ID information to a firewall on a central network often is beneficial.

User-ID overview

User mapping methods overview

Configuring User-ID

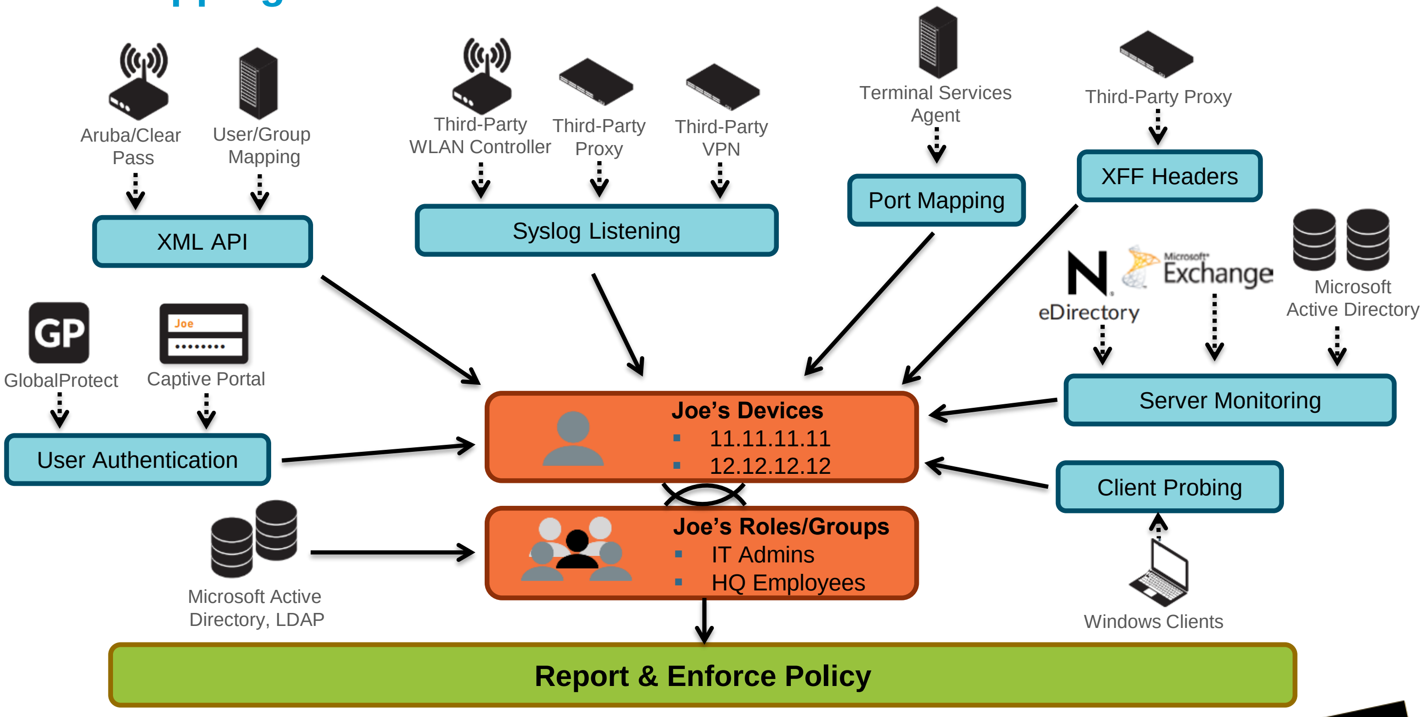
PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy

User Mapping Methods



Aruba/Clear Pass

User/Group Mapping

XML API

Third-Party WLAN Controller

Third-Party Proxy

Third-Party VPN

Syslog Listening

Terminal Services Agent

Port Mapping

Third-Party Proxy

XFF Headers

eDirectory

Microsoft Exchange

Microsoft Active Directory

Server Monitoring

GlobalProtect

Captive Portal

User Authentication

Joe's Devices

- 11.11.11.11
- 12.12.12.12

Joe's Roles/Groups

- IT Admins
- HQ Employees

Client Probing

Windows Clients

Microsoft Active Directory, LDAP

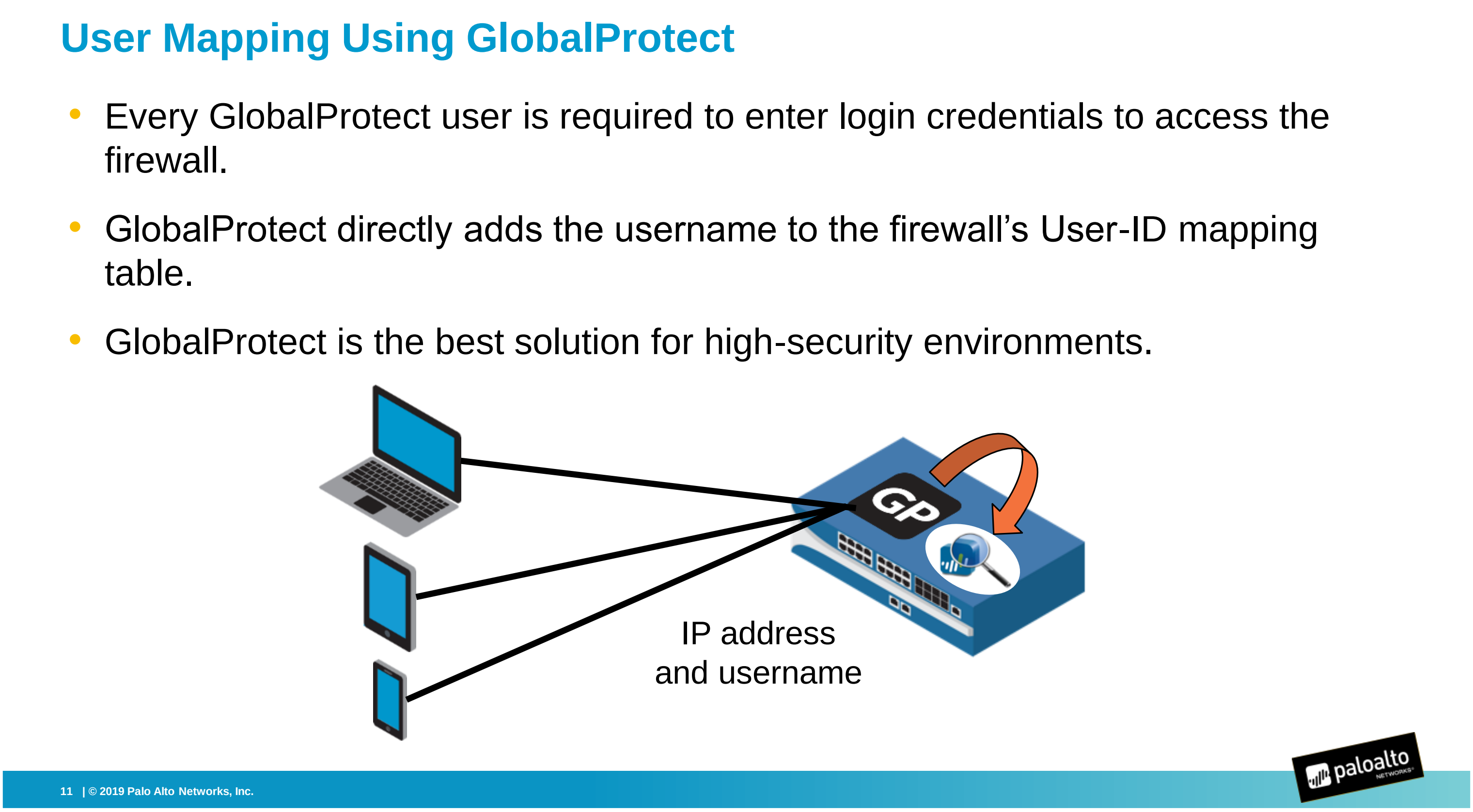
Report & Enforce Policy

10 | © 2019 Palo Alto Networks, Inc.

User-ID technology includes multiple methods to map IP addresses to users. The decision about which methods you employ depends on the operating systems, applications, and network infrastructure used in your organization. If any of the methods successfully maps an IP address to a user, the user's name can be used by the firewall for policy rule matches, logs, and reports.

The following list is a brief description of each method shown in the illustration:

- User-ID acquires username information from Captive Portal web forms and login events on GlobalProtect client machines.
- User-ID listens for syslog login and logout messages from network access control (NAC) systems, 802.1*x* devices, and wireless controllers.
- User-ID monitors Microsoft AD Domain Controllers, Microsoft Exchange Servers, or Novell eDirectory Servers for login or logout events recorded in Authentication logs. User-ID also reads session tables to confirm known IP address-to-username mappings based on current Windows file and printer shares.
- User-ID maps IP address and port number combinations to usernames for Microsoft Remote Desktop Services and Citrix Presentation Server or Citrix XenApp.
- User-ID probes Windows systems to verify current user mappings and to discover new IP address-to-username mappings.
- When other methods cannot be used, User-ID can consume PAN-OS XML API user login and logout messages sent from terminal servers, NAC systems, and other network devices that can format and send XML over HTTP.



User Mapping Using GlobalProtect

- Every GlobalProtect user is required to enter login credentials to access the firewall.
- GlobalProtect directly adds the username to the firewall’s User-ID mapping table.
- GlobalProtect is the best solution for high-security environments.

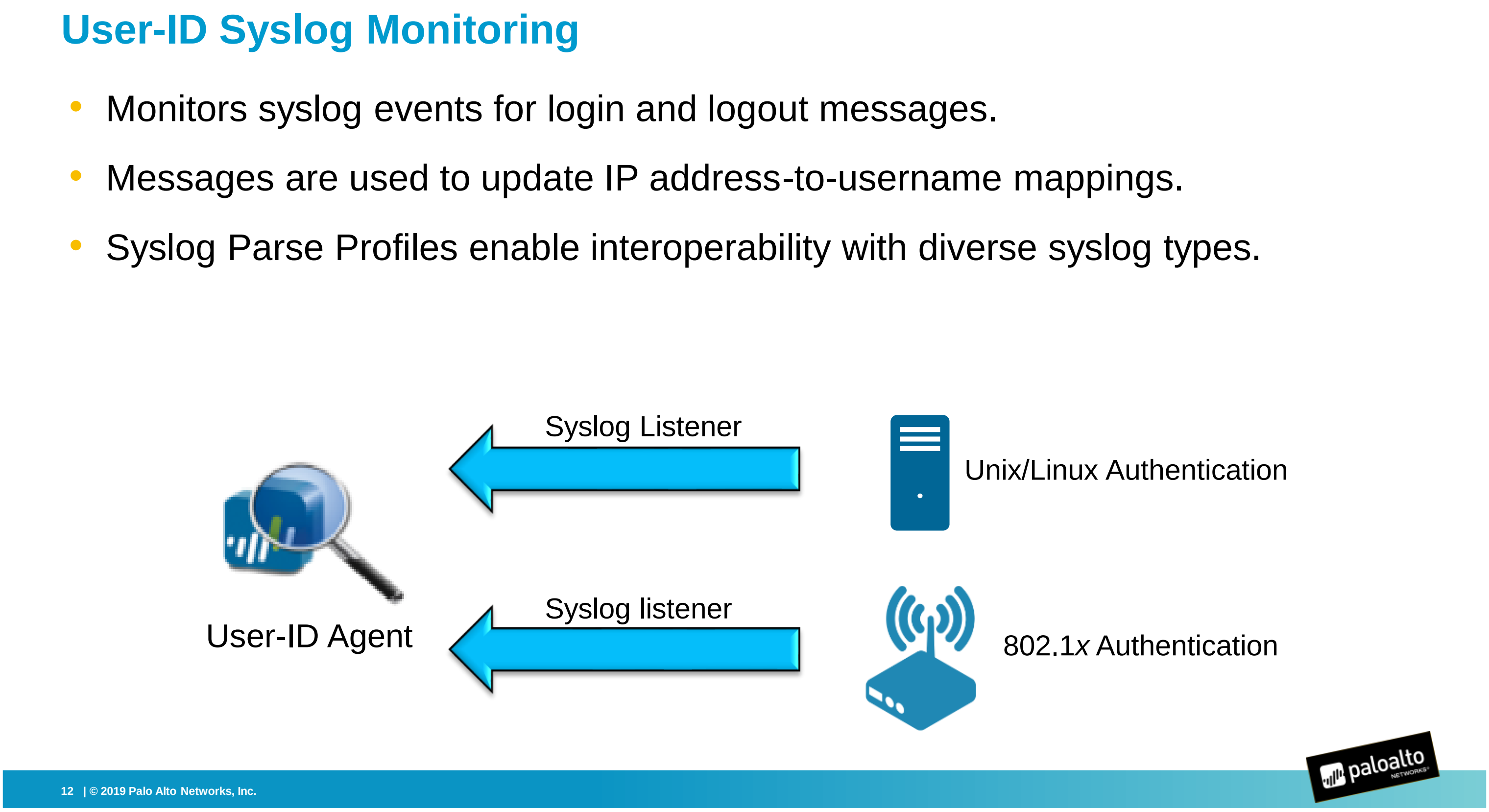
11 | © 2019 Palo Alto Networks, Inc.

For remote roaming users, the GlobalProtect client provides the user mapping information to the firewall directly. In this case, every GlobalProtect user has an agent or app running on the client that requires the user to enter login credentials for VPN access to the firewall. This login information then is added to the User-ID user mapping table on the firewall for visibility and user-based policy rule enforcement.

User-ID information also can be provided from clients that are connected to an internal network via an internal GlobalProtect gateway without establishing a VPN tunnel to a firewall. Every internal GlobalProtect user has an agent or app running on the internal client that requires the user to enter login credentials that can be used by the firewall.

Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. GlobalProtect is the best solution in sensitive environments where you must be certain of who a user is to allow access to an application or service.

For more information about configuring GlobalProtect, see the *GlobalProtect Administrator’s Guide* at https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin.html.

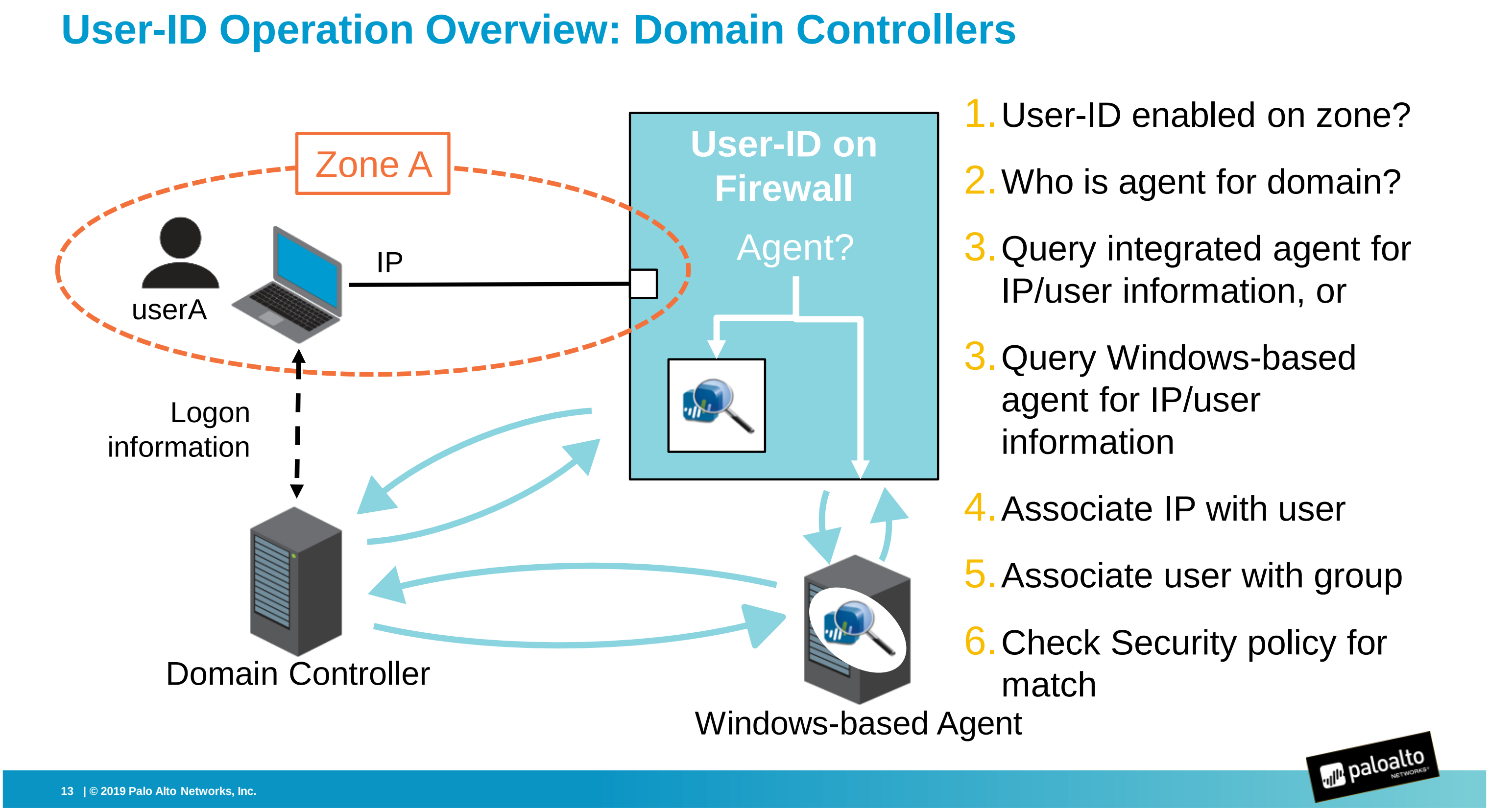


User-ID Syslog Monitoring

- Monitors syslog events for login and logout messages.
- Messages are used to update IP address-to-username mappings.
- Syslog Parse Profiles enable interoperability with diverse syslog types.

Your environment might have existing network services that authenticate users. These services include wireless controllers, 802.1*x* devices, Apple Open Directory servers, proxy servers, and other NAC mechanisms. You can configure these services to send syslog messages that contain information about login and logout events and configure the User-ID agent to parse those messages. Both the integrated and Windows-based agents can retrieve syslog messages. The User-ID agent can parse for login events to map IP addresses to usernames and parse for logout events so that the firewall deletes outdated mappings. Deletion of outdated mappings is particularly useful in environments where IP address assignments change often.

Both the PAN-OS integrated User-ID agent and Windows-based User-ID agent use Syslog Parse Profiles to parse syslog messages. In environments where services send the messages in different formats, you can create a custom profile for each format and associate multiple profiles with each sender. If you use the PAN-OS integrated User-ID agent, you also can use predefined Syslog Parse Profiles that Palo Alto Networks provides through Applications content updates.



User-ID Operation Overview: Domain Controllers

Zone A

userA

IP

User-ID on Firewall

Agent?

Logon information

Domain Controller

Windows-based Agent

1. User-ID enabled on zone?
2. Who is agent for domain?
3. Query integrated agent for IP/user information, or
3. Query Windows-based agent for IP/user information
4. Associate IP with user
5. Associate user with group
6. Check Security policy for match

The diagram and text provide an overview of the operation of User-ID technology in the scenario where userA logs in to their laptop. The laptop is an AD domain member, so userA's logon information is recorded on the AD Domain Controller. The logon information includes userA's username and IP address.

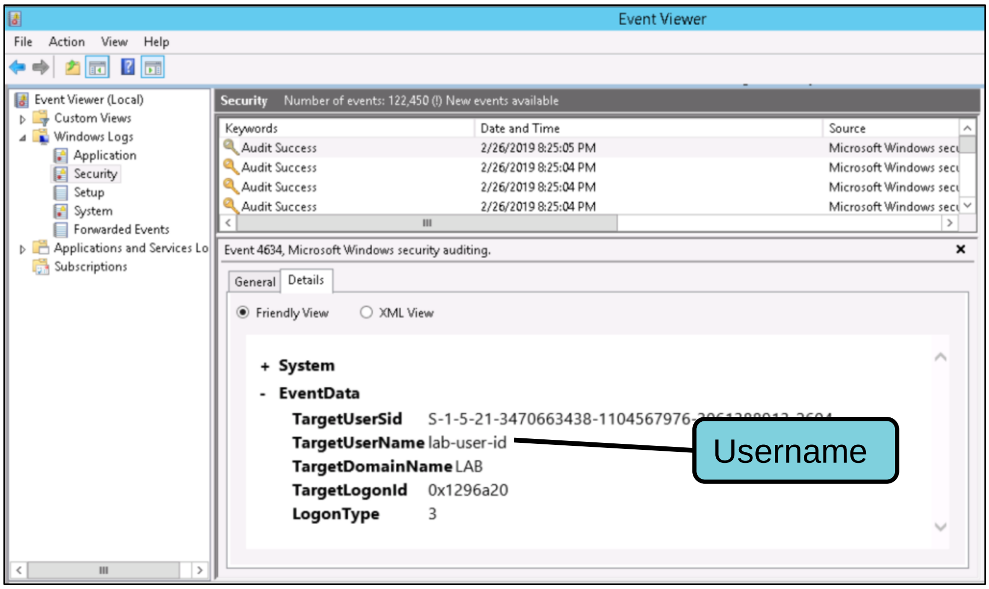
Before User-ID can operate, it must be enabled on the security zone. If User-ID is enabled, then the firewall consults the administrator-defined User-ID configuration to determine which agents the firewall has available to gather IP address and username information. Depending on the configuration, User-ID on the firewall could query either an integrated agent or a Windows-based agent. The agent retrieves IP address and username information from the Domain Controller.

After User-ID has retrieved the IP address and username information from an agent, it can use the firewall's LDAP configuration to retrieve user-to-group mapping information from an LDAP server.

At this point, User-ID will have an IP address associated with a username and possibly a username associated with one or more group names. If traffic arrives from the IP address associated with userA, the firewall can use the User-ID information to check its Security policy rules for a match and determine how to handle traffic from userA.

User-ID Domain Controller Monitoring

- Monitors Security logs of Domain Controllers
- Monitors all Domain Controllers per domain to get all logon and logout events



Security Number of events: 122,450 (!) New events available

Keywords	Date and Time	Source
Audit Success	2/26/2019 8:25:05 PM	Microsoft Windows secu
Audit Success	2/26/2019 8:25:04 PM	Microsoft Windows secu
Audit Success	2/26/2019 8:25:04 PM	Microsoft Windows secu
Audit Success	2/26/2019 8:25:04 PM	Microsoft Windows secu

Event 4634, Microsoft Windows security auditing.

● Friendly View

```
+ System
- EventData
    TargetUserSid        S-1-5-21-3470663438-1104567976-
    TargetUserName       lab-user-id
    TargetDomainName     LAB
    TargetLogonId        0x1296a20
    LogonType            3
```

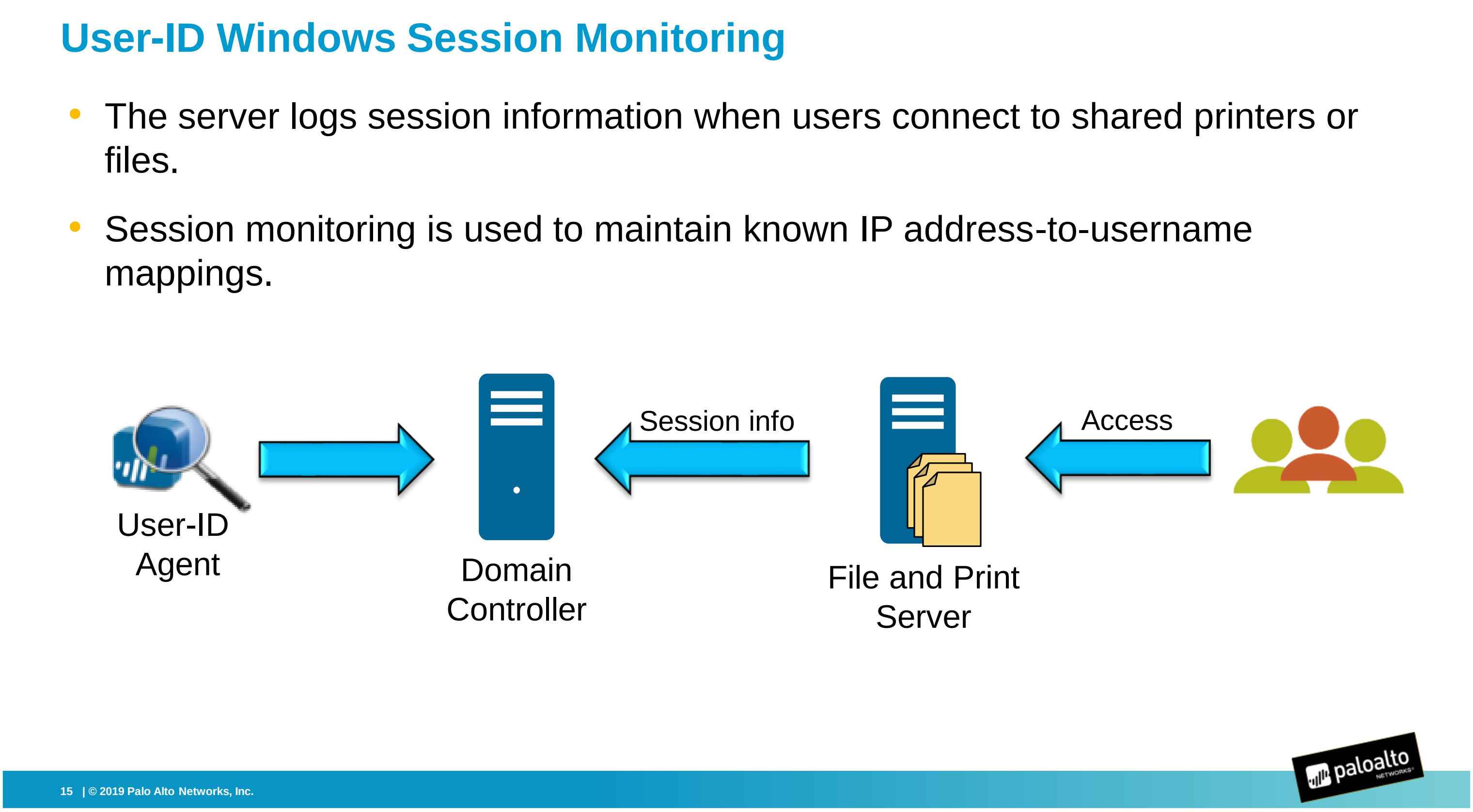
With passive server monitoring, a User-ID agent—either a Windows-based agent or the integrated User-ID agent—monitors the Security logs for user logon or logout events for the specified Microsoft Domain Controllers:

- When the User-ID agent first starts up, it will parse the security event logs and record all of the user logon events.
- Afterward, it will check the Security logs on a regular basis for only new logon or logout events.
- User mappings are cached for an amount of time equal to the timeout value set in the User-ID agent interface.

Note that, for security events to be recorded in the Security logs, the AD domain must be configured to log successful account logon events.

Because users can authenticate to any Domain Controller in a domain and the Security logs are not replicated between Domain Controllers, you also must set up server monitoring for all Domain Controllers to capture all user logon events. Each User-ID agent can monitor multiple Domain Controllers per domain. However, each User-ID agent can monitor only a single domain.

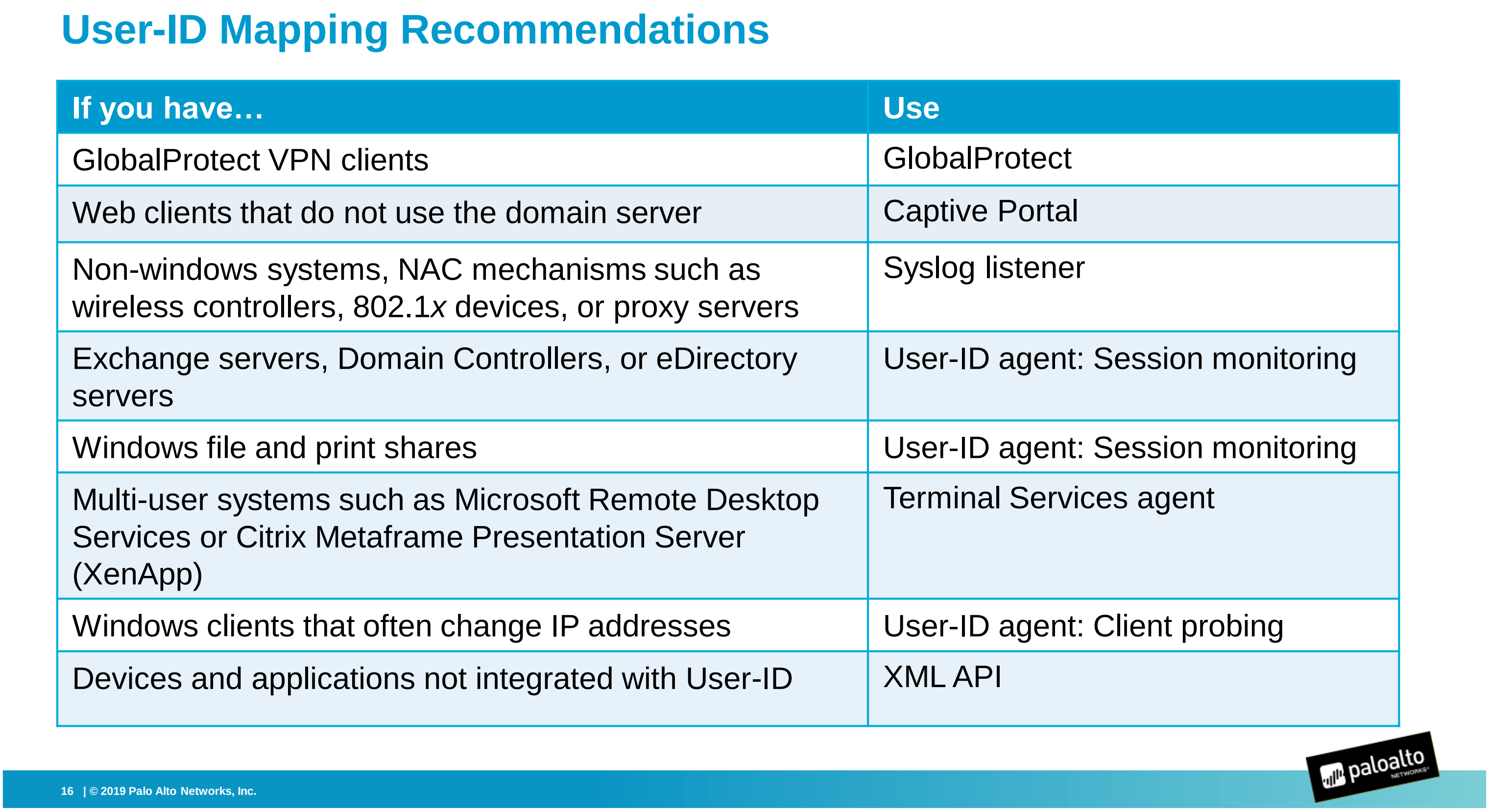
Because server monitoring requires very little overhead and because the majority of users generally can be mapped using this method, Palo Alto Networks recommends it as the base user mapping method for most User-ID deployments.



User-ID Windows Session Monitoring

- The server logs session information when users connect to shared printers or files.
- Session monitoring is used to maintain known IP address-to-username mappings.

Clients who have connected to a shared file or print resource will have their session information stored on the Domain Controller. An additional Windows-based method to resolve IP addresses to users is to consult the shared resource session table recorded on the Domain Controller.



User-ID Mapping Recommendations

If you have…	Use
GlobalProtect VPN clients	GlobalProtect
Web clients that do not use the domain server	Captive Portal
Non-windows systems, NAC mechanisms such as wireless controllers, 802.1*x* devices, or proxy servers	Syslog listener
Exchange servers, Domain Controllers, or eDirectory servers	User-ID agent: Session monitoring
Windows file and print shares	User-ID agent: Session monitoring
Multi-user systems such as Microsoft Remote Desktop Services or Citrix Metaframe Presentation Server (XenApp)	Terminal Services agent
Windows clients that often change IP addresses	User-ID agent: Client probing
Devices and applications not integrated with User-ID	XML API

16 | © 2019 Palo Alto Networks, Inc.

The table shows the circumstances under which different User-ID components and mapping methods are recommended by Palo Alto Networks.

User-ID overview

User mapping methods overview

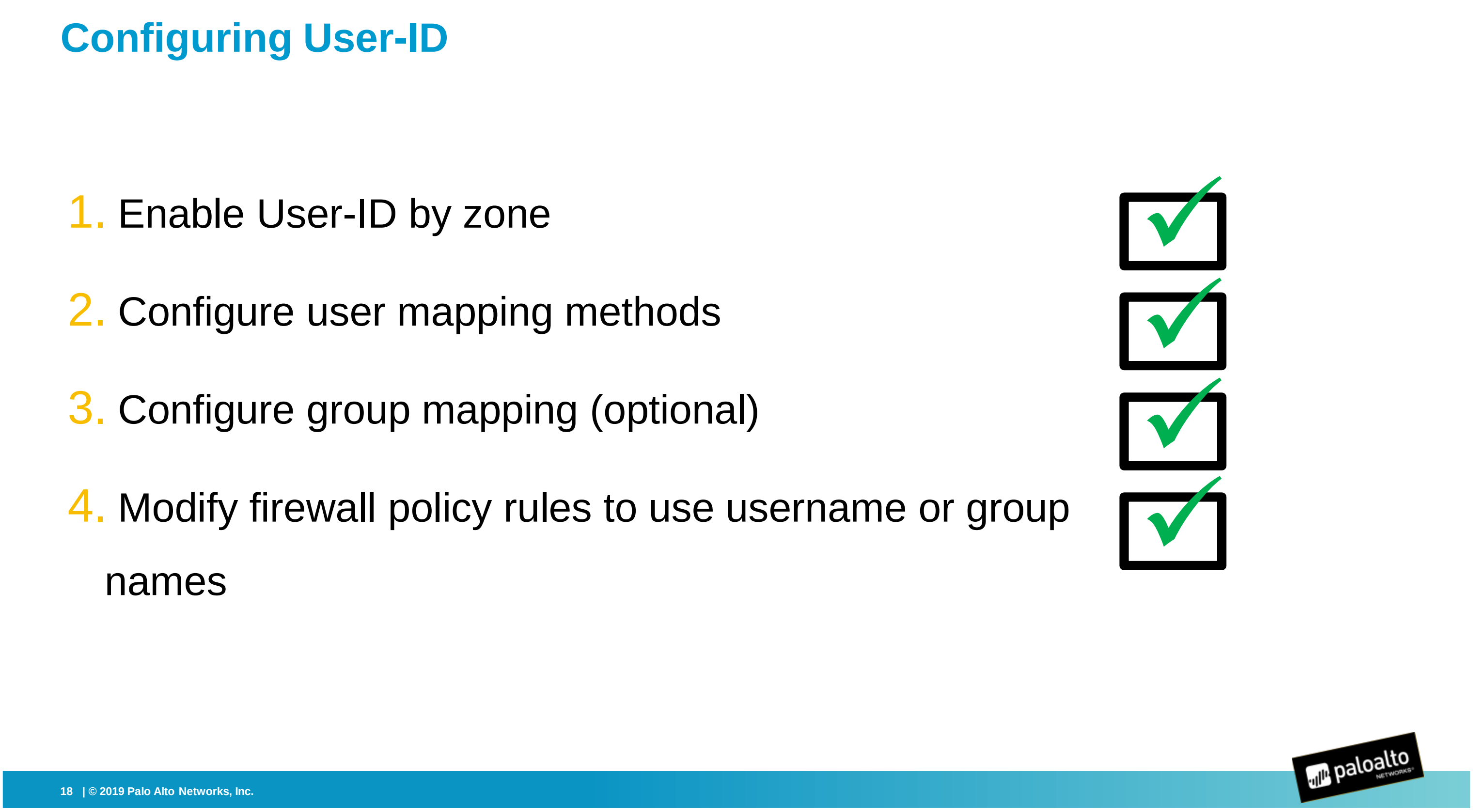
Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy



Configuring User-ID

1. Enable User-ID by zone ☑
2. Configure user mapping methods ☑
3. Configure group mapping (optional) ☑
4. Modify firewall policy rules to use username or group names ☑

18 | © 2019 Palo Alto Networks, Inc.

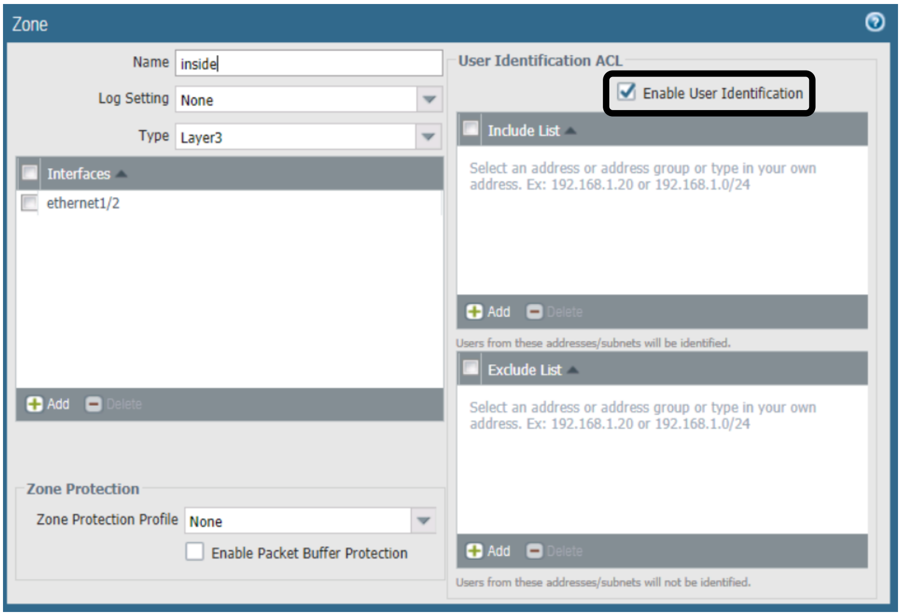
The list shows the four general steps to configure User-ID technology. The specific steps to configure group mapping, and particularly user mapping, depend on your environment.

Definition of policy rules based on group names rather than on individual usernames simplifies firewall administration because you do not have to update the rules or perform a commit whenever users are added to, or removed from, a group.

Enabling User-ID Per Zone

- Enable User-ID by the source zone where user traffic originates
- Enable User-ID only for internal zones
- By default all subnetworks in the source zone are mapped:
  - Modify using Include Lists or Exclude Lists

Network > Zones > <select_zone>



Zone

Name: inside

Log Setting: None

Type: Layer3

□ Interfaces

□ ethernet1/2

Add Delete

Zone Protection

Zone Protection Profile: None

□ Enable Packet Buffer Protection

User Identification ACL

☑ Enable User Identification

□ Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will be identified.

□ Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Add Delete

Users from these addresses/subnets will not be identified.

Enable User-ID technology per zone on the firewall. For each zone you must click the **Enable User Identification** check box to activate User-ID on the zone. User-ID tracks only users associated with the source zone of a session. Never enable User-ID for a zone that contains the internet, or your firewall will attempt to identify every user from outside your network.

By default User-ID will try to map users from all subnetworks found within a User-ID-enabled zone. Use the **Include List** to limit the subnetworks or specific addresses that the firewall will attempt to map to users. Use the **Exclude List** only to exclude user mapping information for a subset of the subnetworks you added to the **Include List**.

If WMI probing is enabled, WMI will probe private IP addresses, but not probe public IP addresses by default. Private addresses are those found in the IP addresses ranges 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. To enable WMI probing to map public addresses, you must use the addresses or address ranges in the **Include List**.

User-ID overview

User mapping methods overview

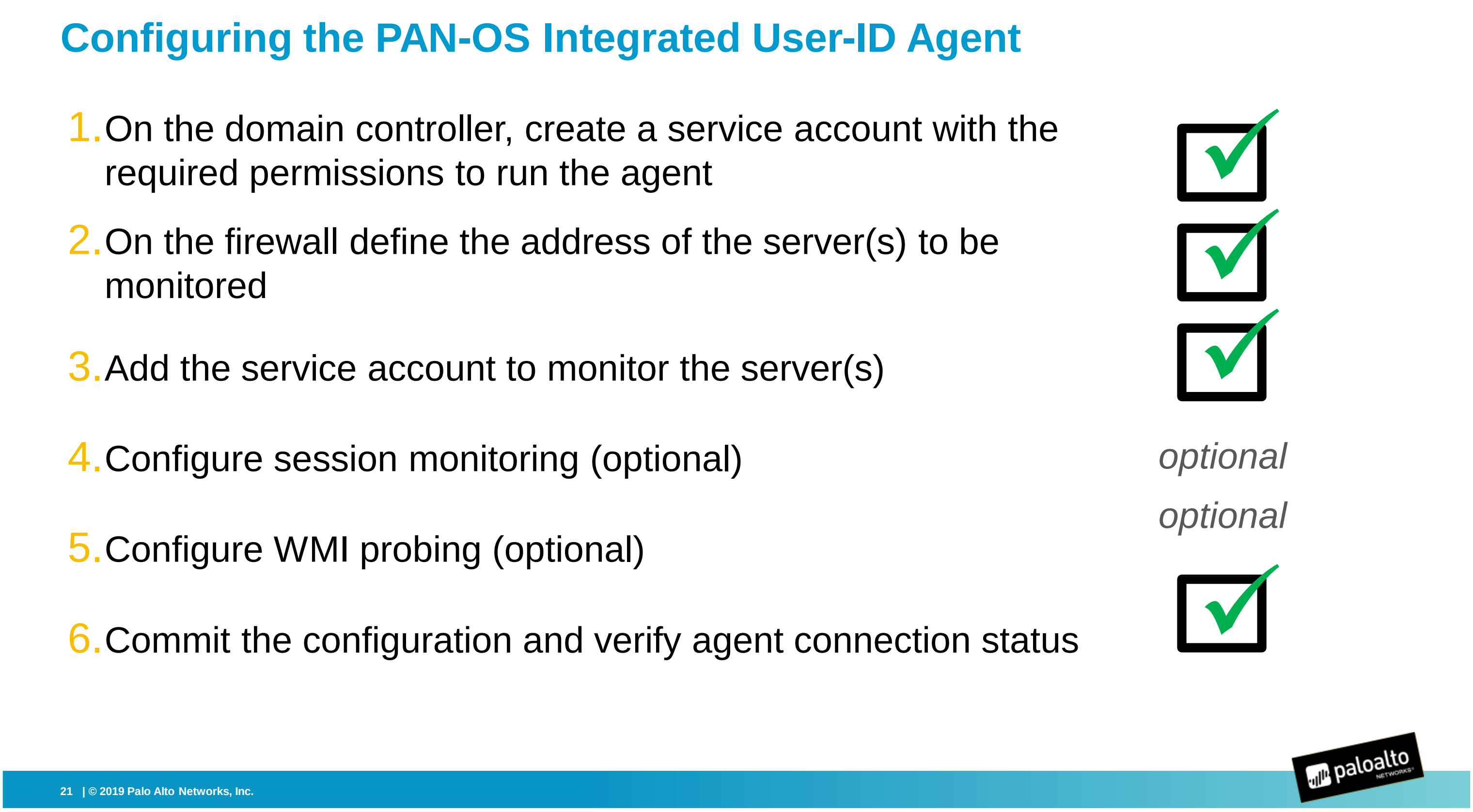
Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy



Configuring the PAN-OS Integrated User-ID Agent

1. On the domain controller, create a service account with the required permissions to run the agent ☑
2. On the firewall define the address of the server(s) to be monitored ☑
3. Add the service account to monitor the server(s) ☑
4. Configure session monitoring (optional) *optional*
5. Configure WMI probing (optional) *optional*
6. Commit the configuration and verify agent connection status ☑

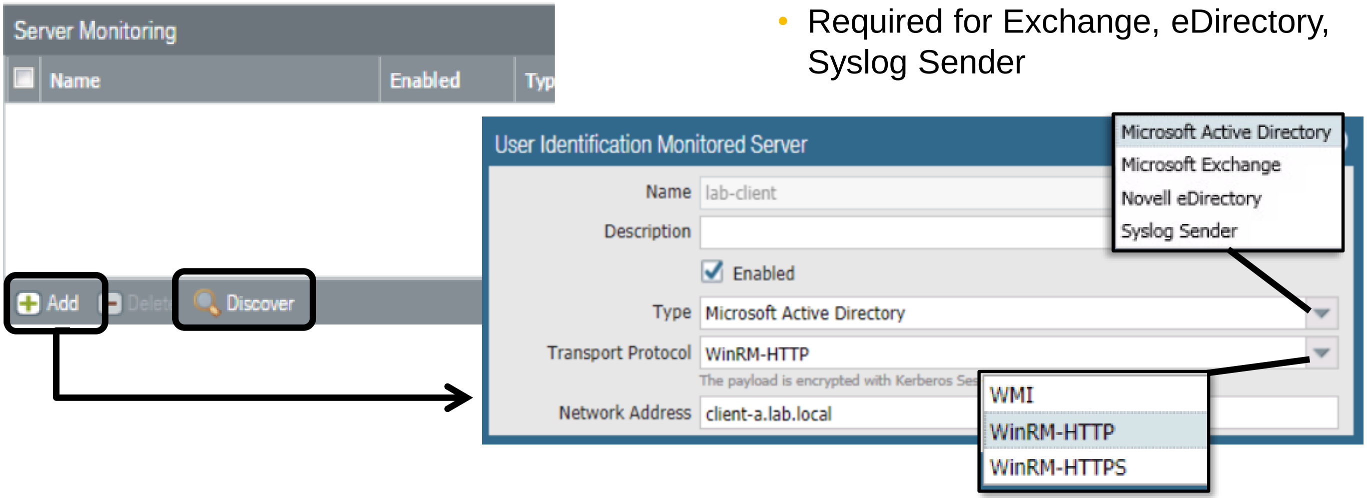
21 | © 2019 Palo Alto Networks, Inc.

The list shows the main steps used to configure a PAN-OS integrated User-ID agent to connect to monitored servers.

Defining the Monitored Server(s)

- Use **Discover** for domain controllers
- Use **Add** to manually add servers:
  - Required for Exchange, eDirectory, Syslog Sender

Device > User Identification > User Mapping



User Identification Monitored Server

Name: lab-client

Description:

☑ Enabled

Type: Microsoft Active Directory

Transport Protocol: WinRM-HTTP

The payload is encrypted with Kerberos Ses

Network Address: client-a.lab.local

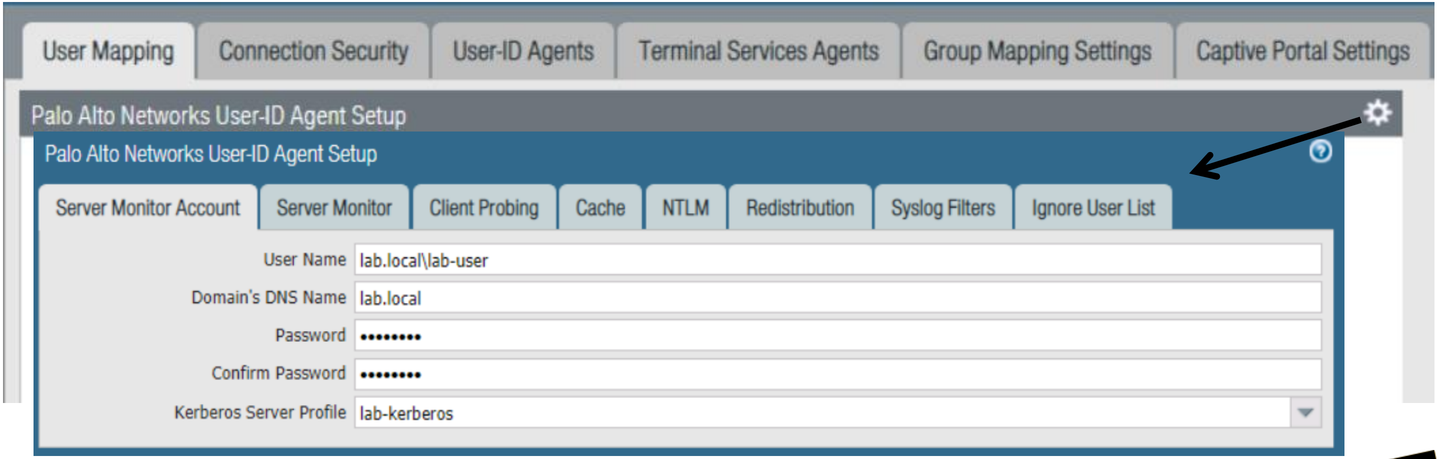
Each User-ID agent must be configured for the servers it needs to monitor. The agent includes an autodiscovery feature that automatically identifies available Microsoft Windows Servers via DNS for event log monitoring. With the release of PAN-OS 9.0, the integrated agent supports WMI and WinRM protocols to map IP addresses to usernames.

The firewall will discover domain controllers based on the domain name entered in the **Domain** field of the **Device** > **Setup** > **Management** > **General Settings** page.

Defining the User-ID Agent Account

- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

Device > User Identification > User Mapping



Palo Alto Networks User-ID Agent Setup

User Name: lab.local\lab-user

Domain's DNS Name: lab.local

Password: ••••••••

Confirm Password: ••••••••

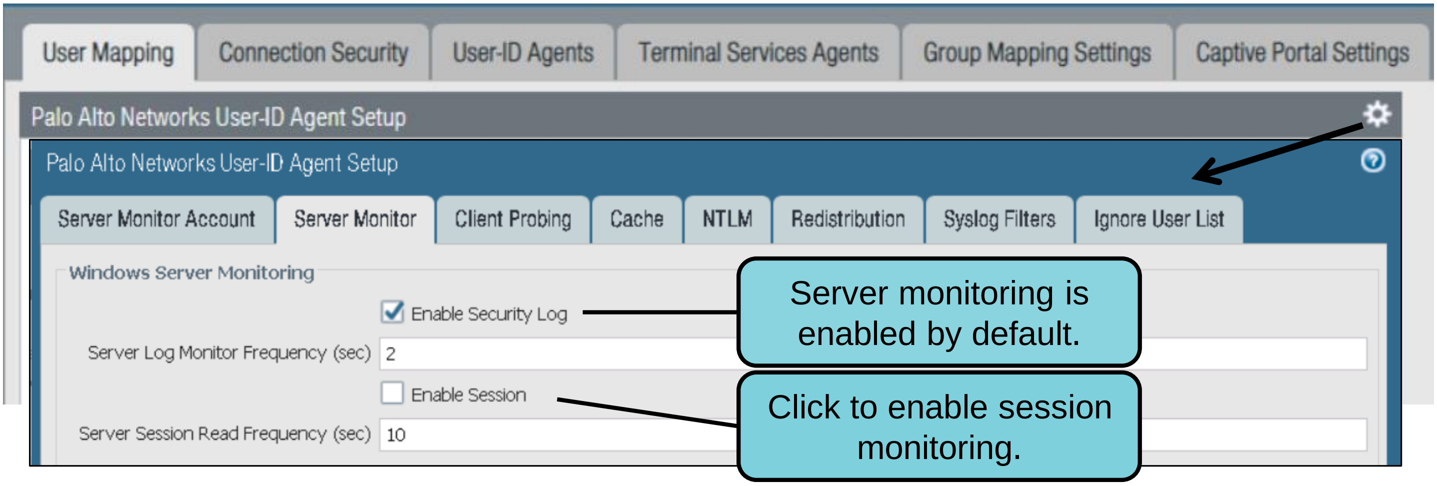
Kerberos Server Profile: lab-kerberos

Set the domain credentials for the account the firewall will use to access Windows resources. This setting is required for monitoring domain controllers and Exchange Servers. The information in the **User Name** field must be entered using the format domain\username.

No special permissions configuration is necessary if the integrated agent runs as an account that belongs to the Domain Administrators group or belongs to the Server Operators and Event Log Readers groups. However, membership in these groups provides the account with more permissions than just the capability to perform server monitoring or client probing. Therefore, you might want to run the agent using a restricted account with minimal permissions. To create a Windows account with minimal permissions, see the permissions configuration instructions in the *PAN-OS Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin.html. The steps to configure an account with minimal Windows permissions depend on the Windows operating system version you have.

Optional Session Monitoring

Device > User Identification > User Mapping



☑ Enable Security Log

Server Log Monitor Frequency (sec) 2

□ Enable Session

Server Session Read Frequency (sec) 10

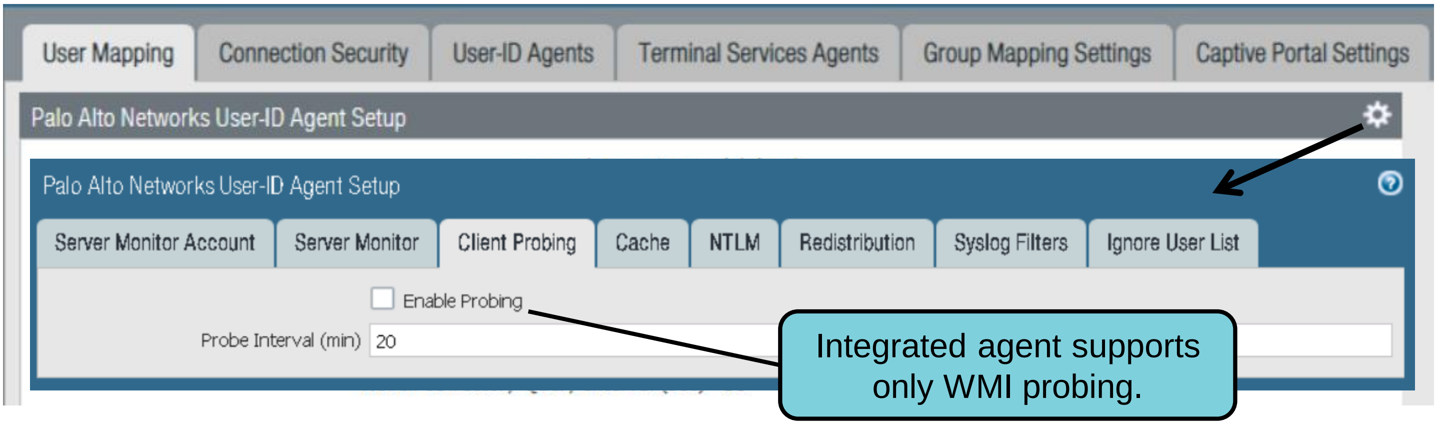
Server monitoring is enabled by default.

Click to enable session monitoring.

To enable session monitoring, select the **Enable Session** check box. This setting enables the integrated agent to use current file and print sharing information to verify current IP address-to-username mappings.

Optional WMI Client Probing

Device > User Identification > User Mapping



User Mapping | Connection Security | User-ID Agents | Terminal Services Agents | Group Mapping Settings | Captive Portal Settings

Palo Alto Networks User-ID Agent Setup

Palo Alto Networks User-ID Agent Setup

Server Monitor Account | Server Monitor | Client Probing | Cache | NTLM | Redistribution | Syslog Filters | Ignore User List

□ Enable Probing

Probe Interval (min) 20

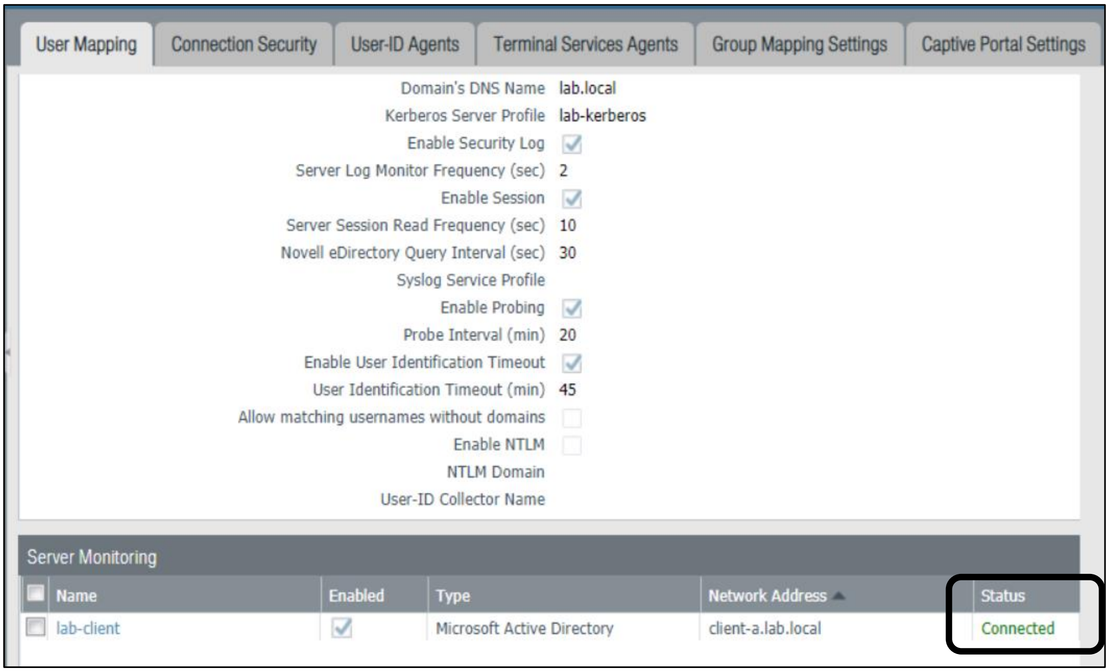
Integrated agent supports only WMI probing.

You can enable the integrated agent to perform WMI probing for each client system that the user mapping process identifies. The integrated agent periodically probes each learned IP address to verify that the same user still is logged in. When a firewall encounters an IP address for which it has no user mapping, it sends the address to the integrated agent for an immediate probe.

Client probing was designed for legacy networks where most users were on Windows workstations on the internal network, but is not ideal for current networks that support a roaming and mobile user base on a variety of devices and operating systems.

Verifying Connection Status

Device > User Identification



Domain's DNS Name	lab.local
Kerberos Server Profile	lab-kerberos
Enable Security Log	☑
Server Log Monitor Frequency (sec)	2
Enable Session	☑
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30
Syslog Service Profile	
Enable Probing	☑
Probe Interval (min)	20
Enable User Identification Timeout	☑
User Identification Timeout (min)	45
Allow matching usernames without domains	☐
Enable NTLM	☐
NTLM Domain	
User-ID Collector Name	

Server Monitoring

☐	Name	Enabled	Type	Network Address	Status
☐	lab-client	☑	Microsoft Active Directory	client-a.lab.local	Connected

After you commit your configuration changes, the status of each of your monitored servers should display as **Connected**.

User-ID overview

User mapping methods overview

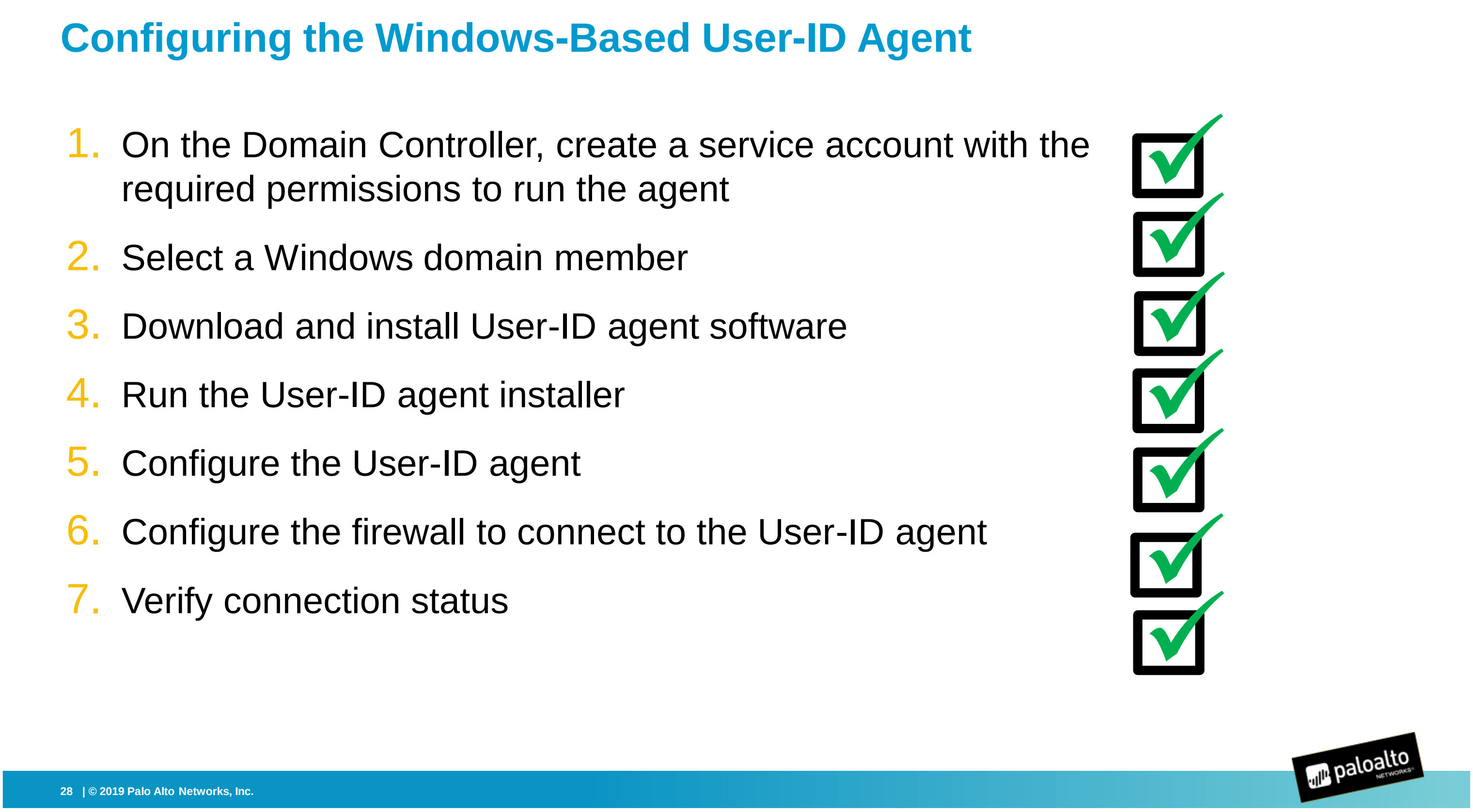
Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

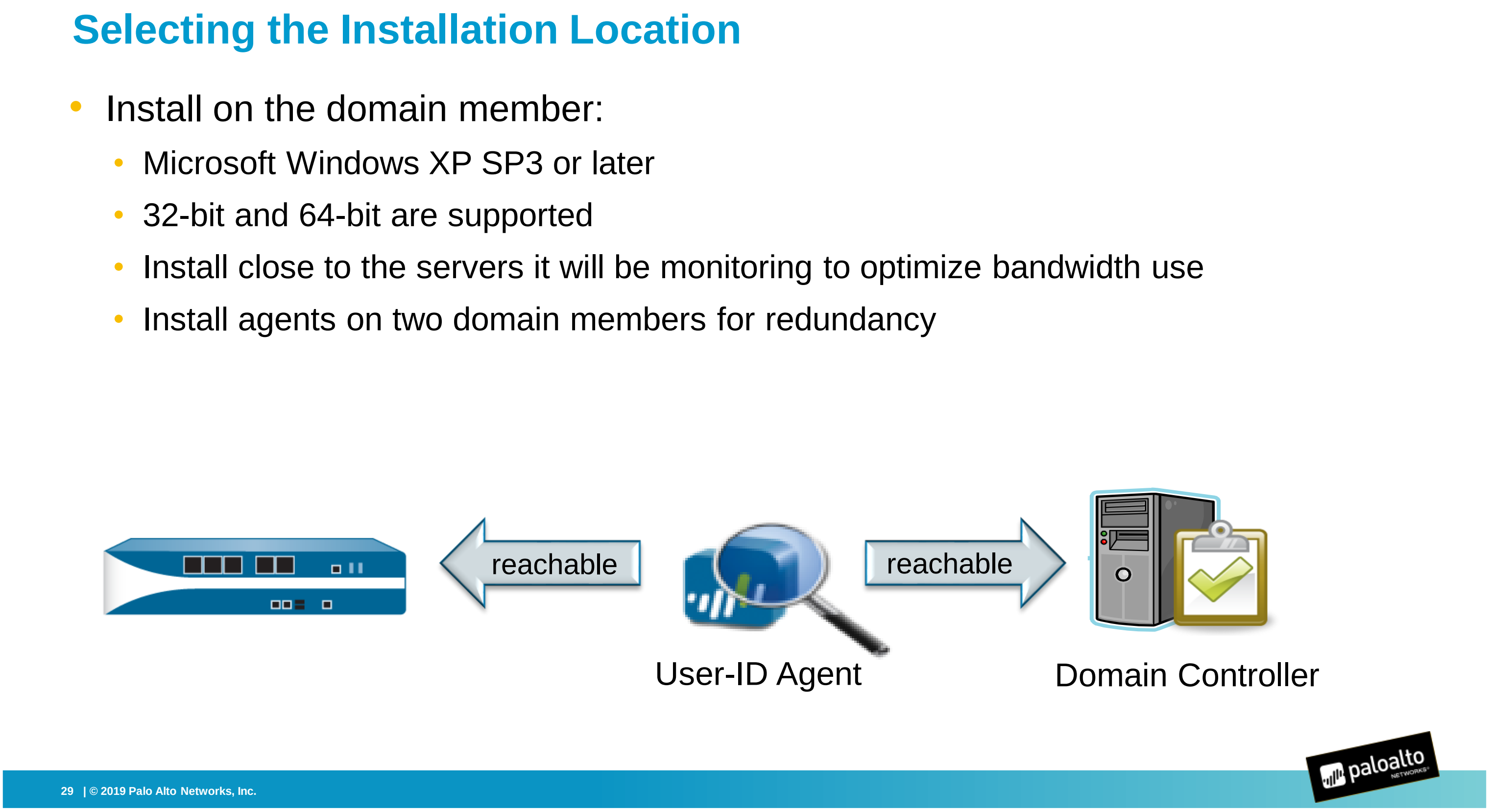
User-ID and security policy



Configuring the Windows-Based User-ID Agent

1. On the Domain Controller, create a service account with the required permissions to run the agent ☑
2. Select a Windows domain member ☑
3. Download and install User-ID agent software ☑
4. Run the User-ID agent installer ☑
5. Configure the User-ID agent ☑
6. Configure the firewall to connect to the User-ID agent ☑
7. Verify connection status ☑

The list shows the main steps used to configure a Windows-based agent to connect to monitored servers.



Selecting the Installation Location

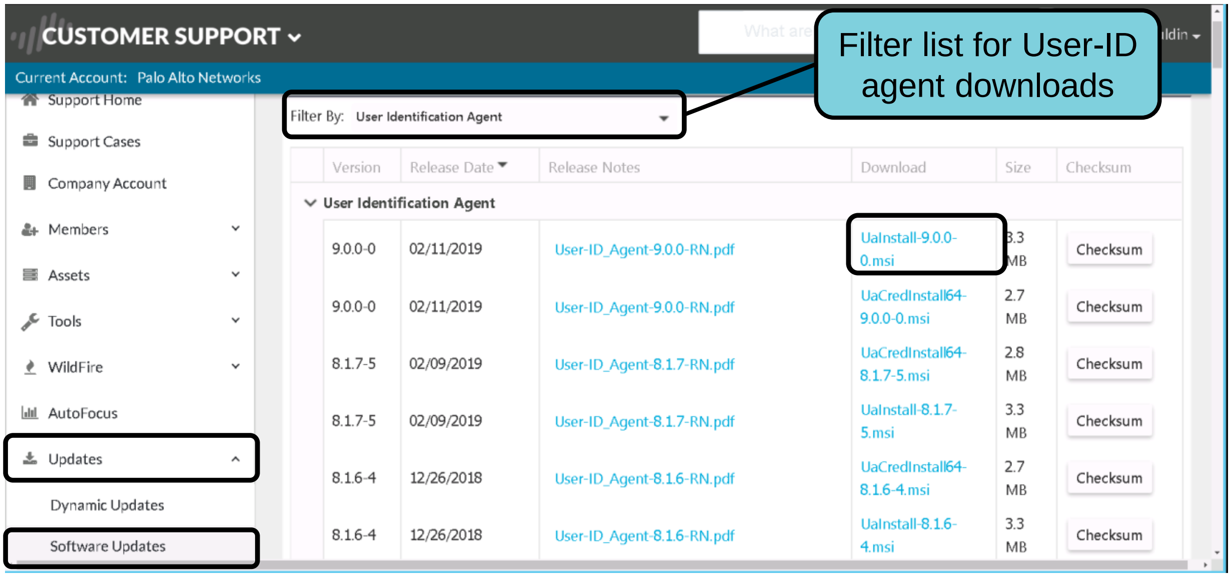
- Install on the domain member:
  - Microsoft Windows XP SP3 or later
  - 32-bit and 64-bit are supported
  - Install close to the servers it will be monitoring to optimize bandwidth use
  - Install agents on two domain members for redundancy

The Windows-based agent can be installed on 32-bit or 64-bit machines running Windows XP SP3 or later. You should install the agent in the same network site as the monitored server to optimize bandwidth use. You should install two agents on two member servers for redundancy in case one agent or one Domain Controller fails.

Note: Although an agent could be installed directly on a Domain Controller, it is not a best practice.

Download User-ID Agent Software

- Download the Windows agent from https://support.paloaltonetworks.com
- Install the agent



Filter By: User Identification Agent

Version	Release Date	Release Notes	Download	Size	Checksum
User Identification Agent					
9.0.0-0	02/11/2019	User-ID_Agent-9.0.0-RN.pdf	UaInstall-9.0.0-0.msi	3.3 MB	Checksum
9.0.0-0	02/11/2019	User-ID_Agent-9.0.0-RN.pdf	UaCredInstall64-9.0.0-0.msi	2.7 MB	Checksum
8.1.7-5	02/09/2019	User-ID_Agent-8.1.7-RN.pdf	UaCredInstall64-8.1.7-5.msi	2.8 MB	Checksum
8.1.7-5	02/09/2019	User-ID_Agent-8.1.7-RN.pdf	UaInstall-8.1.7-5.msi	3.3 MB	Checksum
8.1.6-4	12/26/2018	User-ID_Agent-8.1.6-RN.pdf	UaCredInstall64-8.1.6-4.msi	2.7 MB	Checksum
8.1.6-4	12/26/2018	User-ID_Agent-8.1.6-RN.pdf	UaInstall-8.1.6-4.msi	3.3 MB	Checksum

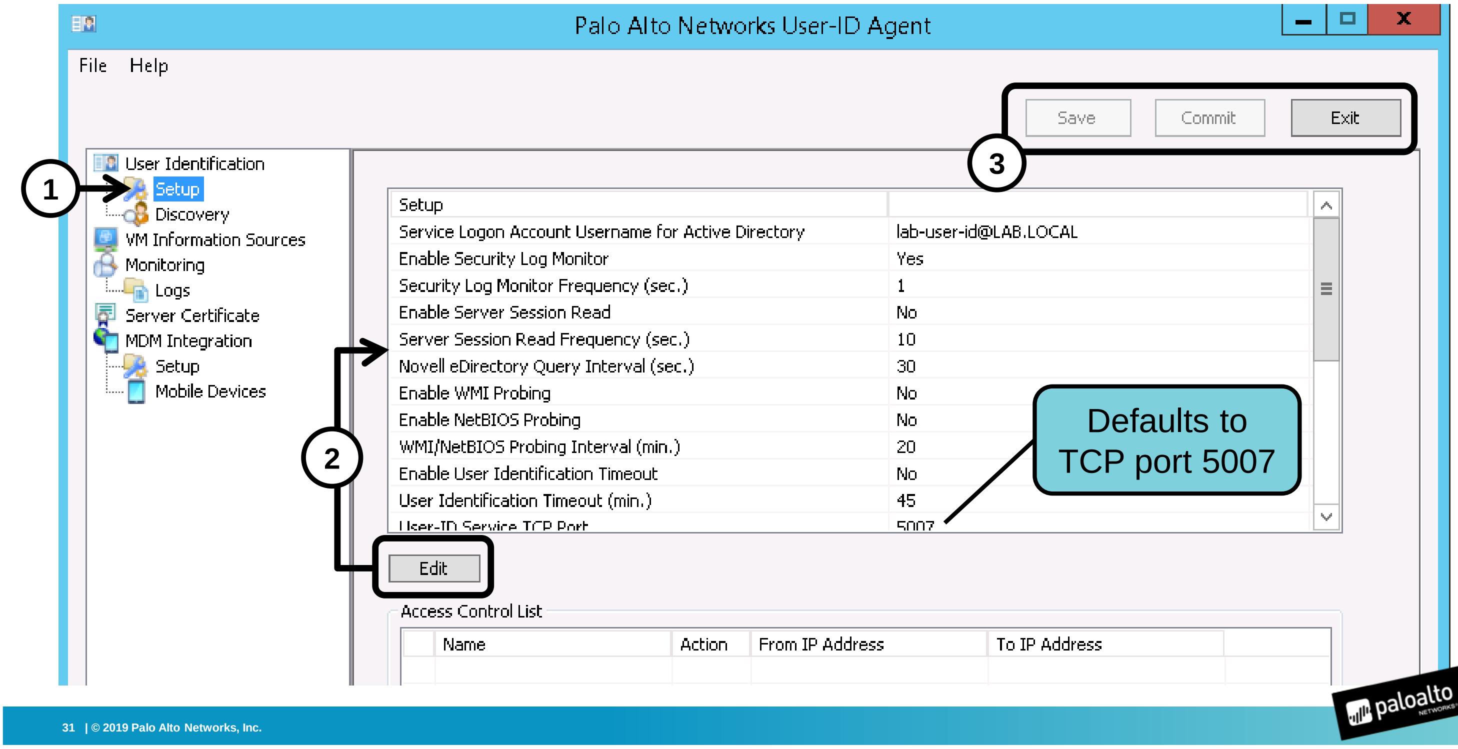
Use your Palo Alto Networks support account to log in to the support website. When you are logged in, click the **Updates** > **Software Updates** link to open the page shown here. To simplify finding the User-ID agent download links, use the **Filter By** menu to filter the list for **User Identification Agent**. Then find and download the User-ID agent version that matches your PAN-OS version.

Also download the **Release Notes** document because it contains important information about supported hardware configurations and software versions.

There are two choices for installing the agent software:

- You could install each agent individually by manually launching the downloaded MSI file.
- Beginning with PAN-OS 8.0, you can use endpoint management software such as Microsoft System Center Configuration Manager (SCCM) to remotely install, configure, or upgrade multiple agents in a single operation.

Agent Setup Process



Setup	
Service Logon Account Username for Active Directory	lab-user-id@LAB.LOCAL
Enable Security Log Monitor	Yes
Security Log Monitor Frequency (sec.)	1
Enable Server Session Read	No
Server Session Read Frequency (sec.)	10
Novell eDirectory Query Interval (sec.)	30
Enable WMI Probing	No
Enable NetBIOS Probing	No
WMI/NetBIOS Probing Interval (min.)	20
Enable User Identification Timeout	No
User Identification Timeout (min.)	45
User-ID Service TCP Port	5007

Access Control List

	Name	Action	From IP Address	To IP Address

Defaults to TCP port 5007

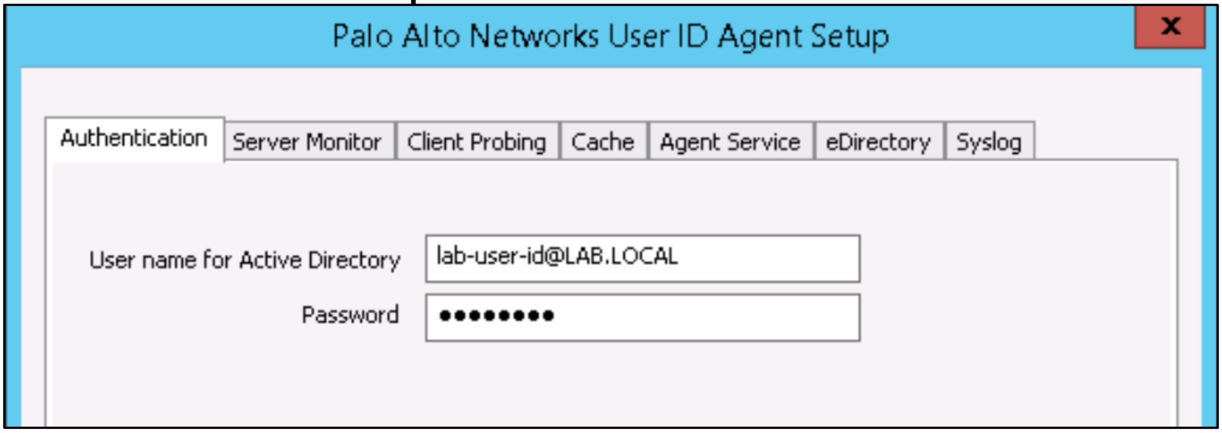
Open the User-ID Agent window after the agent software has been installed. First, click **Setup** in the left-side pane to configure the User-ID agent. Second, click the **Edit** button to open a separate tabbed window that enables you to change any of the settings shown in the **Setup** pane. Third, click **Save** to save your configuration changes but not to activate them. Click **Commit** to save and activate your configuration changes. Click **Exit** to close the window without saving your changes.

By default the User-ID agent uses TCP port 5007 to communicate to the firewall. You can change to another port, if necessary, by clicking **Edit** and then clicking the **Agent Service** tab in the window that opens.

Configuring the User-ID Agent Account

- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

User Identification > Setup > Edit



User name for Active Directory: lab-user-id@LAB.LOCAL

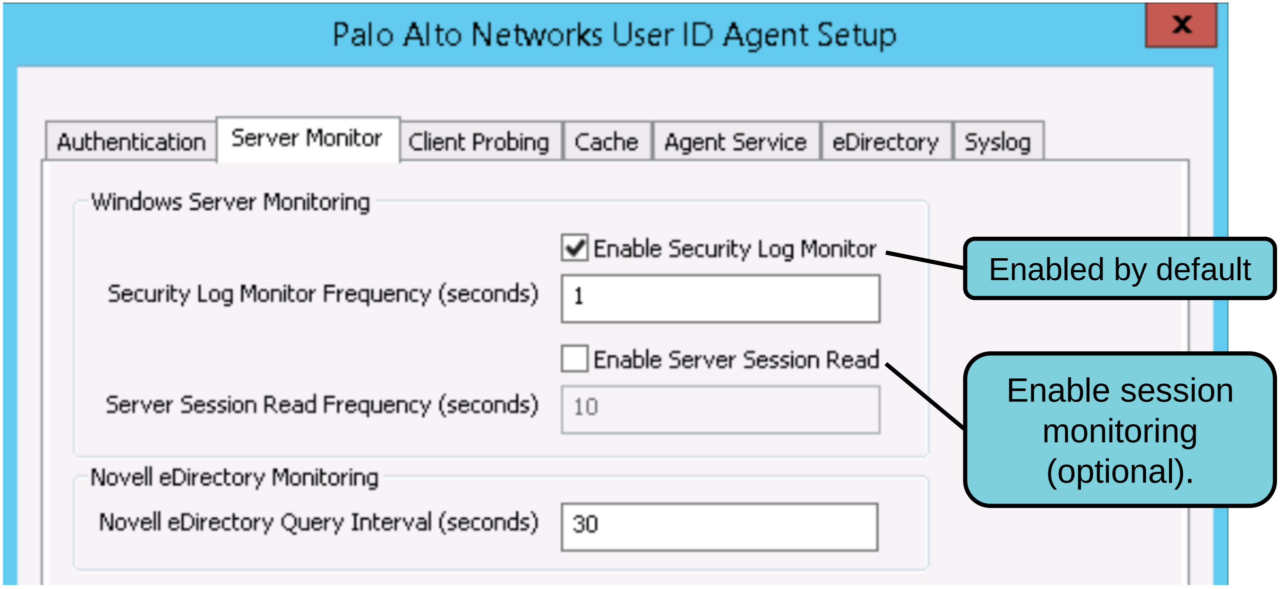
Password: ●●●●●●●●●

The agent should run with a Windows service account that has the necessary permissions to read the security event logs or to perform WMI probing. Use the **Authentication** tab to configure the agent to use a specific Windows service account. The authentication information must be configured before you can configure access to monitored servers.

By default, the Windows agent runs as the user account used to install the .msi file. Most of the necessary permissions are provided if the Windows-based agent runs as an account that belongs to the Domain Administrators group or belongs to the Server Operators and Event Log Readers groups. The user account running the agent also must have permissions to start a Windows service. However, membership in these groups provides the account with more permissions than just the capability to perform server monitoring or client probing. Therefore, you might want to run the agent using a restricted account with minimal permissions. To create a Windows account with minimal permissions, see the permissions configuration instructions in the *PAN-OS Administrator's Guide* at http://www.paloaltonetworks.com/documentation. The steps to configure an account with minimal Windows permissions depend on the Windows operating system version you have.

Configuring Server Monitoring

User Identification > Setup > Edit



Windows Server Monitoring

☑ Enable Security Log Monitor

Security Log Monitor Frequency (seconds): 1

□ Enable Server Session Read

Server Session Read Frequency (seconds): 10

Novell eDirectory Monitoring

Novell eDirectory Query Interval (seconds): 30

Enabled by default

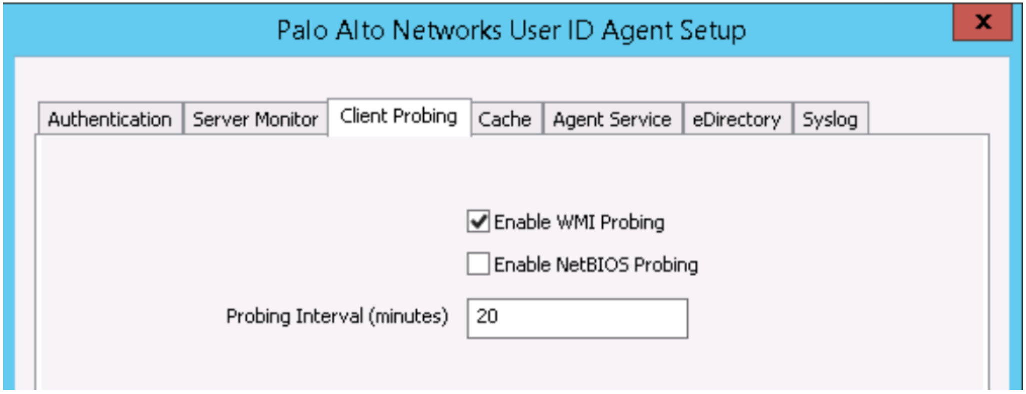
Enable session monitoring (optional).

Use the **Server Monitor** tab to configure server monitoring or to enable the optional session monitoring.

Configuring Client Probing

- Optional NetBIOS client probing requires:
  - Access through Windows firewall to port 139
  - File and print services enabled
- NetBIOS does not require Windows authentication.

User Identification > Setup > Edit



☑ Enable WMI Probing

□ Enable NetBIOS Probing

Probing Interval (minutes) 20

Use the Client Probing tab to configure the agent to probe IP addresses for username information.

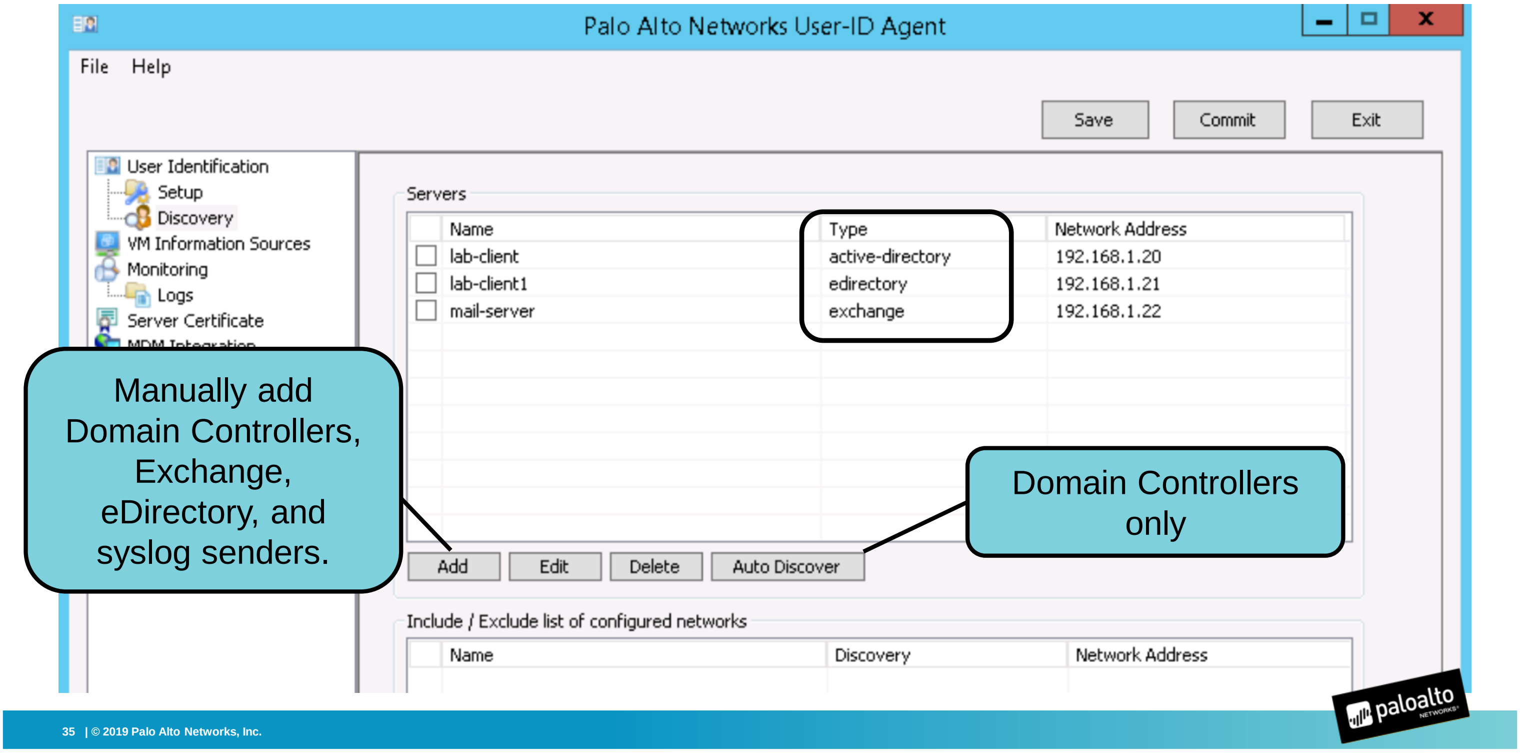
Unlike server monitoring, probing is an active method:

- The User-ID agent sends a probe at a configurable interval to each learned IP address in its list to verify that the same user is still logged in.
- The results of the probes are used to update the records on the agent, which are passed on to the firewall.
- Each learned IP is probed once per interval period.
- WMI probing must be enabled on the Windows machines for the probe to succeed.

Ensure that large environments have a long enough interval for all IP addresses to be probed. For example, a network with 6,000 users and an interval of 10 minutes would require 10 WMI requests a second from each agent. These probes are queued and processed by the agent as needed.

If you enable the optional NetBIOS client probing feature, then the agent requires access through the Windows firewall to port 139. Windows file and print services also must be enabled. NetBIOS probing is available primarily for backward compatibility with Windows XP and earlier, and is not recommended.

Configuring the Monitored Servers



Servers

	Name	Type	Network Address
□	lab-client	active-directory	192.168.1.20
□	lab-client1	edirectory	192.168.1.21
□	mail-server	exchange	192.168.1.22

Include / Exclude list of configured networks

	Name	Discovery	Network Address

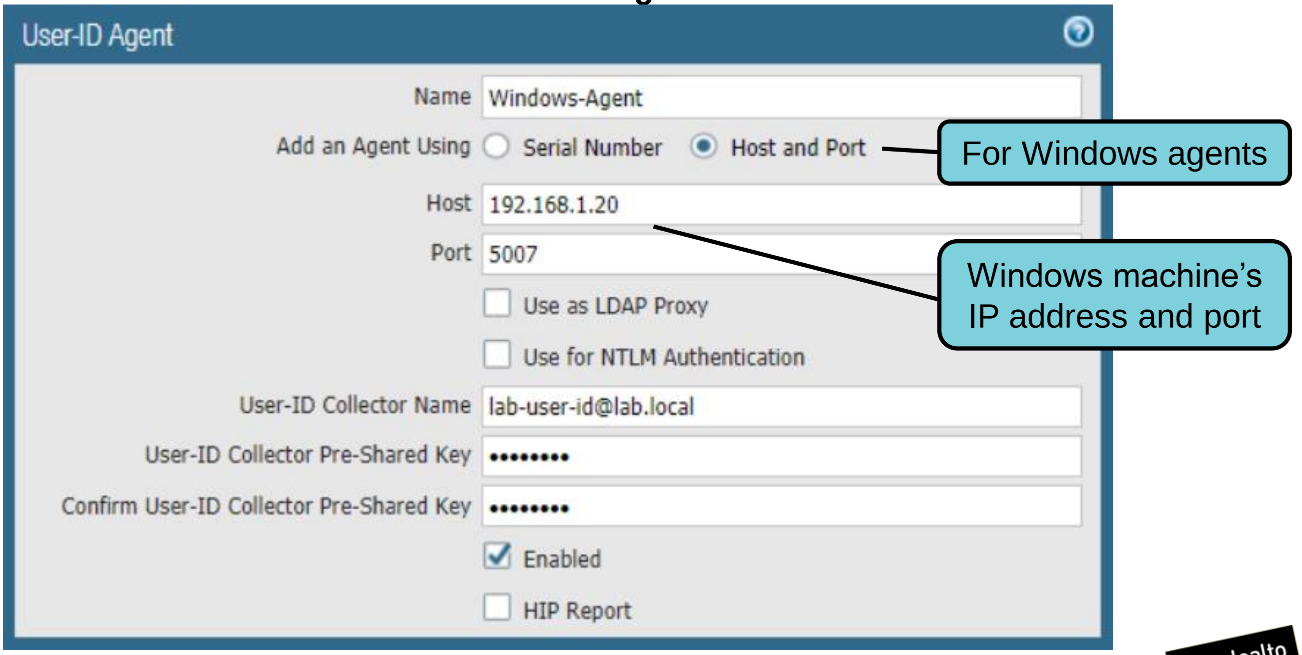
Manually add Domain Controllers, Exchange, eDirectory, and syslog senders.

Domain Controllers only

Select **Discovery** in the left-side pane to configure the monitored servers and networks. The **Auto Discover** button works only for Domain Controllers. Use the **Add** button to add Exchange Servers, Novell eDirectory servers, and syslog senders, or to manually add Domain Controllers. Click **Add** to open a separate window, where you are prompted for a server name, server address, and server type.

Configuring the Firewall to Connect to the Agent

Device > User Identification > User-ID Agents > Add



User-ID Agent

Name: Windows-Agent

Add an Agent Using: ○ Serial Number ● Host and Port

Host: 192.168.1.20

Port: 5007

□ Use as LDAP Proxy

□ Use for NTLM Authentication

User-ID Collector Name: lab-user-id@lab.local

User-ID Collector Pre-Shared Key: ••••••••

Confirm User-ID Collector Pre-Shared Key: ••••••••

☑ Enabled

□ HIP Report

For Windows agents

Windows machine's IP address and port

36 | © 2019 Palo Alto Networks, Inc.

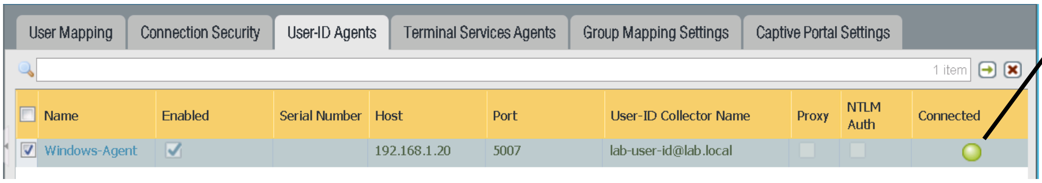
The firewall must be configured with information for every User-ID agent that it will connect to. If the firewall will connect to a Panorama management appliance to collect User-ID information, then select **Serial Number** as the host type. If the firewall will connect to a Windows-based agent or to an agent on another firewall, then select **Host and Port** as the host type. If you select **Host and Port**, then you must specify each agent's IP address and listening port. Communication between the firewall and a User-ID agent is secured using an encrypted SSL connection.

The firewall has the following specific, nonconfigurable timers for its communication to the agent:

- 2 seconds: Get the list of new IP address-to-username mappings from the agent. This list contains only new mappings since the last interval.
- 2 seconds: Send the list of unknown IP addresses that were encountered in traffic to the agent
- 5 seconds: Get the agent status
- 1 hour: Get the full list of IP address-to-username mappings from the agent

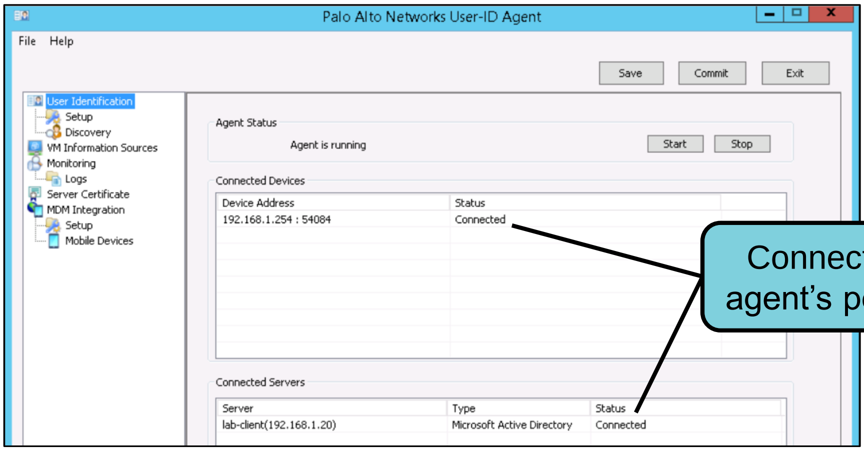
Confirm Connection to the User-ID Agent

Device > User Identification



□ Name	Enabled	Serial Number	Host	Port	User-ID Collector Name	Proxy	NTLM Auth	Connected
☑ Windows-Agent	✓		192.168.1.20	5007	lab-user-id@lab.local	□	□	●

Connection from firewall’s perspective – green is good



Agent Status

Agent is running

Connected Devices

Device Address	Status
192.168.1.254 : 54084	Connected

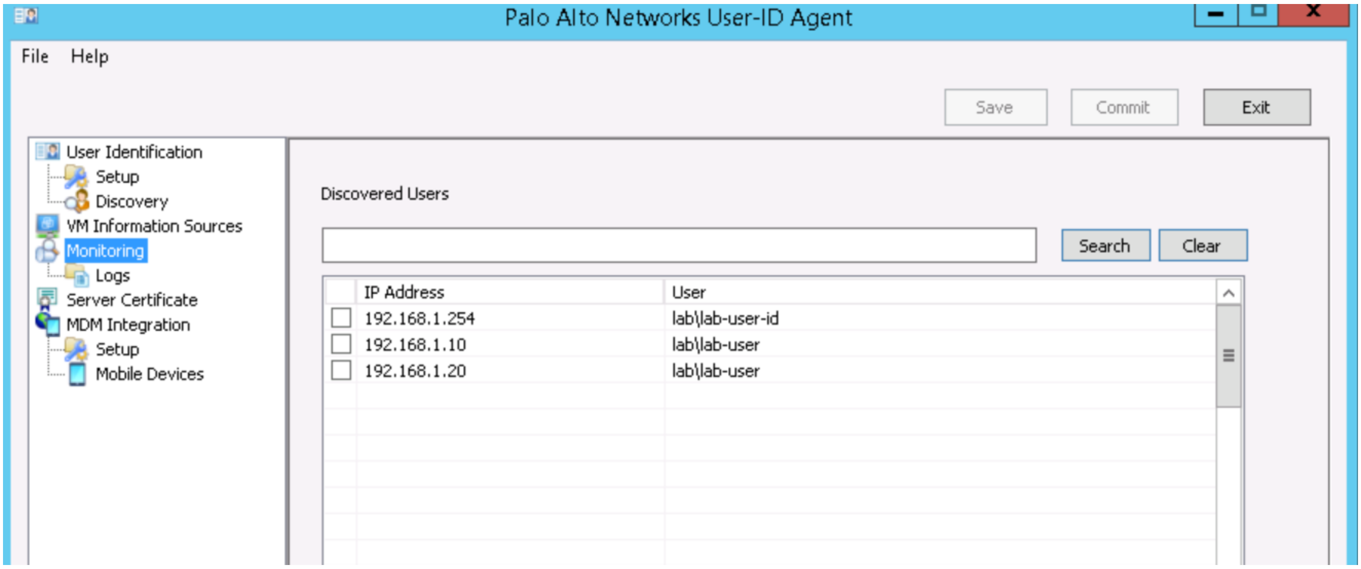
Connected Servers

Server	Type	Status
lab-client(192.168.1.20)	Microsoft Active Directory	Connected

Connection from agent’s perspective

Use the firewall’s web interface and the Windows agent to confirm connectivity between the firewall and the Windows agent.

Display Mappings from the Windows Agent

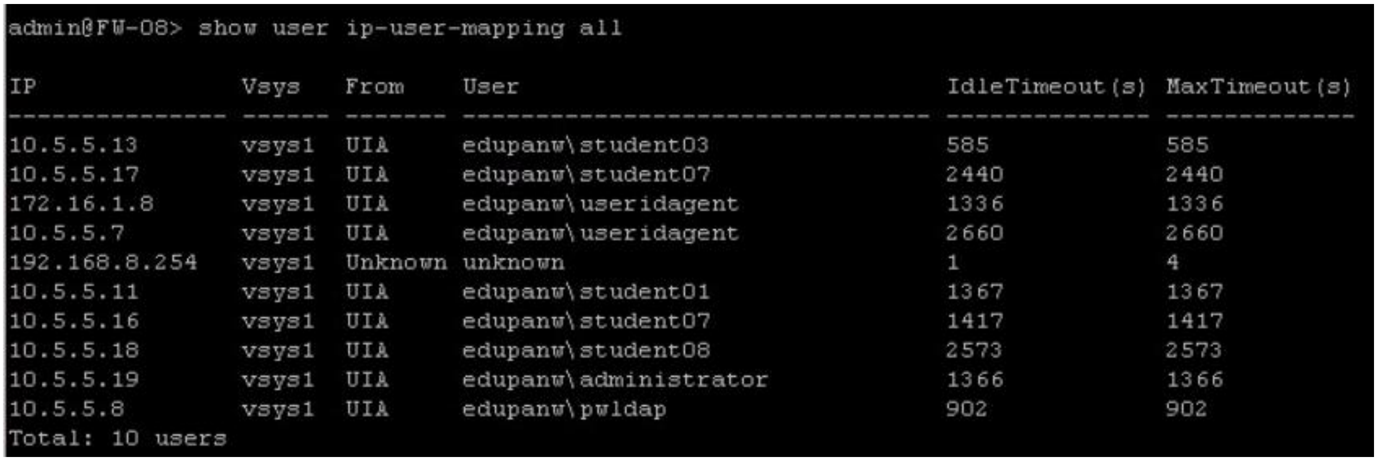


	IP Address	User
□	192.168.1.254	lab\lab-user-id
□	192.168.1.10	lab\lab-user
□	192.168.1.20	lab\lab-user

Use the **Monitoring** tab in the Windows agent to display IP address-to-username mapping by the Windows agent.

Display Mappings from the Firewall CLI

- Show mapping for all or specific IP addresses



```
admin@FW-08> show user ip-user-mapping all

IP              Vsys   From    User                             IdleTimeout(s) MaxTimeout(s)
--------------- ------ ------- -------------------------------- -------------- -------------
10.5.5.13       vsys1  UIA     edupanw\student03                585            585
10.5.5.17       vsys1  UIA     edupanw\student07                2440           2440
172.16.1.8      vsys1  UIA     edupanw\useridagent              1336           1336
10.5.5.7        vsys1  UIA     edupanw\useridagent              2660           2660
192.168.8.254   vsys1  Unknown unknown                          1              4
10.5.5.11       vsys1  UIA     edupanw\student01                1367           1367
10.5.5.16       vsys1  UIA     edupanw\student07                1417           1417
10.5.5.18       vsys1  UIA     edupanw\student08                2573           2573
10.5.5.19       vsys1  UIA     edupanw\administrator            1366           1366
10.5.5.8        vsys1  UIA     edupanw\pwldap                   902            902
Total: 10 users
```

You can display how users and IP addresses are being mapped on the firewall only by using the firewall’s CLI.

Commonly used commands for checking User-ID mappings include the following:

- `> show user user-id-agent statistics`
- `> show user user-ids all`
- `> show user ip-user-mapping all`
- `> show user ip-user-mapping <ip/netmask>`

User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

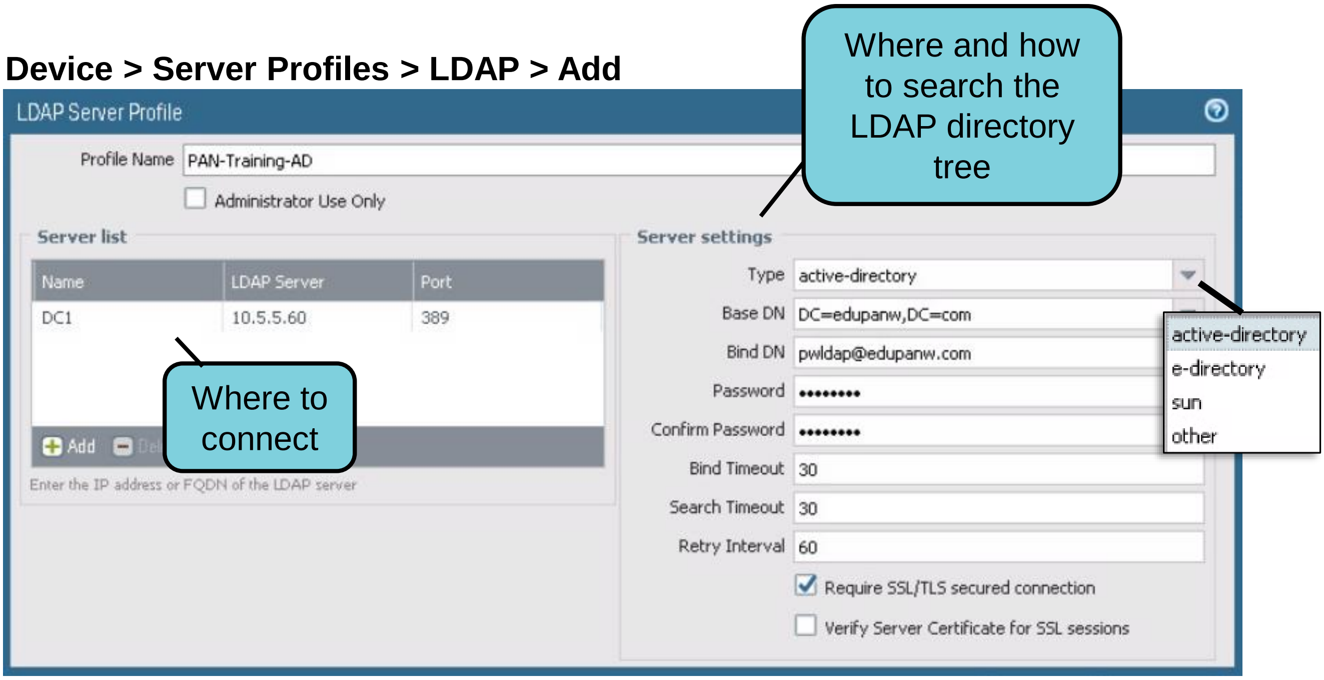
Windows-based agent configuration

Configuring group mapping

User-ID and security policy

LDAP Server Profile

Device > Server Profiles > LDAP > Add



LDAP Server Profile

Profile Name: PAN-Training-AD

☐ Administrator Use Only

Server list

Name	LDAP Server	Port
DC1	10.5.5.60	389

Enter the IP address or FQDN of the LDAP server

Server settings

Type: active-directory

Base DN: DC=edupanw,DC=com

Bind DN: pwldap@edupanw.com

Password: ••••••••

Confirm Password: ••••••••

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☑ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

Where and how to search the LDAP directory tree

Where to connect

A Server Profile specifies which LDAP servers will be contacted, the order in which they are contacted, and how and where to search the LDAP directory tree. By default, port 389 communicates to the LDAP server using TLS. To use SSL instead, specify port 636.

The **Type** menu specifies the type of LDAP server to which the firewall will connect.

The **Base DN** field represents the point in the LDAP directory tree where the firewall will begin its search for users and groups. The **Base DN** information should autopopulate from the LDAP server when you click the **Base DN** drop-down arrow, but you can manually override the value. If you have difficulties identifying your directory base DN, on the Domain Controller open the **Active Directory Domains and Trusts** Microsoft Management Console snap-in and look at the name of the top-level domain.

The **Bind DN** and **Password** fields contain the LDAP username and password that the firewall uses to connect to the LDAP server. The format of this field must match what the LDAP server is expecting. For example, it could be either a fully qualified LDAP name (cn=administrator,cn=users,dc=cse,dc=local) or a user principal name (administrator@cse.local). The bind DN account must have sufficient LDAP permissions to read the LDAP directory.

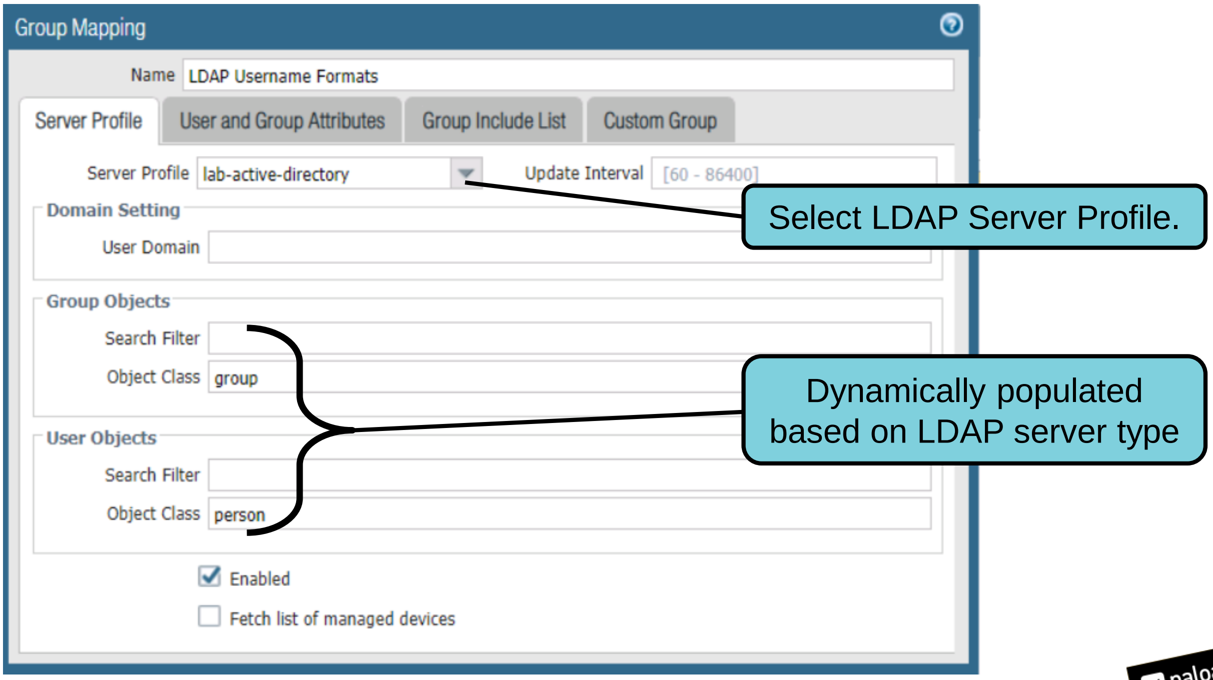
If universal groups are used in AD, a global catalog, or GC, server must be used to capture group memberships. The firewall can access a GC server only if the LDAP port is set to 3268.

The default timeout and interval settings can be overridden as necessary based on the performance of your network and LDAP server.

Ensure that the **Require SSL/TLS secured connection** check box is selected. By default it should be. To have the firewall verify the LDAP server's certificate, select the **Verify Server Certificate for SSL sessions** check box.

Creating User-ID Group Mapping Filters

Device > User Identification > Group Mapping Settings > Add



Group Mapping

Name: LDAP Username Formats

Server Profile: lab-active-directory

Update Interval: [60 - 86400]

Domain Setting

User Domain:

Group Objects

Search Filter:

Object Class: group

User Objects

Search Filter:

Object Class: person

☑ Enabled

□ Fetch list of managed devices

Select LDAP Server Profile.

Dynamically populated based on LDAP server type

On the **Server Profile** tab, use the **Server Profile** menu to select your LDAP Server Profile.

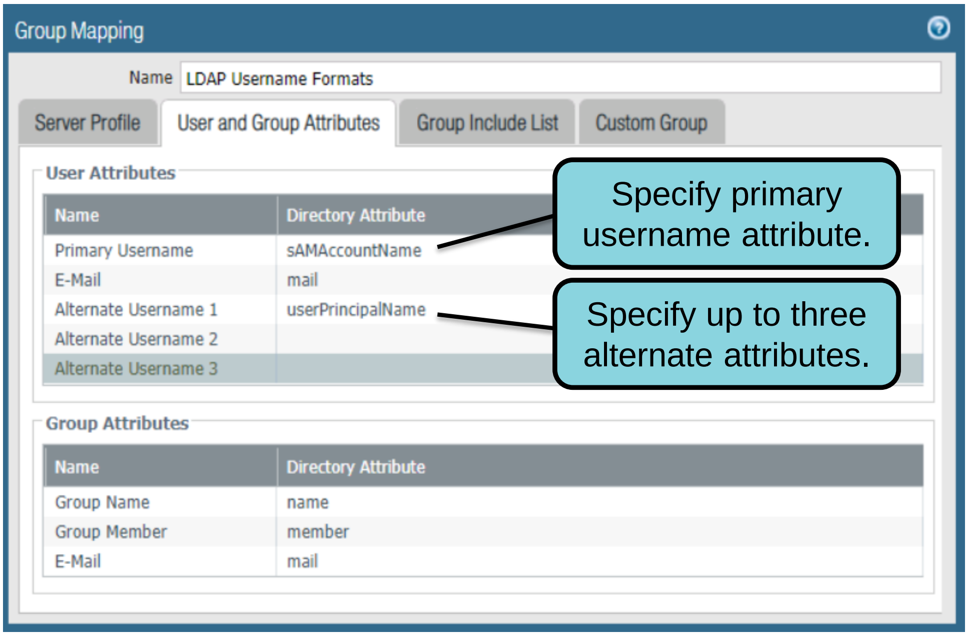
The **Domain Setting** value normally is blank. Enter a NetBIOS domain name value only if you need to override the domain automatically detected on the LDAP server.

The **Group Objects** fields are dynamically populated. Modify the **Group Objects** fields to configure the firewall to look for group names in non-standard LDAP tree locations. The groups found by the firewall will be displayed in the **Available Groups** pane on the **Group Include List** tab.

The **User Objects** fields are dynamically populated. Modify the **User Objects** fields to configure the firewall to look for usernames in non-standard LDAP tree locations.

Multiple Username Formats

Device > User Identification > Group Mapping



Name: LDAP Username Formats

User Attributes

Name	Directory Attribute
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

Group Attributes

Name	Directory Attribute
Group Name	name
Group Member	member
E-Mail	mail

Specify primary username attribute.

Specify up to three alternate attributes.

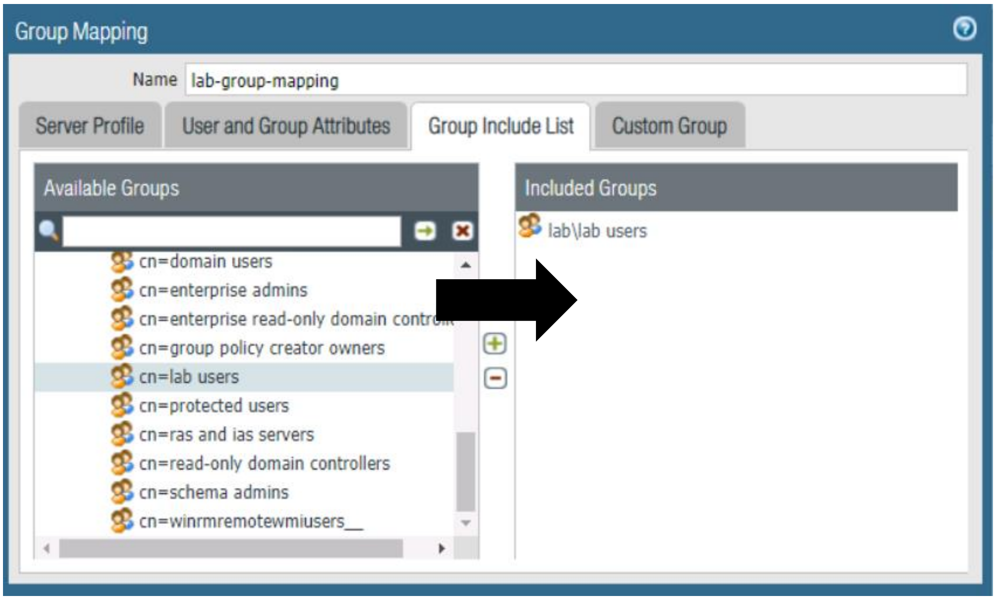
Starting with PAN-OS 8.1, the firewall can identify a user even if the User-ID sources send usernames in multiple formats. For example, the username format could be a Sam Account Name, E-mail, User Principal Name, or UPN, or Common Name. When the firewall identifies a user, the usernames are matched based on the user attributes that the firewall will read from the LDAP-compliant directory service. You can specify which attributes are used to collect usernames from the directory service using a Group Mapping Profile.

When the firewall supports multiple user attributes, you should specify an attribute as the **Primary User Name** for users. This value represents the username in the logs, in the reports, and in the policy configuration.

In addition to configuring a **Primary User Name**, you can configure an email or up to three alternate usernames to uniquely identify users.

Filtering Groups Sent to the Firewall

Device > User Identification > Group Mapping Settings > Add



Name: lab-group-mapping

Available Groups:
- cn=domain users
- cn=enterprise admins
- cn=enterprise read-only domain contro
- cn=group policy creator owners
- cn=lab users
- cn=protected users
- cn=ras and ias servers
- cn=read-only domain controllers
- cn=schema admins
- cn=winrmremotewmiusers__

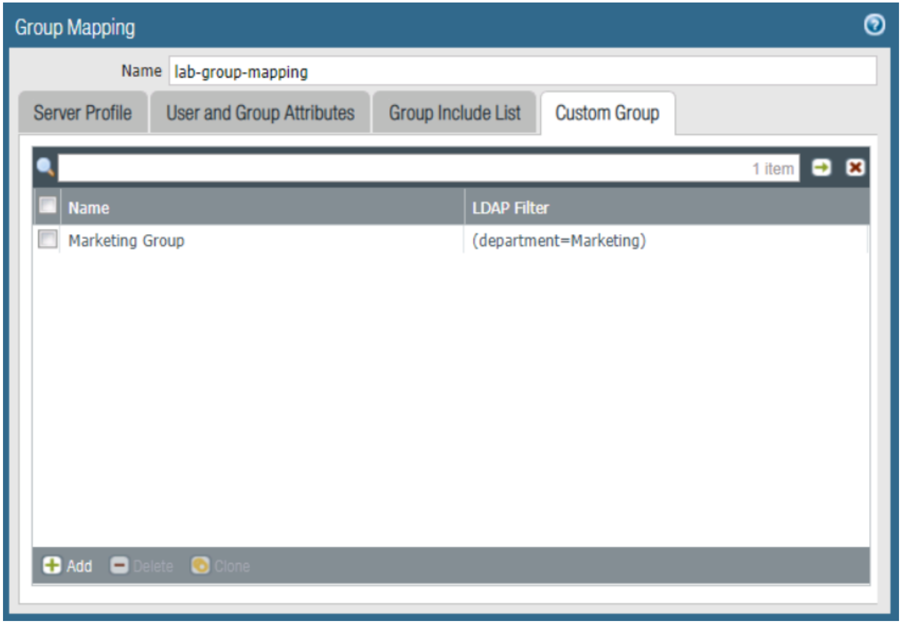
Included Groups:
- lab\lab users

- Only Included Groups are available on drop-down lists in policy rules.
- Shorter lists simplify firewall policy rule administration.

Use the **Group Include List** tab to filter which groups discovered on the LDAP server are displayed on the drop-down lists in firewall policy rules. By default, if you do not move groups to the **Included Groups** pane, all discovered groups are available in policy rules.

Custom Groups Based on LDAP Filters

Device > User Identification > Group Mapping Settings > Add



Name: lab-group-mapping

Name	LDAP Filter
□ Marketing Group	(department=Marketing)

- Define custom LDAP filters that select group members.
- Assign a custom filter a group name.
- Use a group name in policy rules.

The **Custom Group** tab enables you to define custom groups based on LDAP filters so that you can base firewall policy rules on user attributes that do not match existing LDAP user groups. Definition of a custom group can be quicker than the creation of new group or by changing an existing group on an LDAP server, and does not require an LDAP administrator to intervene. User-ID maps all the LDAP directory users who match your filter to the custom group. For example, you might want a Security policy rule that allows only users in the marketing department to access social networking sites. If no LDAP group exists for that department, you can configure an LDAP filter that matches users for whom the LDAP attribute department is set to Marketing.

Log queries and reports that are based on user groups include custom groups.

You can add custom groups to the **Allow List** of Authentication Profiles.

User-ID overview

User mapping methods overview

Configuring User-ID

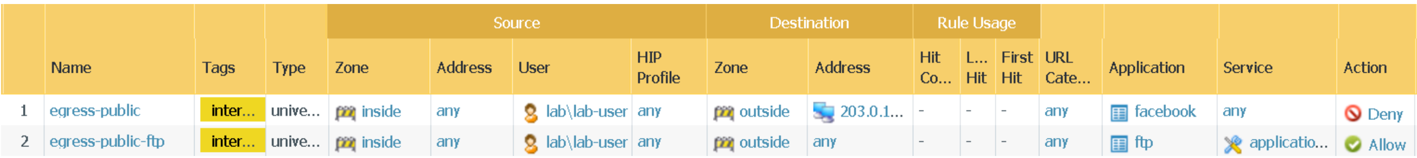
PAN-OS integrated agent configuration

Windows-based agent configuration

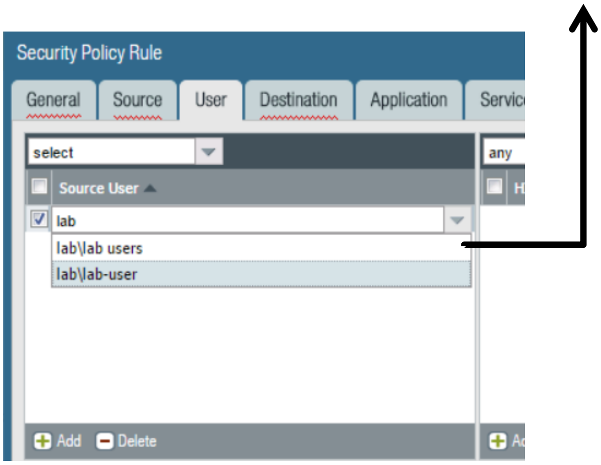
Configuring group mapping

User-ID and security policy

Selecting Users and Groups for a Security Policy



				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Co...	L... Hit	First Hit	URL Cate...	Application	Service	Action
1	egress-public	inter...	unive...	inside	any	lab\lab-user	any	outside	203.0.1...	-	-	-	any	facebook	any	Deny
2	egress-public-ftp	inter...	unive...	inside	any	lab\lab-user	any	outside	any	-	-	-	any	ftp	applicatio...	Allow



Security Policy Rule

select

any

Source User

☑ lab

lab\lab users

lab\lab-user

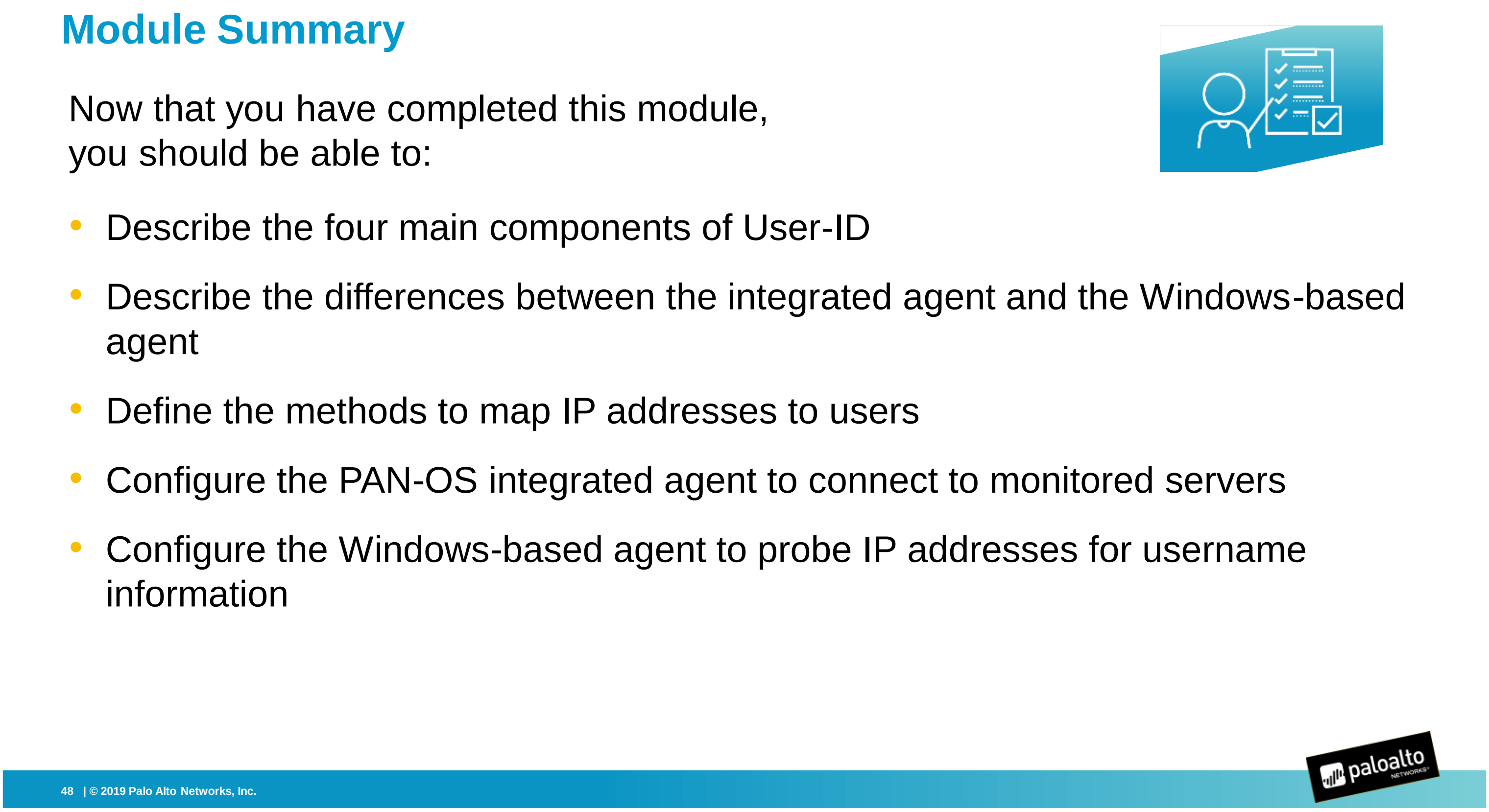
- Source User options:
  - any
  - pre-logon
  - known-user
  - unknown
  - select

When you select users for a Security policy, these options are available:

- any: Matches any value for user
- pre-logon: Used with certain GlobalProtect implementations
- known-user: Matches any user or group identified by User-ID
- unknown: Matches traffic where the user could not be identified by User-ID methods
- select: Matches a specific user or group identified by User-ID

When you use a user or group in a policy rule, remember that the **Source Address** field and the **Source User** field are evaluated with a logical AND condition. The rule applies only if both the specified user or group and the specified source addresses match. Be careful not to make the match conditions so specific that the policy eliminates permitted traffic.

Users and groups can be used in a policy rule only if they are known on the firewall. For larger environments, a best practice usually is to set policies based on groups rather than on individual users. The number of users often becomes unwieldy for defining policy as the number of users in an environment increases.



Module Summary

Now that you have completed this module,
you should be able to:

- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information

Now that you have completed the module, you should be able to:

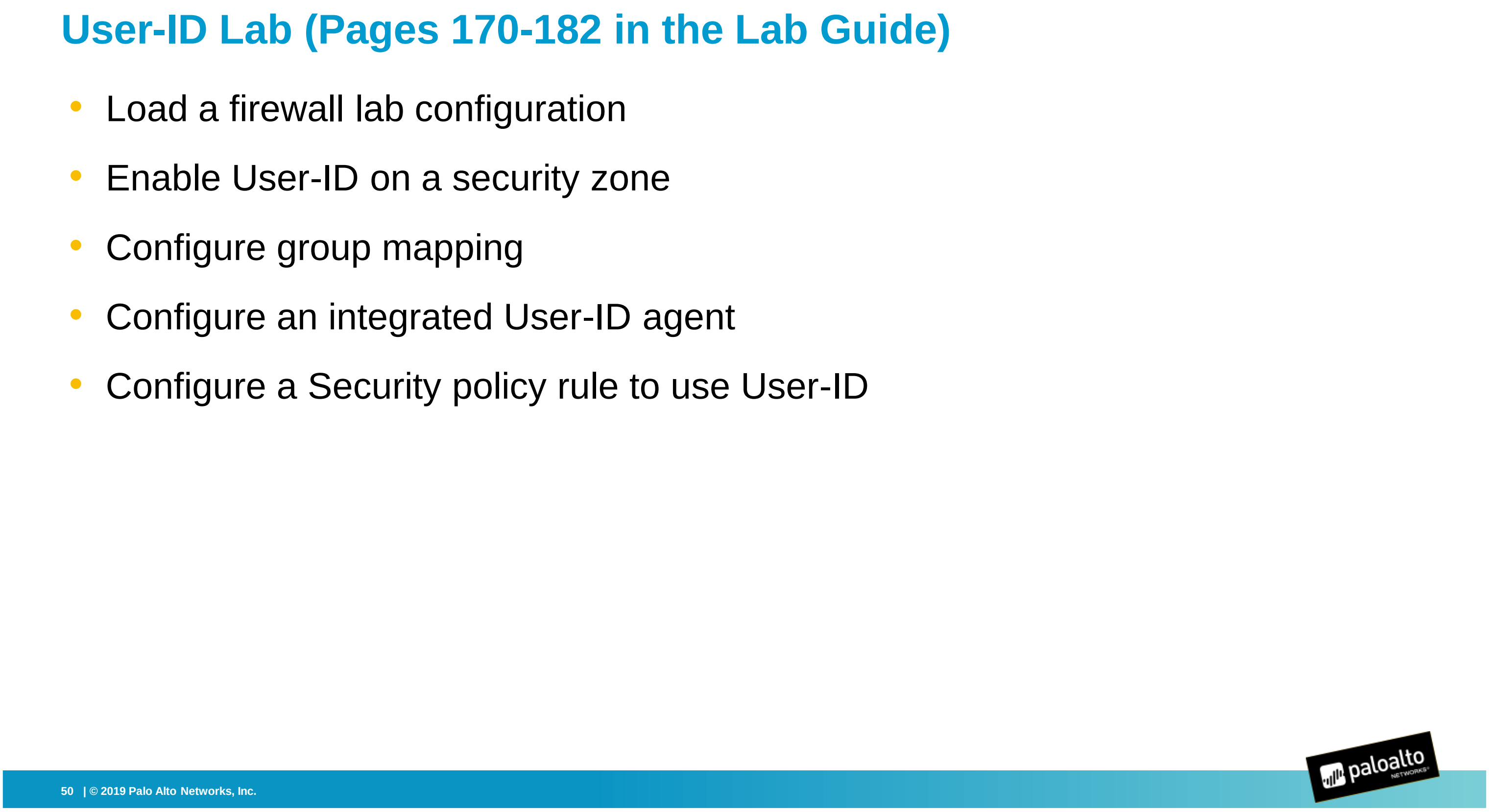
- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information

Questions?

49 | © 2019 Palo Alto Networks, Inc.

Review Questions

1. Which two statements are true regarding User-ID and firewall configuration? (Choose two.)
   a. Communications between the firewall and the User-ID agent are sent over an encrypted SSL connection.
   b. The firewall needs to have information for every User-ID agent to which it will connect.
   c. NetBIOS is the only client probing method supported by the User-ID agent.
   d. The User-ID agent must be installed on the Domain Controller.
2. Which three items are valid choices when configuring the **Source User** field in a Security policy rule? (Choose three.)
   a. all
   b. known-user
   c. any
   d. unknown
   e. none
3. True or false? You must deploy the Windows-based User-ID agent to collect IP address-to-username mappings from a Windows AD Domain Controller.
   a. true
   b. false
4. Which statement is true regarding User-ID and Security policy rules?
   a. If the user associated with an IP address cannot be determined, all traffic from that address will be dropped.
   b. The **Source User** field can match only users, not groups.
   c. The **Source IP** and **Source User** fields cannot be used in the same policy.
   d. Users can be used in policy rules only if they are known by the firewall.



User-ID Lab (Pages 170-182 in the Lab Guide)

- Load a firewall lab configuration
- Enable User-ID on a security zone
- Configure group mapping
- Configure an integrated User-ID agent
- Configure a Security policy rule to use User-ID

PROTECTION. DELIVERED.

Answers to Review Questions

1. a, b
2. b, c, d
3. b (false)
4. d

This page intentionally left blank