User Identification with PAN-OS 2.1

Tech Note

Overview

PAN-OS running on Palo Alto Networks (PAN) firewalls is capable of leveraging user and user group information from Active Directory (AD) and user information from RADIUS servers for visibility and policy enforcement.

The User Identification Agent[1] (UIA) interfaces with Active Directory to communicate user group, user, and IP address information to the Palo Alto Networks firewalls for visibility only or visibility and policy enforcement.

The ACC, App-Scope, and logs will include username in addition to IP address when user identification is configured, showing visibility into individual user activity. If used to enforce policy as well, users and user groups can be selected in the security policies as well as the SSL decryption policies when Active Directory is used. When only a RADIUS server is used, usernames must be manually entered into policy for enforcement.

This document provides an overview of how to implement user identification with Active Directory and RADIUS servers; describing how these methods work and how to best implement them.

Available Methods

Three methods are available with PAN-OS 2.1 for user identification:

- Agent with Active Directory
- Captive Portal with NTLM
- Captive Portal with Web Forms

The three user identification methods are shown in preferred order of use. When Agent with AD is unable to associate a user with an IP address, the Captive Portal methods can take over to identify the user with a browser. Within Captive Portal, if the NLTM method is unable to identify users, the last resort is to identify with a web form, soliciting input directly from the user.

Captive Portal with NTLM is preferred over Captive Portal with Web Forms, as the former can be configured to work without any user intervention. When using Captive Portal with Web Forms, user browsing is stopped until their username and password is entered manually.

Each method initiates a process to map users to IP addresses. Once the mapping is in place, all IP traffic from the mapped IP address is associated with the mapped user, for the purposes of visibility and policy enforcement. The user to IP address mapping is valid for a certain amount of time. The mapping will expire unless the method successfully re-associates the user to the IP address before the timeout/age-out limits.

Due to the nature of user to IP address mapping, PAN-OS 2.1 is unable to provide accurate user identification in the following environments, as multiple users may appear to utilizing the same host IP address:

- Citrix servers
- when a NAT device sits downstream, between the users and PAN firewall
- when a proxy device sits downstream, between the users and the PAN firewall

---

[1] The User Identification Agent is referred to as UIA or just ‘Agent’ throughout this document

The table below summarizes key points for each method.

Points	Agent with AD	Captive Portal with NTLM	Captive Portal with Web Forms
Software required	• PAN UIA	• PAN UIA • Browser	• Browser
Required Software location	• Windows Member Server	• Windows Member Server • Client Desktop	• Client Desktop
Requires Active Directory	Yes	Yes	No, but suggested for policy creation and group information
Active Directory Interfaces	Native LDAP RADIUS	Native	RADIUS
Requires manual user interaction	No	No, but available as a fallback	Yes
Requires NTLM-aware browser	No	Yes	No
Supports non-Windows users	Yes, if they can log into the domain	No	Yes
Requires NTLM hostname in DNS	No	Yes	No
Users should trust PAN firewall web management certificate (or the local CA that signed it)	N/A	N/A	Yes
Users will always receive Hostname Mismatch SSL browser warning	No	No	Yes
When unable to identify user, falls back to ...	Captive Portal with NTLM (if Captive Portal Policy configured)	Captive Portal with Web Forms (automatic)	None - traffic subject to policy decision without any user information

Points	Agent with AD	Captive Portal with NTLM	Captive Portal with Web Forms
Credentials passed securely	never passed	user password combined with random token, passed in the clear	SSL-encrypted base-64 encoded cleartext
IP address → user idle timeout	60 min	15 min	15 min
IP address → user max timeout (per identification)	n/a	60 min	60 min

Each method employ various underlying mechanisms to identify users, which are described in Part I: Fundamentals of this document.

Selecting a Method

Each of the three available identification methods has pros and cons associated with their implementation. The best combination and configuration of these methods depends on the individual needs and size of an organization.

In general, the preferred implementation will take advantage of all three methods, to encompass the entire range of users and devices in an organization's network.

The only time all three methods would not be used would be in the case when no Active Directory server is on the network.

Capacity

User Identification capacity limits:

- The PA-4000 series can support up to 64,000 concurrent users; the PA-2000 series can support up to 47,000 concurrent users.
- Up to 640 groups can be used in policies for each virtual system (vsys)
- Each UIA can connect to up to 10 Domain Controllers
- Each firewall can support up to 100 UIA's
- Limit of 100 entries each in the Allow and Ignore list on the UIA
- Only 1 NTLM handshake can be in process between a UIA and AD server at a time

Performance

A few performance characteristics that are important to understand and plan for:

- Latency of user propagation: the latency of user propagation measures the time between the user authenticating to the network and the Palo Alto device retrieving the IP address to user to user group information. This typically takes a maximum of 1 second, which will almost always be unnoticeable to the user.
- Impact on PAN device performance: specifically the impact on the session setup rate: when users or user groups are used in policies, it adds one more attribute to the policy match criteria. This results in a variable impact to session setup rates. To minimize the impact, it is recommended to use user groups instead of individual users in policies.
- Impact on AD server and Windows UIA host performance: large deployments can consume substantial computing resources

Part I : Fundamentals

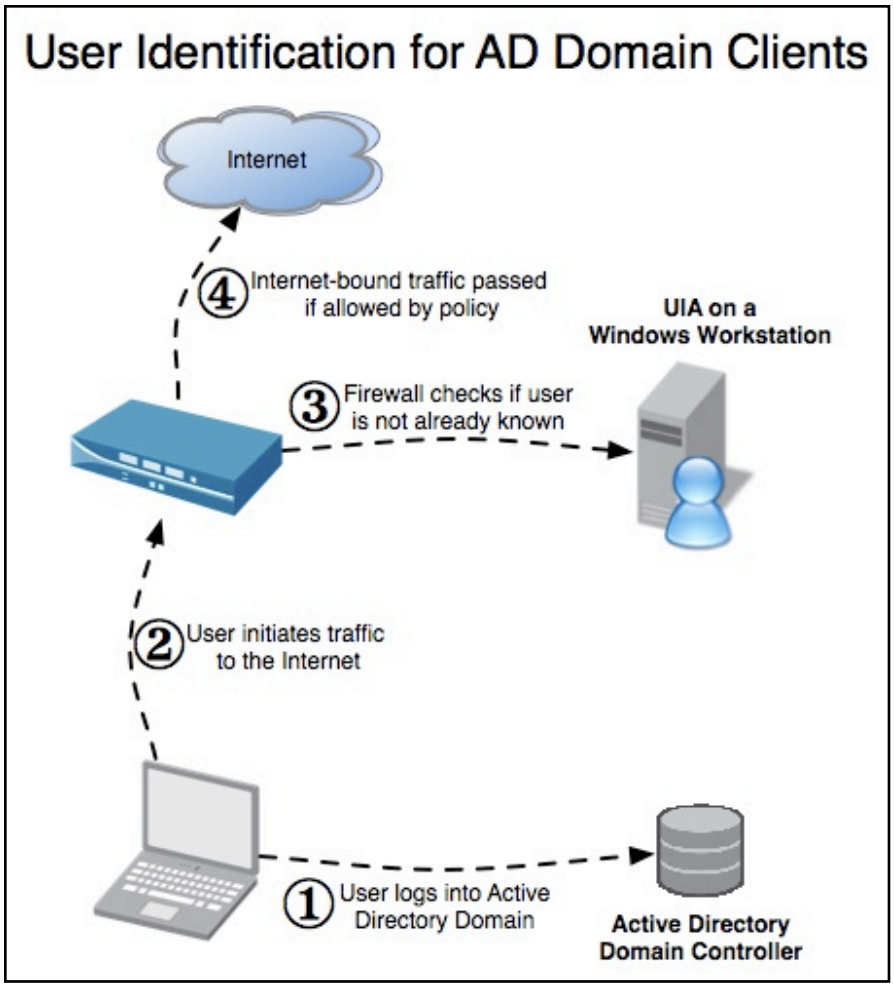
Agent with Active Directory

With the User Identification Agent with Active Directory method, user information is made available automatically to the firewall, for visibility and policy enforcement. If users log into their desktop with their AD credentials, this method should detect their network login, then maintain their user to IP address mapping until within *X* minutes (by default) of when they log off form their computer.

To use this method, the UIA must be installed and configured to work with the AD domain and PAN firewall.

The diagram below depicts the four steps involved for user identification within an Active Directory domain:

1. User logs into their desktop with domain credentials
2. User initiates IP-based traffic that traverses the PAN firewall
3. PAN firewall checks with the UIA if the user isn't already mapped to an IP address
4. Firewall policy is applied, based on the user information, not just the IP address



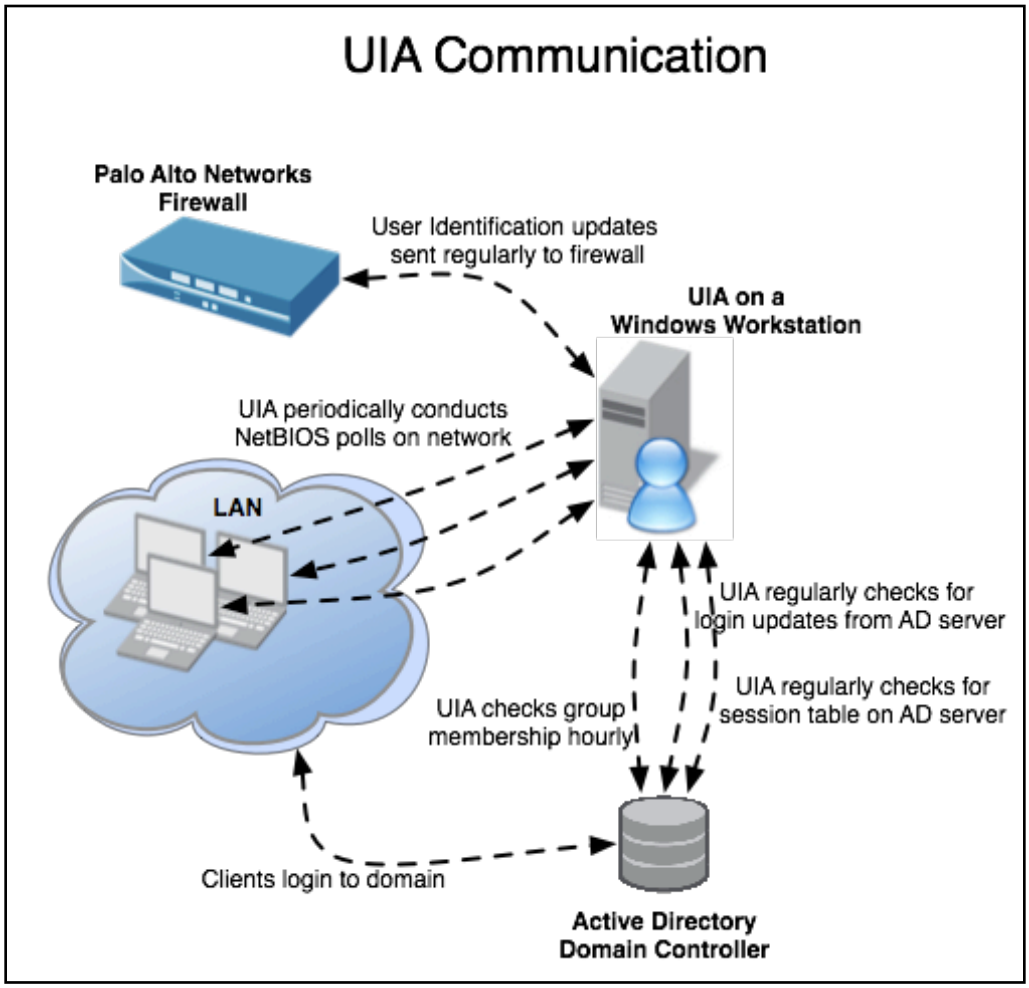
Agent User to IP address Mapping

The User Identification Agent maintains a mapping of **IP address → user → user group → domain**, which can be used for visibility and policy enforcement. To understand how it maintains this mapping, the underlying mechanisms are described here.

The mapping is achieved via three concurrent mechanisms.

- Direct connection to the Domain Controller to map group membership information. The group membership information is used to map users to user groups and domains that allow policies to be defined by user group and domain. This information is synchronized on an hourly basis by default. Users do not need to be online for their group information to be included in this communication. All group information for the domain is included.
- Direct connection to the Domain Controller to monitor activity. The agent monitors users signing in, as well as watching the active sessions to determine what IP addresses users have.
- Polling the host PC to verify IP address and user information using NetBIOS. This occurs when an IP address is seen that doesn't have a user name associated with it, as well as every 20 minutes to verify the IP address to user name mapping is still correct.

The connections described above are also depicted in the diagram below. The traffic between desktop clients and Active Directory server is also included.

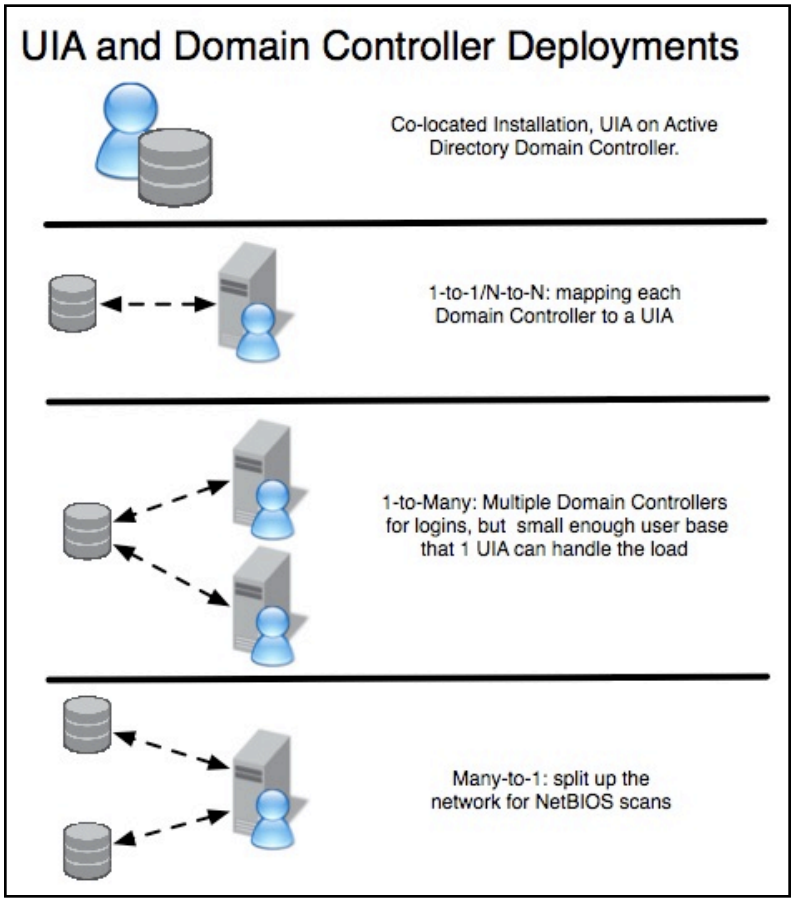


Agent Deployment

The Palo Alto Networks UIA is installed on a Domain Controller or a member Windows workstation with at least read-only access to the Domain Controller. Whether installed on a Domain Controller, Windows workstation or other Windows server in the domain, appropriate UIA placement should be determined. There are a number of factors to keep in mind when choosing the number and location of User Identification Agents to install.

- Each UIA has two purposes: collect login/active session information from a Domain Controller and scan part of a network with NetBIOS queries.
- The UIA can be co-located on the target Domain Controller.
- Each Domain Controller accepting logins from desktop users must be associated with at least one UIA.
- Associate a single UIA with multiple Domain Controllers when each Domain Controller has a limited number of users, yet the single UIA is still in a position to perform NetBIOS queries to all desktops.
- When a User Identification Agent is associated with multiple Active Directory domain controllers, each domain controller must be in the same AD domain.
- At least one User Identification Agent is required for each Active Directory domain.

The diagram on the next page depicts the different deployment scenarios between the UIA (blue figure), domain controller (circular grey object), and Windows domain member servers (grey computer).



Note: There must be at least one User Identification Agent in each Active Directory domain

In all examples in the previous diagram, users continue to authenticate to Active Directory with no change. The User Identification Agent(s) watch the activity on the Domain Controller(s) and maintain a table of IP address → user → user groups. The Palo Alto Networks firewall maintains a connection to the agent via SSLv2 and polls the agent(s) for updated information every second to maintain an up-to-date table for visibility and enforcement.

All Palo Alto Networks firewalls in the deployment should be configured to communicate with all the User Identification Agents associated with Domain Controllers the firewall would like user identification on.

Agent to Firewall Communication

The User Identification Agent must have IP connectivity to the firewall management interface. This is true even if the firewall is managed by an inline, Layer 3 interface on the firewall. All Agent communication to the firewall is sent and received through the firewall management interface. It is not possible to use an inline Layer 3 interface for this function in PAN-OS 2.1.

NetBIOS Probes

The Agent with AD method is most accurate when NetBIOS probes are enabled, more quickly verify changes relating to logged in users. While the UIA will learn from the AD security log when new user log into their desktop when they arrive in at work in the morning, and will be able to reconfirm users when network resources such as network shares or printers are used; it will not necessarily detect when users have logged off from their workstations. NetBIOS probes confirm that previously identified active users are still active on their workstations.

Three things can make the use of NetBIOS probes unattractive:

- Bandwidth utilization for all the NetBIOS probes, particularly in WAN environments
- Computing resource utilization of the Windows member server hosting the UIA
- Desktop hosts unable to respond to probes, due to 3rd party security applications or use of Windows Vista

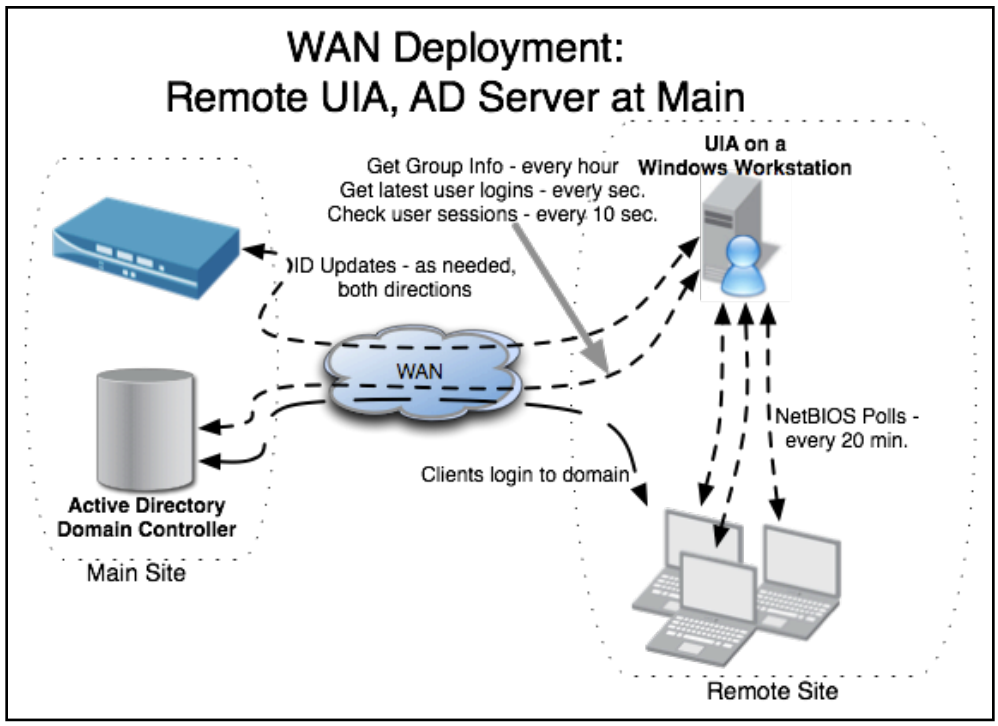
With Redundancy

If the firewall looses connectivity with any User Identification Agents, the firewall is no longer able to prevent the mappings of **IP addresses → users** from aging-out. To avoid this scenario, deploy at least one other UIA. If each DC communicates to at least two UIA's, the outage of a single UIA will not hamper user identification on the firewall. However, each redundant UIA to the DC multiplies the information sent to the firewall. The firewall must still process the duplicate information.

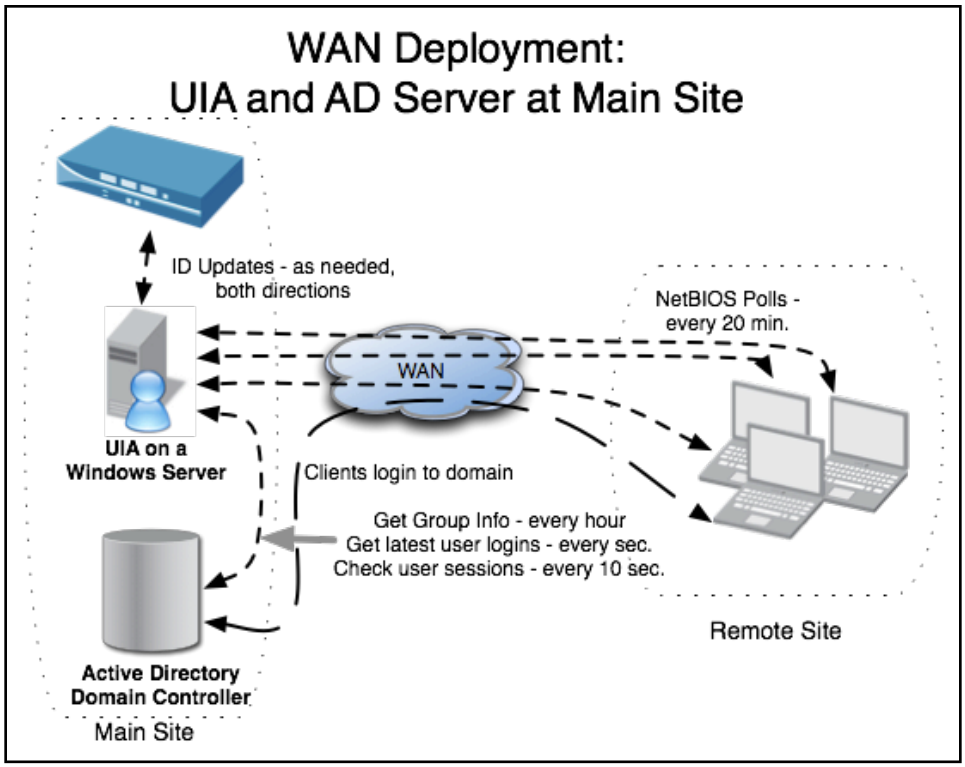
Redundant deployments are similar to the Many-to-1 scenario above, except that redundant deployments perform the same NetBIOS probes as their peer with the same DC.

Over WAN links

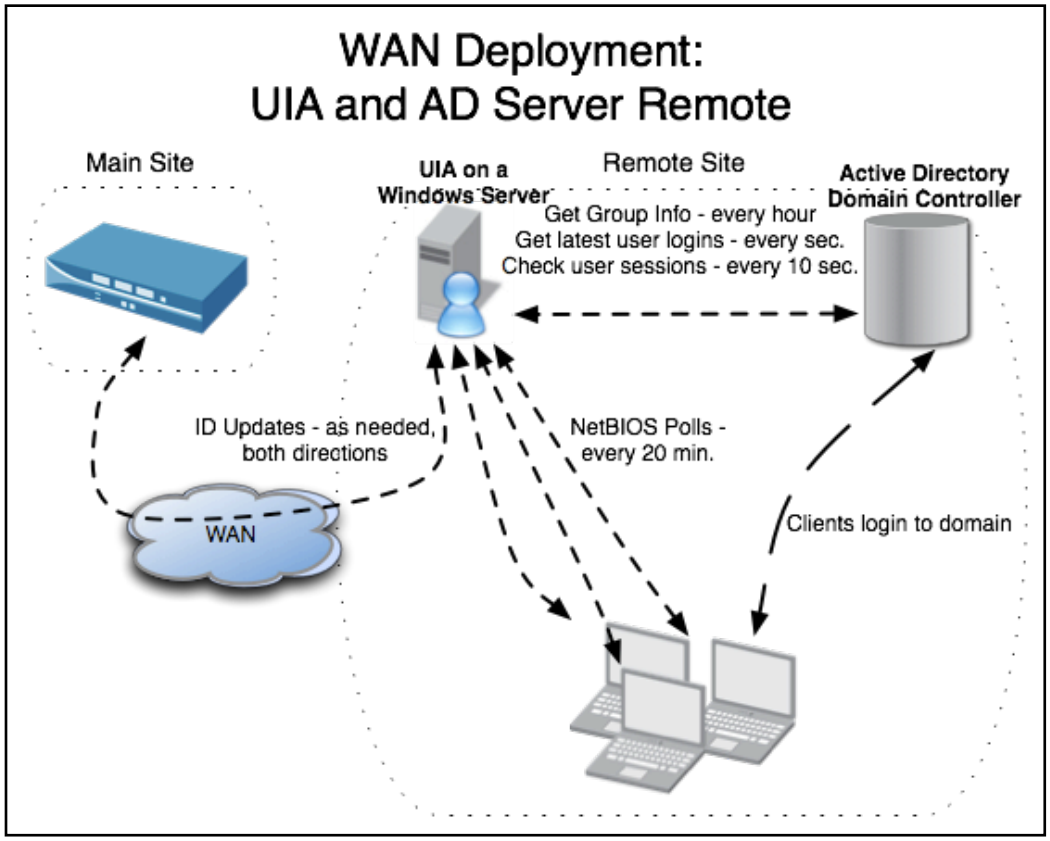
Deployments involving low bandwidth or high latency WAN links will have to choose between the communication from UIA to firewall; UIA to the DC; and/or UIA to the desktops traversing the WAN link.



In the diagram to the right, the UIA is at the remote site with NetBIOS probes enabled. The frequent (every 20 minutes by default) and numerous (to every IP address in the target network) NetBIOS probes are confined to the local remote network, whereas the UIA to AD domain controller communication of group information (every hour), latest user logins from the AD security log (every second), and active user sessions (when users use AD shared resources) traverse the WAN link. In addition, updates and requests between the firewall and UIA are sent as needed.



In the event that the UIA is located at the main site along with the AD server, NetBIOS probes will traverse the WAN links. This may be an unwelcome configuration when either the WAN link is low bandwidth (such as a 56K link) or the remote network has many computers. NetBIOS probes should be disabled if this is the case, with Captive Portal methods configured to augment the Agent with AD deployment.



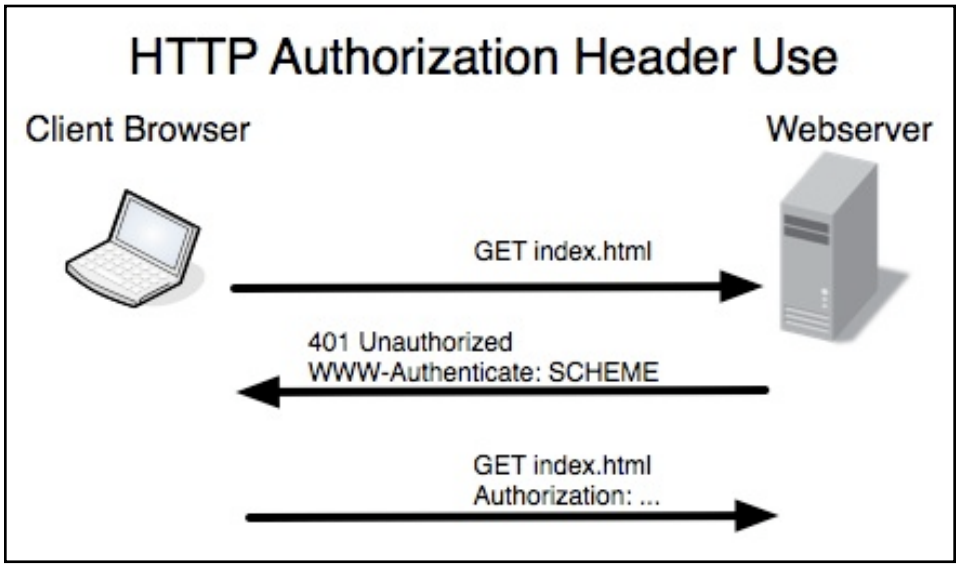
In some cases, both the AD server and the UIA agent are located at the remote site. Only the UIA to firewall requests and updates will traverse the WAN link. The frequent communications between the UIA, AD Server, and user computers will be confined to the remote LAN network.

Captive Portal with NTLM

The preferred method of browser-based identification makes use of the HTTP Authorization header and NTLM authentication, as the user is not prompted to manually submit their username and password if they are logged into their domain.

HTTP Authentication Headers

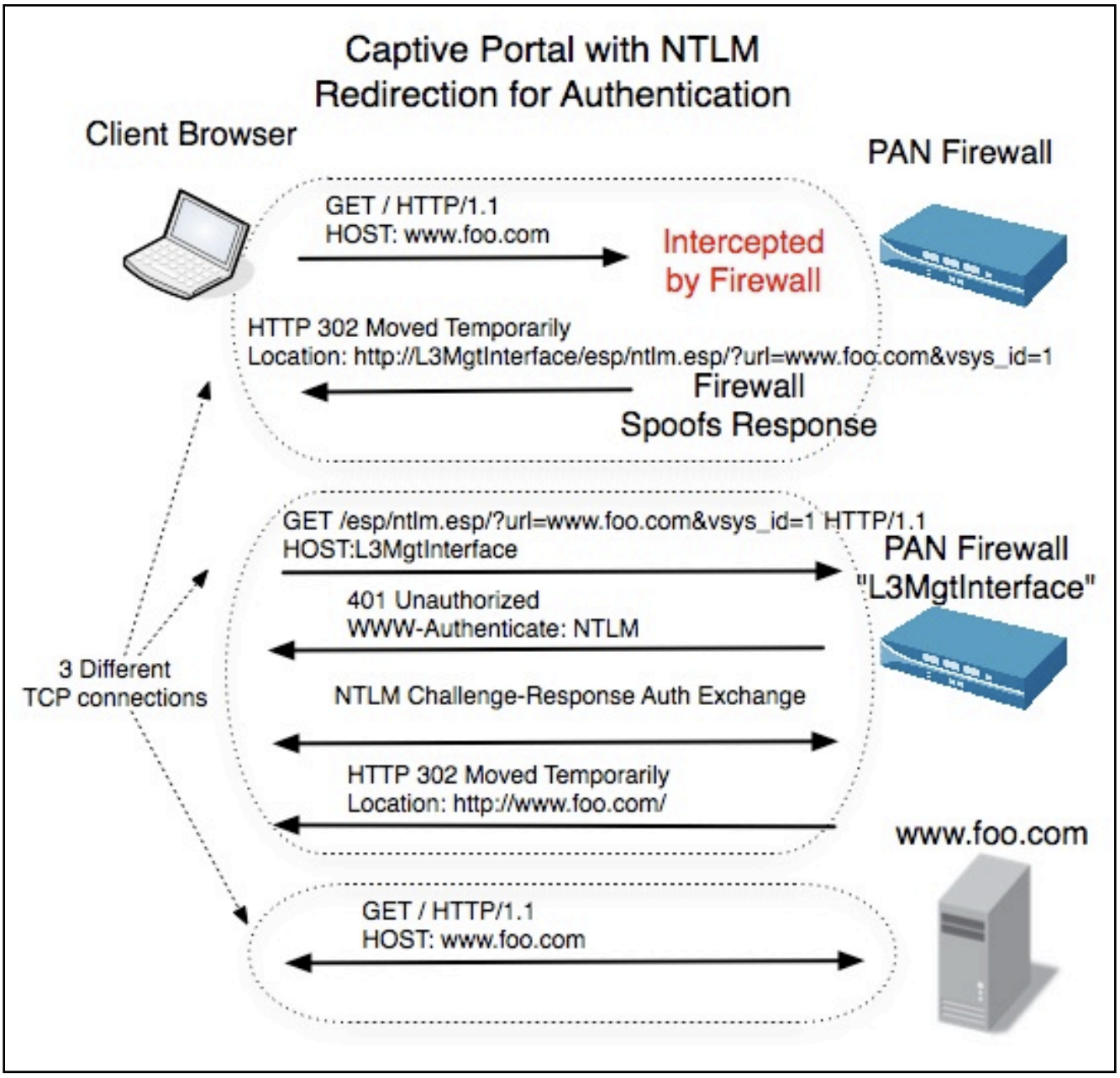
In the diagram on the next page, we see the Client Browser send an HTTP GET requests to the webserver. Instead of returning the requested webpage, the webserver tells the client the user does not have access to the requested webpage (401 Unauthorized), and that if the browser would like to gain access, it must authenticate (WWW-Authenticate: SCHEME) with the particular scheme specified by the server. The client re-sends the original GET request with pertinent authentication information for the authentication scheme.



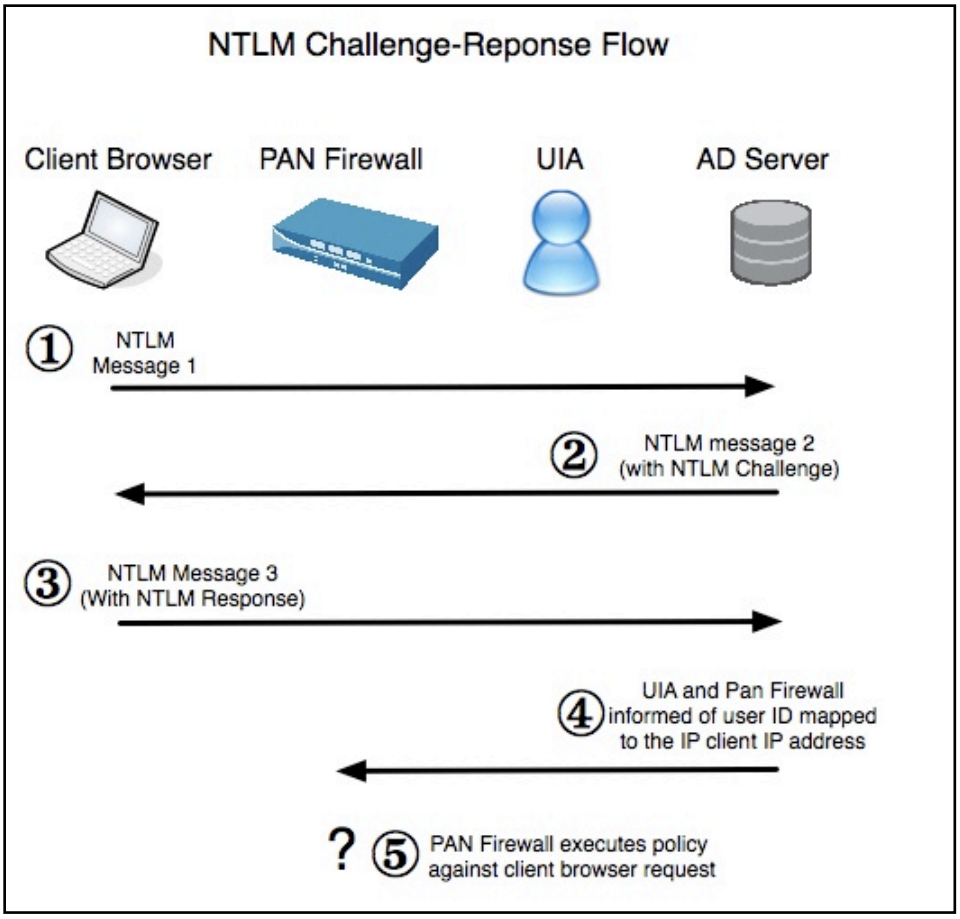
Redirection Mechanics

PAN-OS uses HTTP headers (previous page) in conjunction with the HTTP 302 Moved Temporarily server response. Together, a PAN device can redirect users to a temporary webserver purely for the sake of authenticating.

The diagram below walks through the sequence of steps that take place when the Authorization/ WWW-Authenticate headers successfully identify users. There are three distinct phases, which correspond to the three TCP connections that take place: the original (intercepted) request; the NTLM authentication between client and firewall; and the original request, resent.



The diagram below shows detail on the NTLM Challenge-Response exchange mentioned in the diagram on the previous page. Note that the exchange flows through four devices in total, to complete the transaction.



Defining the Hostname

As in the diagram on the previous page, PAN-OS can request user credentials from browsers.

When specifying hostname, keep the following PAN-OS requirements in mind:

- Hostname must resolve in DNS to an inline management interface on firewall.
- Firewall inline management interface must allow HTTP management traffic.
- Users must have a route to the inline management interface.

When defining the NTLM Authentication hostname on the firewall, it should *not* be fully qualified, but rather contain just the hostname itself, without any subdomains or domains attached. The hostname specified must not contain a period. Internet Explorer will only participate in NTLM authentication if the requesting server is in the same intranet domain. Microsoft verifies the browser and server as in the same intranet domain if the destination server does not have a period in the hostname.

NTLM, Versions 1 & 2

A number of different schemes exist to use with the WWW-Authenticate and Authorization headers, however just the NTLM scheme is offered in PAN-OS.

NTLM is a challenge-response authentication mechanism, where the client must take new information from a server when formulating its password response. As the Active Directory server is the only server able to validate the NTLM response from the user, the webserver acts as a conduit, forwarding the NTLM challenges and responses. In the case of PAN-OS, the challenges and responses are sent to User Identification Agents, which contact the AD server.

Being a challenge-response authentication scheme, NTLM is resistant to replay attacks. However, as the design of NTLMv1 is flawed (offering a field of only 2^8 possibilities, instead of 2^{14}), making it vulnerable to password cracking attempts when the challenge and response have been captured, NTLMv1[2] is never recommended. Only the stronger, NTLMv2 (with 2^{14} possibilities) is recommended.Browser Support

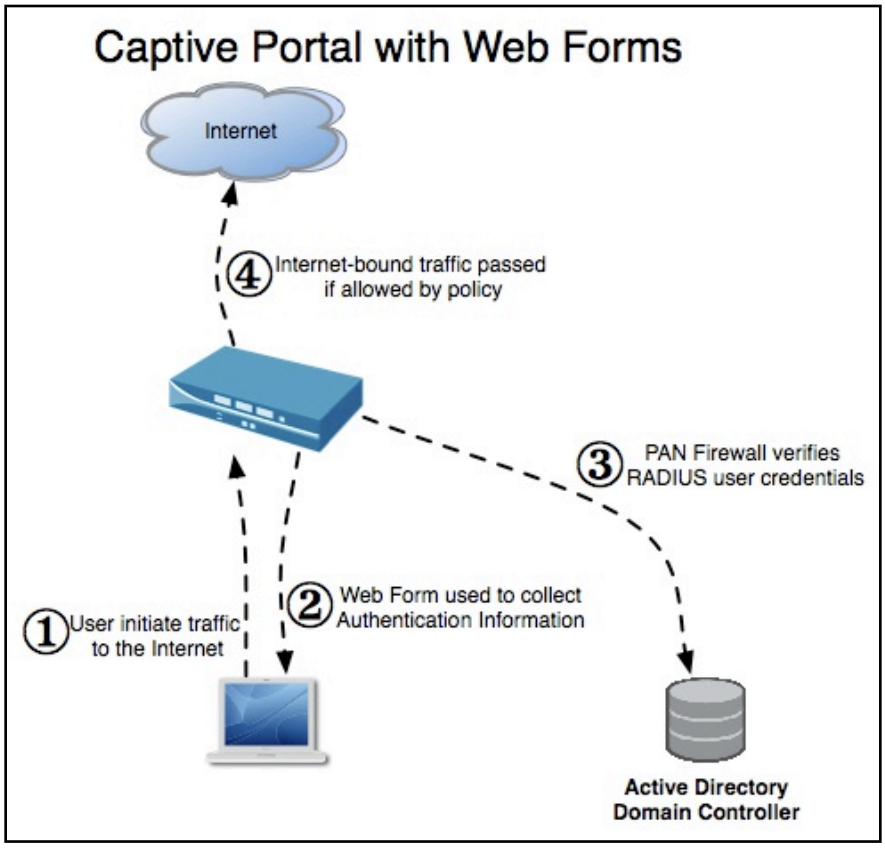
Unlike simpler authentication schemes like the basic authentication (where the username and password are sent in the clear, but base 64 encoded), NTLM is not universally available in browsers. NTLM authentication is enabled by default with Internet Explorer, and is configurable with other browsers like Firefox. Support and configuration among them vary.

With Internet Explorer, NTLM login credentials can be sent to any webserver considered in the browser's Intranet zone. Intranet zones, by Microsoft's usage, are servers without any 'dots' in the servername.

For Windows Firefox, the attribute *network.automatic-ntlm-auth.trusted-uris* should be filled in with the webserver hostname that will be requesting NTLM authentication. To set this hostname, type in **about:config** into the URL window of the browser and type **ntml** into the filter window to find this attribute. If the attribute above is not set, an authentication pop-up will appear, prompting the user for their domain\username and password.

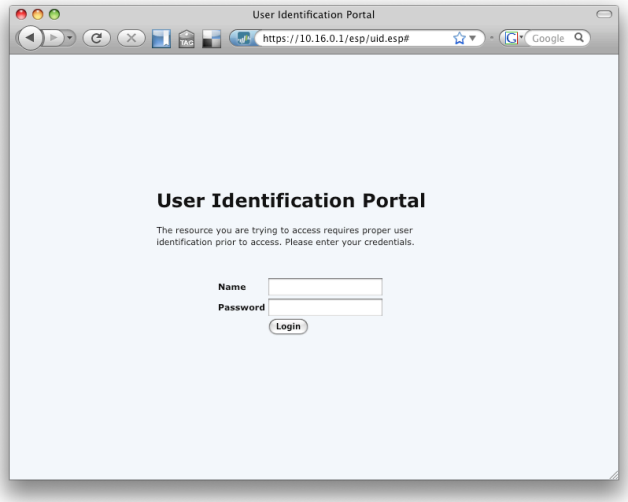
[2] $2^7 + 2^7 = 2^8$ whereas $2^7 \times 2^7 = 2^{14}$. An oversight in NTLMv1 yields the former, while NTLMv2 yields the latter.

Captive Portal with Web Forms



For users left unidentified by the previous two methods, Captive Portal with Web Forms can be used to present an HTTPS-encrytped web form to collect domain user information. The Palo Alto Networks firewall then checks with the Active Directory server via the RADIUS[3] protocol to verify the identification. Unlike Captive Portal with NTLM, this method works with any browser. The diagram below shows the scheme.

To receive the form, users must use a web browser and be in the process of connecting to an unencrypted (HTTP) page. On successful authentication, users will automatically be directed to the website originally requested if allowed by policy. Once identified, policy based on the user information is executed for any applications passing through the Palo Alto Networks firewall by the mapped IP address, not just for browser-based applications.



The default web form presented to users is shown to the left. For more information on customizing the web form, see the Palo Alto Networks Tech Note entitled Customizing Block Pages.

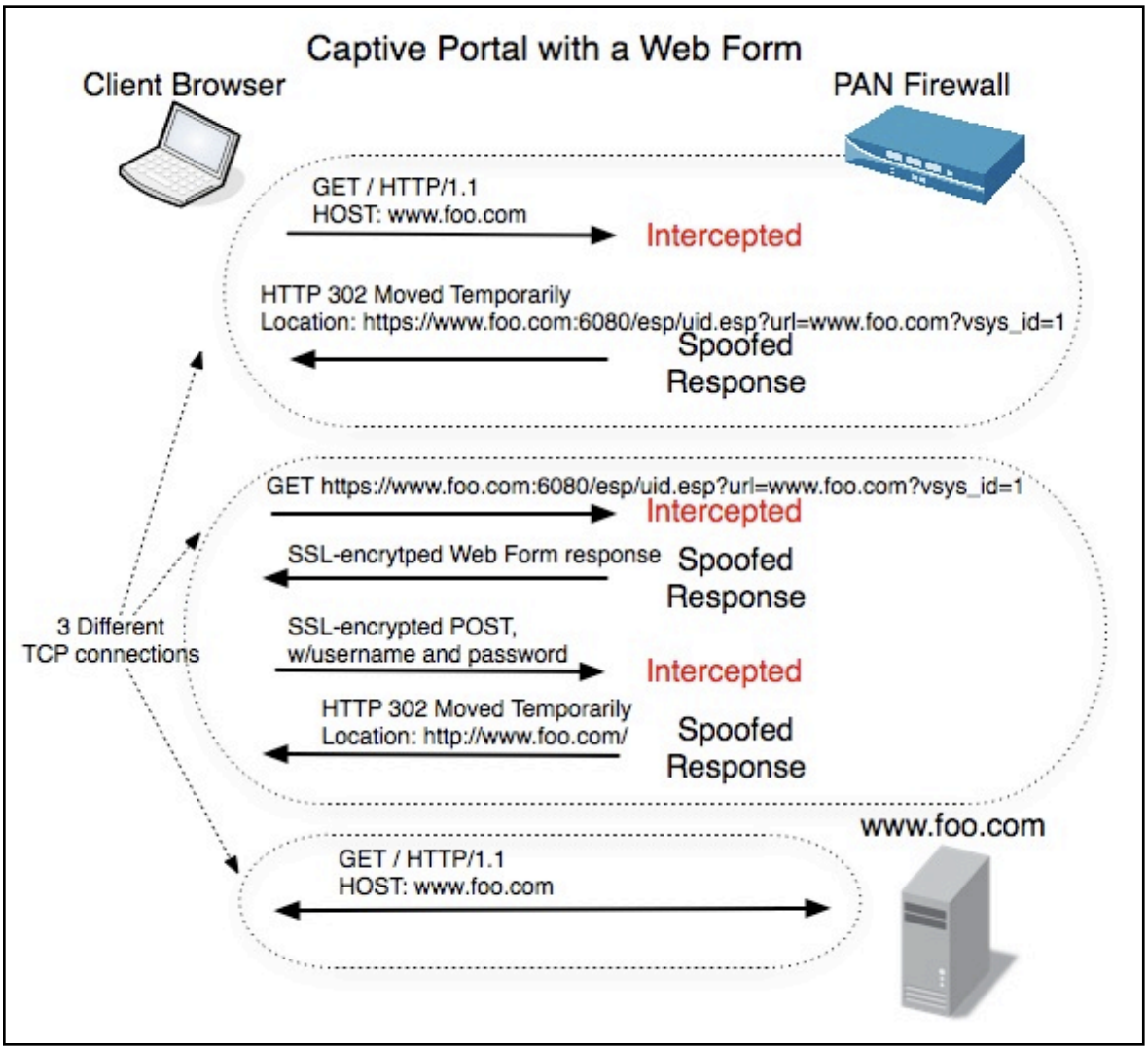
[3] Captive Portal was designed to work with an Active Directory server through its RADIUS interface. If another RADIUS server is used, policy creation is possible, but will be challenging as there is no way to browse a list of existing users. In addition, the RADIUS interface does not make user group information available.

Redirection Mechanics

PAN-OS takes advantage of HTTP 302 Moved Temporarily responses, but in a different way than the Captive Portal with NTLM method. As seen in the diagram depicting the process below, the browser first sends a request for a desired webpage.

In this example, the requested URL is HTTP://www.foo.com/ The firewall does not have a mapping for the requesting client IP address to a user, so it crafts a response to the original request, as if the response came from the specified server. Instead of the actual contents, the firewall sends an HTTP 302, directing the user to a URL similar to the original one, but with HTTPS and to port 6080. This serves as a trigger for the firewall to intercept the next request form the browser, where it responds with a web form page. Not shown in the diagram is how the firewall relays the username and password enclosed in the user's web form response to the RADIUS interface of AD or a standalone RADIUS server. If the RADIUS server finds the user information correct, policy is executed on traffic when the user finally re-sends the original request.

Similar to the other methods, any IP-based traffic originating from the client IP address will be associated with the identified user, until the entry has timed-out. At that point, if the user is still actively using a browser, the sequence will be re-initiated.



Nuances

SSL Certificate Issues

Only the Captive Portal with Web Forms method uses SSL certificates. This process will generate SSL browser warnings. There are three common SSL browser warnings:

- Untrusted Issuer
- Hostname Mismatch
- Expired Certificate

The certificate uploaded to the PAN firewall for web gui management is also used to sign the login page presented to user with this method. If users do not trust the CA that signed the certificate, or the certificate is self-signed, users will see the Untrusted Issuer browser error. This can be fixed by installing a certificate signed by a local CA trusted by the user browser, or installing the firewall certificate in the browser.

In addition, as the server in the URL requested by the user will not match the server certificate hostname, users will see the Hostname Mismatch browser error. In PAN-OS 2.X, there is no workaround to avoid this error.

User Mappings Aging-out/Timeouts

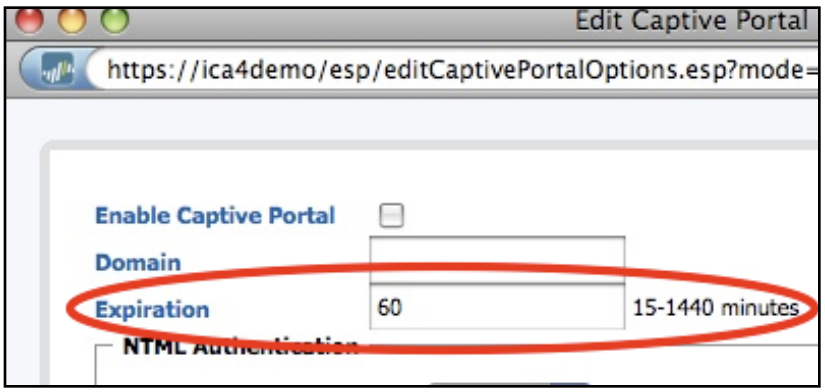
While the UIA has a number of timer settings to coordinate and manage all of the processes necessary to accurately map users to IP addresses within a domain, PAN-OS also has its own table mapping users to IP addresses. This table is populated from the UIA and both Captive Portal methods.

The current table can be viewed from the CLI of the firewall, as in the example here:

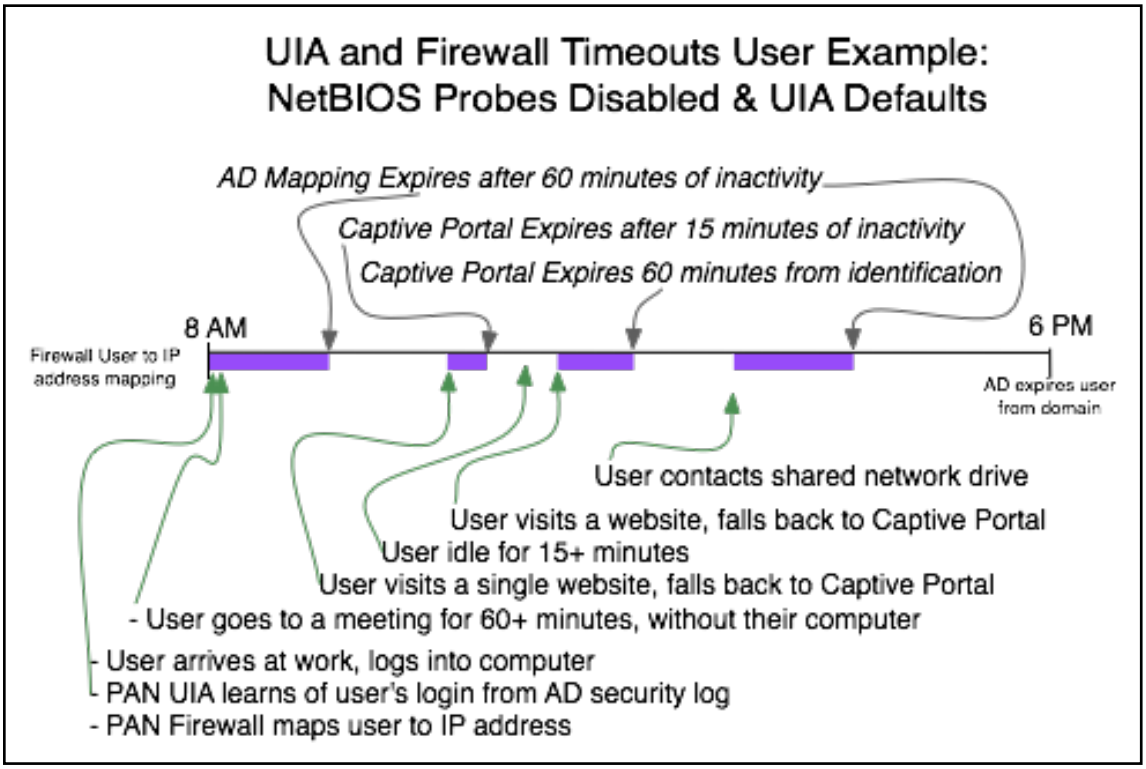
```
test@panos> debug dataplane show user

IP              Ident. By User                            TTL (s) Max. TTL (s)
--------------- --------- ------------------------------- ------- ------------
10.154.172.76   AD        jaugustus                       2949    2949
10.154.90.109   NTLM      lstockton                       889     889
10.154.20.148   CP        dchinn                          720     720
10.154.126.204  AD        mgallagher                      519     519
```

The first TTL time listed is an inactivity timer. If no activity is seen from the IP address after 15 minutes (900 seconds) for either Captive Portal methods, the entry will be removed. The second TTL (Max TTL) refers to the time when the entry will be removed. For Captive Portal methods, users will be redirected for identification once this Max TTL timer expires. For Captive Portal, this value can be changed in the web interface under **Device → User Identification → Captive Portal**.



Below is an example of three different timeouts that go into effect with the PAN-OS user to IP address mapping. The example used the default UIA timeouts (45 minutes for users), no NetBIOS probes, and one of the Captive Portal methods.



Agent with Active Directory

The UIA is set to expire user to IP address mappings every 45 minutes by default, but it is highly advisable to change this to the same timeout used by the AD server on user Kerberos tickets. The default value for AD servers is 10 hours.

When NetBIOS is not used or is ineffective, the entries expire from the UIA before the age-out timeout under the following circumstances:

- The Domain Controller (DC) security log lists a different user logged in from an IP address currently assigned to the another user. The new user takes precedence.
- The DC session table lists a different user for an IP address currently mapped by the UIA to another user. The new user takes precedence.
- No updated information from either the DC session table or security log for the user before age-out timeout

When the IP address in question does respond to NetBIOS probes, the entry is held until a NetBIOS probe either does not return, or returns with a different user. NetBIOS probes can only cause a user to be removed from the mapping.

The Agent with AD method does not have visibility into when users are logged off from the domain, however, if a new domain user logs into a computer, the UIA will immediately be aware of this change and inform the firewall.

Directory Support & Limitations

The User Identification Agent only supports Active Directory.

RADIUS servers can be used with Captive Portal and Web Forms, however, no group information will be available, and any policies specifying individual users requires manual input of needed users.

As there can often be times when users to gain access to the network without authenticating to Active Directory or their browsers are not active, it is important to create rules for unauthenticated users. Depending on the size and make-up of this population, appropriate policies will vary.

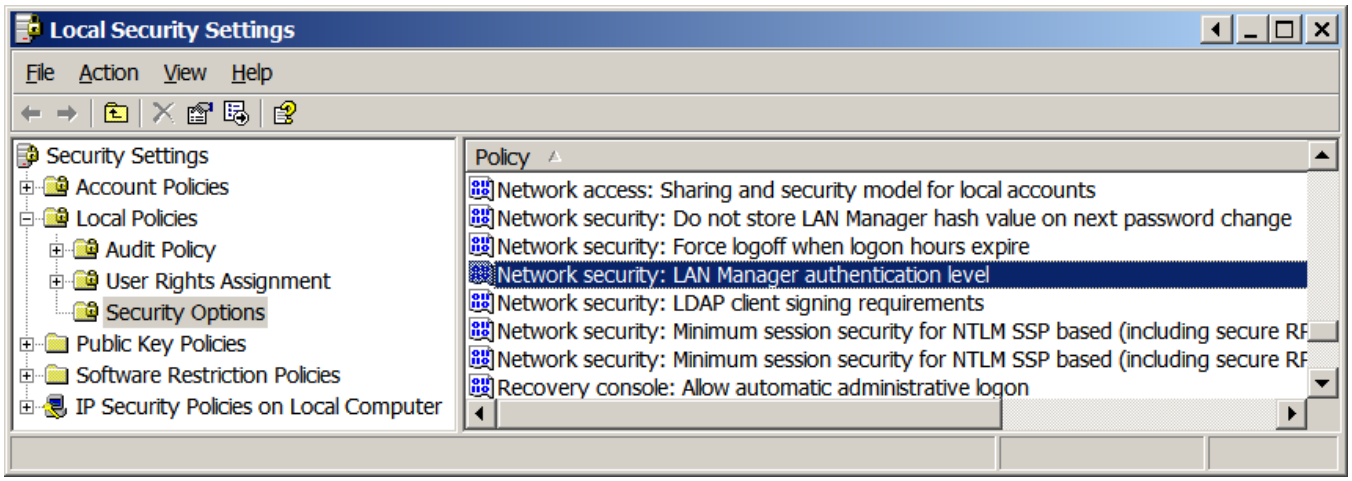
Part II : Configuration

AD Server Configuration

Disable NTLMv1

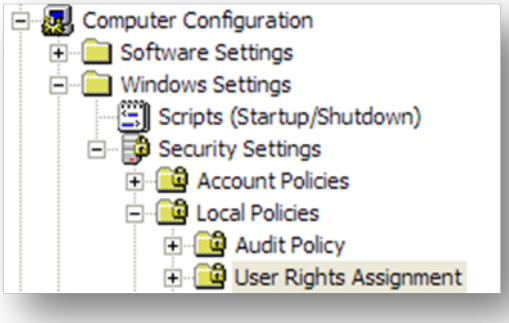
NTLMv1 should never be used. On the Windows member server the UIA will be installed on, verify that NTLMv1 is not allowed.

On each domain controller in the domain, go to **Control Panel → Administrative Tools → Local Security Policy**, find **Local Polices → Security Options** and click on Network Security: LAN Manager authentication level. Select Send NTLMv2 response only\refuse LM as and attribute.

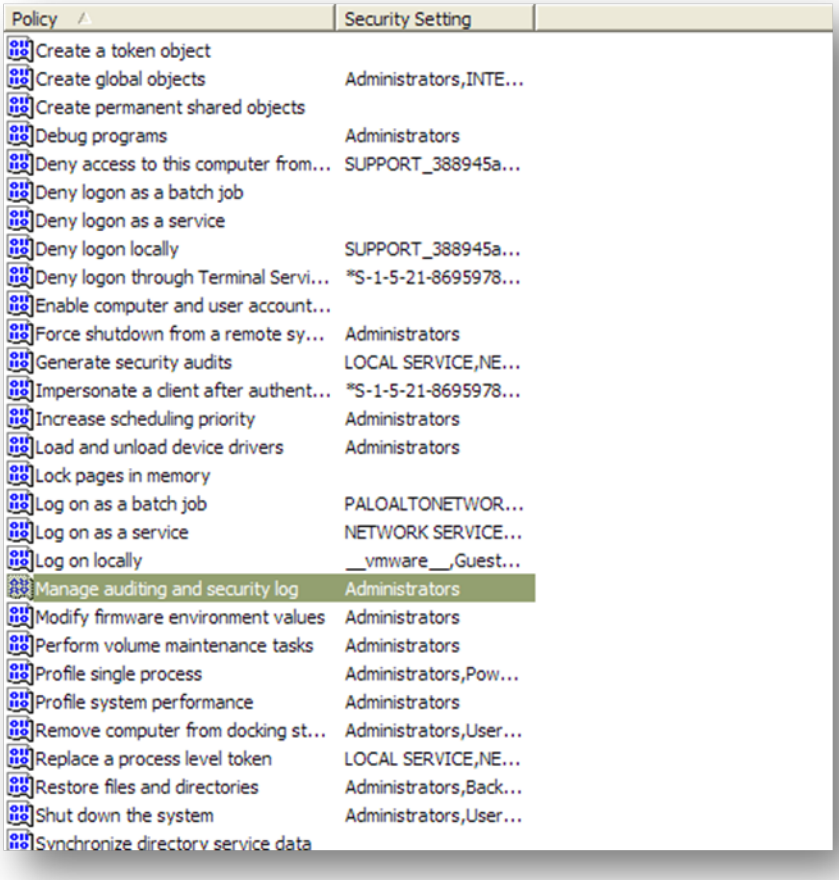


Read Access to the Security Log

The User Identification Agent requires access to the Windows security log to check for user login events. By default only an administrator has this level of access. To give the UIA user account or group read access to the security log, they will need to have the Manage Audit and Security Log user right. This right is assigned through Group Policy. It can be found in the **Computer Settings → Windows Settings → Security Settings → Local Policies → User Rights Assignments.**



The UIA user or the group that the UIA user is part of needs to be added to the "Manage Auditing and Security Log" right. This group policy object will need to be applied to all of the domain controllers that the UIA will be connecting to.



Agent Installation and Configuration

The UIA must be installed for Agent with Active Directory or Captive Portal and NTLM. It is optional (but recommended) with Captive Portal with Web Forms.

The user identification agent requires the following:

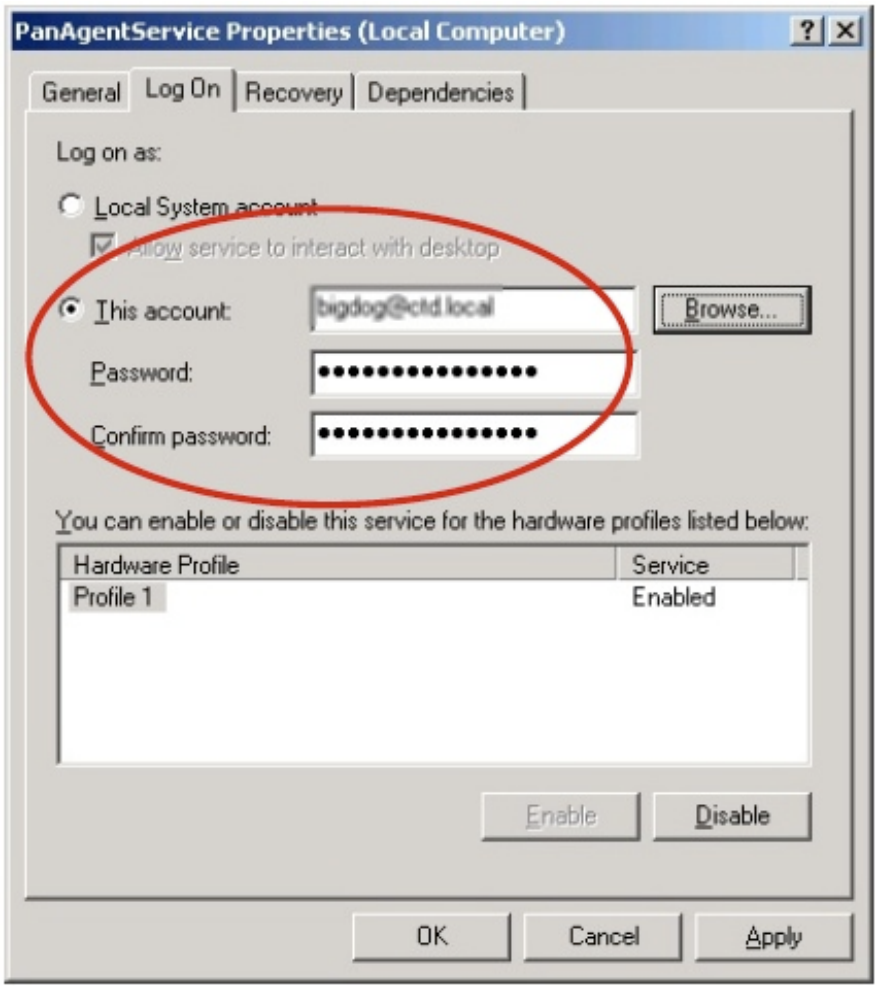
- Hardware: any PC or server with a minimum 2.4GHz CPU, minimum 1GB of memory, and minimum available hard drive space of 100MB
- Software: any server running Windows 2003 server
- Active Directory access: it must run as a user with read access to a Domain Controller (e.g. user account that is a member of the Domain Users group).
- Domain Controller Security Log access: It must run as a service with read access to the Security Logs of the Domain controllers, as noted on the previous page. This requires the User Account Right : “Manage Auditing and Security Log”. The only default Windows group with this right is the Administrators built-in group.
- Installation: It can be installed on a dedicated device or on a Domain Controller

Detailed information about UIA installation and configuration is also included in the PAN 2.0 Administrator’s Guide. The User Identification Agent and Administrator’s Guide can be downloaded from the Palo Alto Networks support site with a valid support account.

UIA Installation

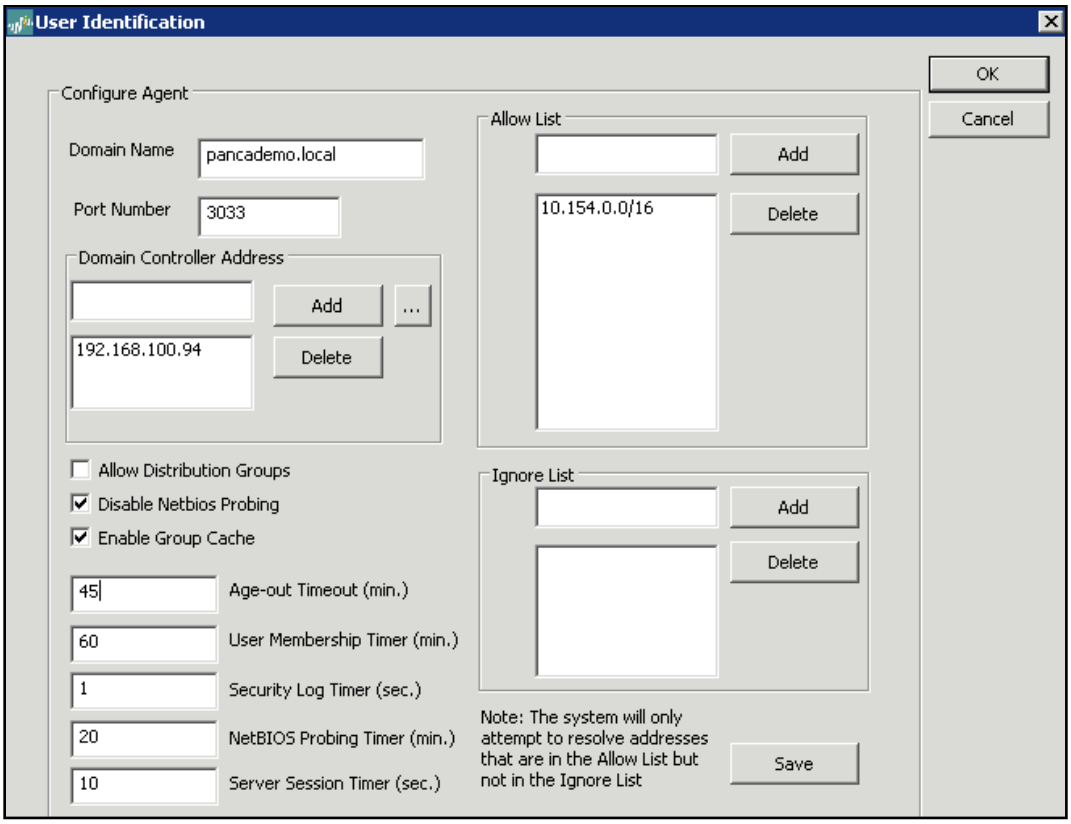
To install the software, follow these steps:

- Install the User Identification Agent by running the Windows installer downloaded from the support site. Follow the installation steps (choose to install for all users when asked).
- Once the UIA has been installed, open the properties for the *PanAgentService* via **Control Panels → Administrative Tools → Services**. Enter the appropriate login information into the "This account" section of the **Log On** tab. An example of this is below.



UIA Configuration

Launch the UIA (**Start → Programs → Palo Alto Networks → User Identification Agent**). Select the Configure button on the right side. A window like the below should appear.

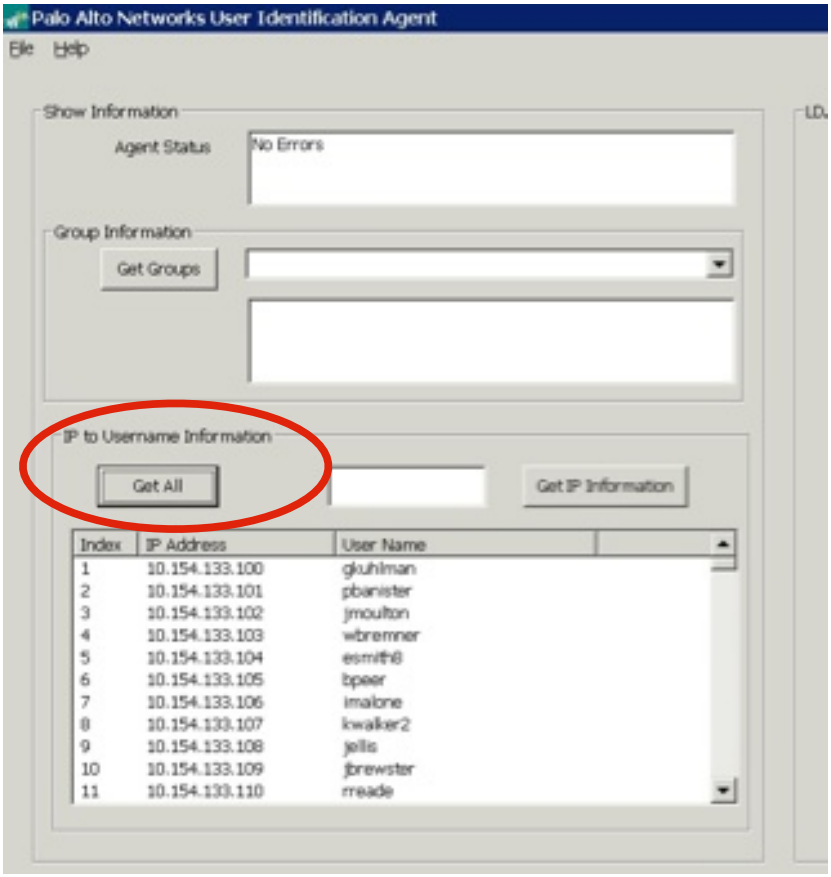


- Fill in the **Configure Agent** section:
  - **Domain Name:** DNS domain, not AD domain
  - **Port Number:** be sure to enter the same port here and in the device configuration
  - **Domain Controller Address:** add the IP address of each Domain Controller you want the agent to get information from
- Fill in the **Allow List**: the UIA will only map IP addresses included in the allow list. add the subnets (e.g. 10.0.0.0/24) or hosts (e.g. 10.0.0.1/32) you would like to have the system try to correlate user and IP information. By specifying the subnets or hosts to correlate user and IP information, you limit the IP addresses that the agent will try to resolve using NetBIOS. For this reason it is important to only enter IP addresses on your network in this field.
  - **Ignore List:** add subnets or hosts that should not be correlated. (e.g. terminal servers, subnets or IP addresses used by NAT, etc.)
  - Click **Save** to make the configuration active

Note: For any correlation to happen, some addresses need to be entered in the Allow List. By default, no addresses are correlated. the UIA will function, but no users will be mapped to IP addresses.

A number of timeouts govern the User Identification Agent. Below is a description of the timeout options available for configuration.

- **Age-out Timeout (min.):** how long entries in the IP to username cache kept by the agent are valid. Current entries can be viewed from the main User Identification Agent Screen under IP to Username Information, as in the graphic below, 45 minute default



- **User Membership Timer (min.):** how often the agent contacts the AD server for group membership information, 60 minute default
- **Security Log Timer (sec.):** how often new user logins are detected by reading the security log on the AD server, 1 second default
- **NetBIOS Probing Timer (min.):** how often the agent will issue NetBIOS queries to desktops, 20 minute default
- **Server Session Timer (sec):** how often additional **user → IP adderss mappings** are derived by reading the session table of active resources on the AD server, 10 second default

The user identification agent is now installed and the device ready to be configured.

Note: Any changes to the timeouts and timers on the configuration screen will restart the PanAgent service. This can affect operation for installations with large security logs to be processed.

Multi-Server, Multi-Agent, or Multi-Device

To configure the setup for multiple Domain Controllers (but with one agent and one device), the previous configuration steps should be augmented in the following ways:

- Configure the User Identification Agent to talk to two or more Domain Controllers. This is accomplished by adding the IP address of each Domain Controller to the Domain Controller Address list in the agent.

To configure multiple User Identification Agents (one for each Domain Controller, for example), the configuration steps should be augmented in the following ways:

- Install multiple User Identification Agents, repeating the installation steps for each.
- Configure the Palo Alto Networks device with multiple User Identification Agents. Simply repeat the steps for the single agent configuration.

To configure multiple devices to talk to one or a common set of User Identification Agents, the configuration steps should be augmented in the following ways:

- Configure each Palo Alto Networks device to communicate with the same User Identification Agent(s) by adding each agent on the User Identification page of the Device tab in the web interface.

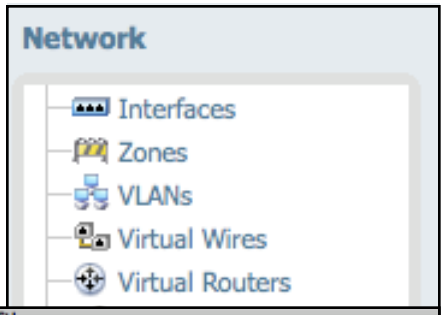
Device Configuration

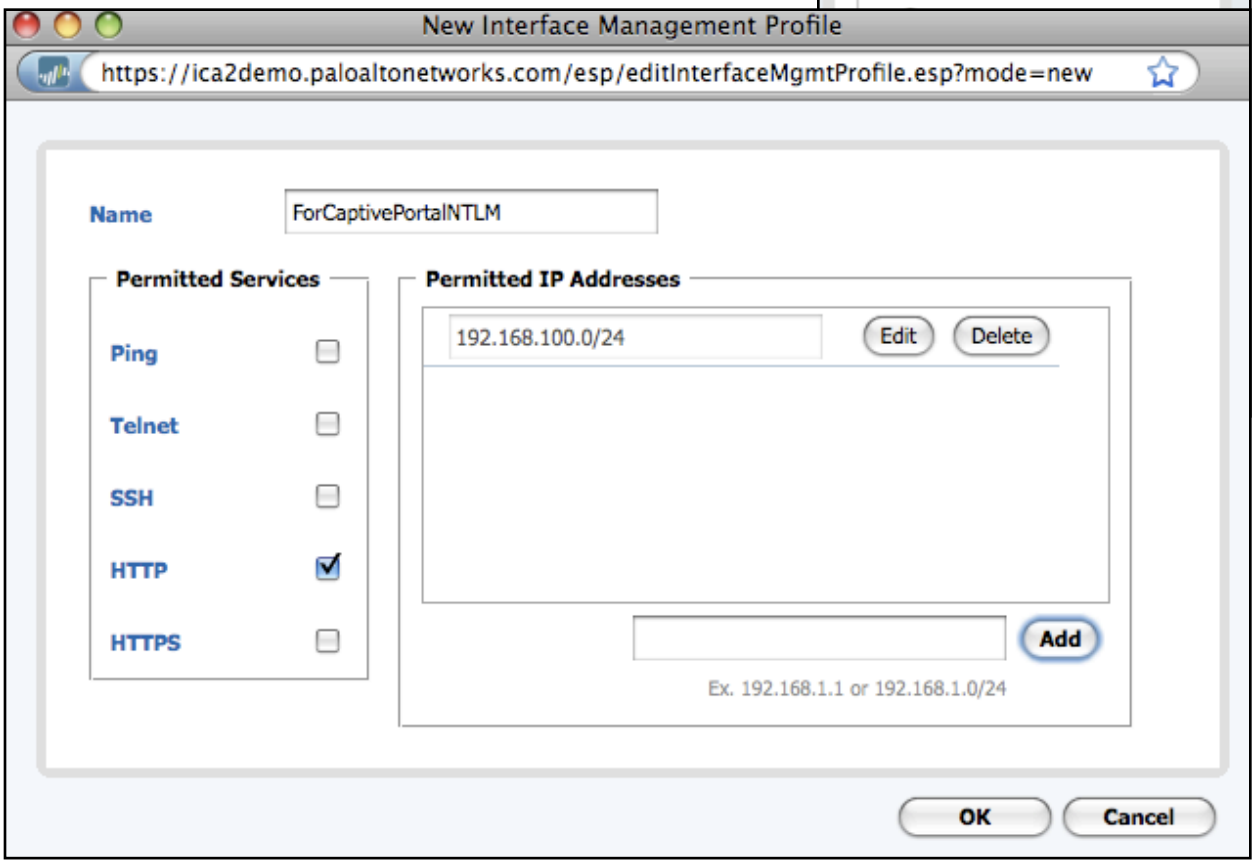
L3 Inline Management Interface

If using the Captive Portal with NTLM method, you must configure an L3 (layer 3) interface on the firewall with inline management.

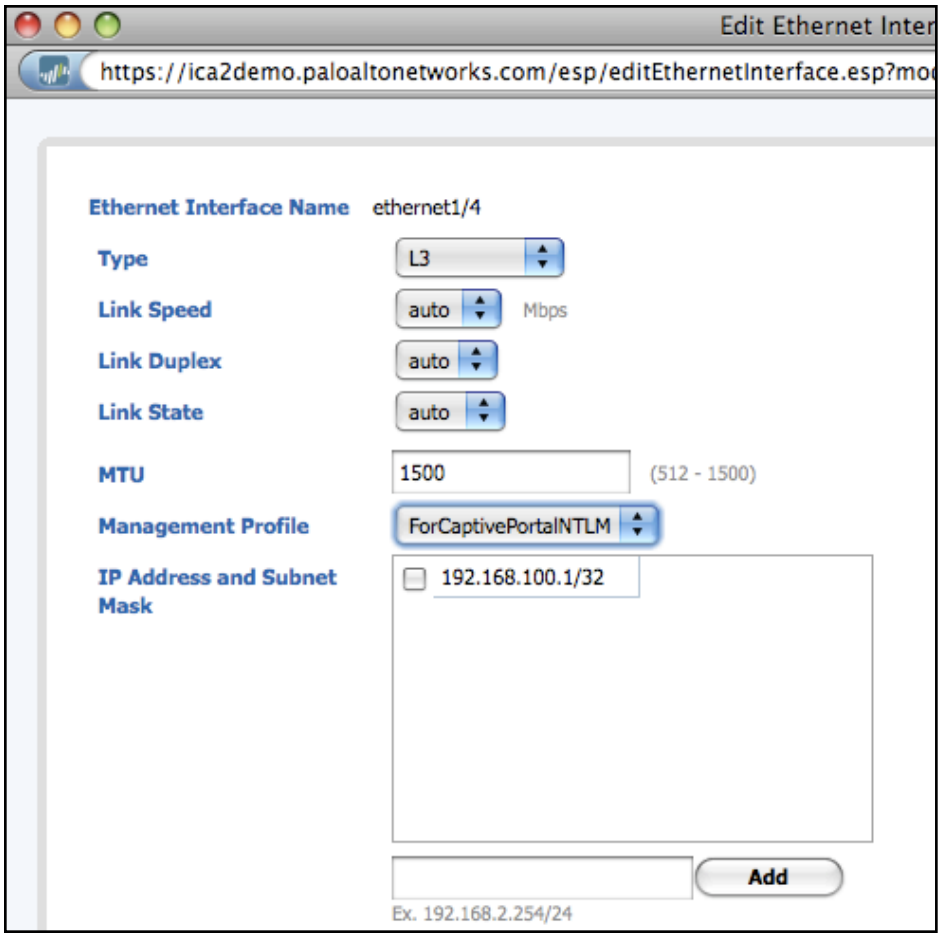
To set this up:

- Define at least 1 Layer 3 (L3) interface on the firewall
- Define an Interface Management Profile in the Network Tab with at least the HTTP management service permitted, with the IP addresses for client browsers listed in the Permitted IP Addresses field.





- Configure an inline management IP address on the target L3 interface, selecting the Interface Management Profile created in the previous step.



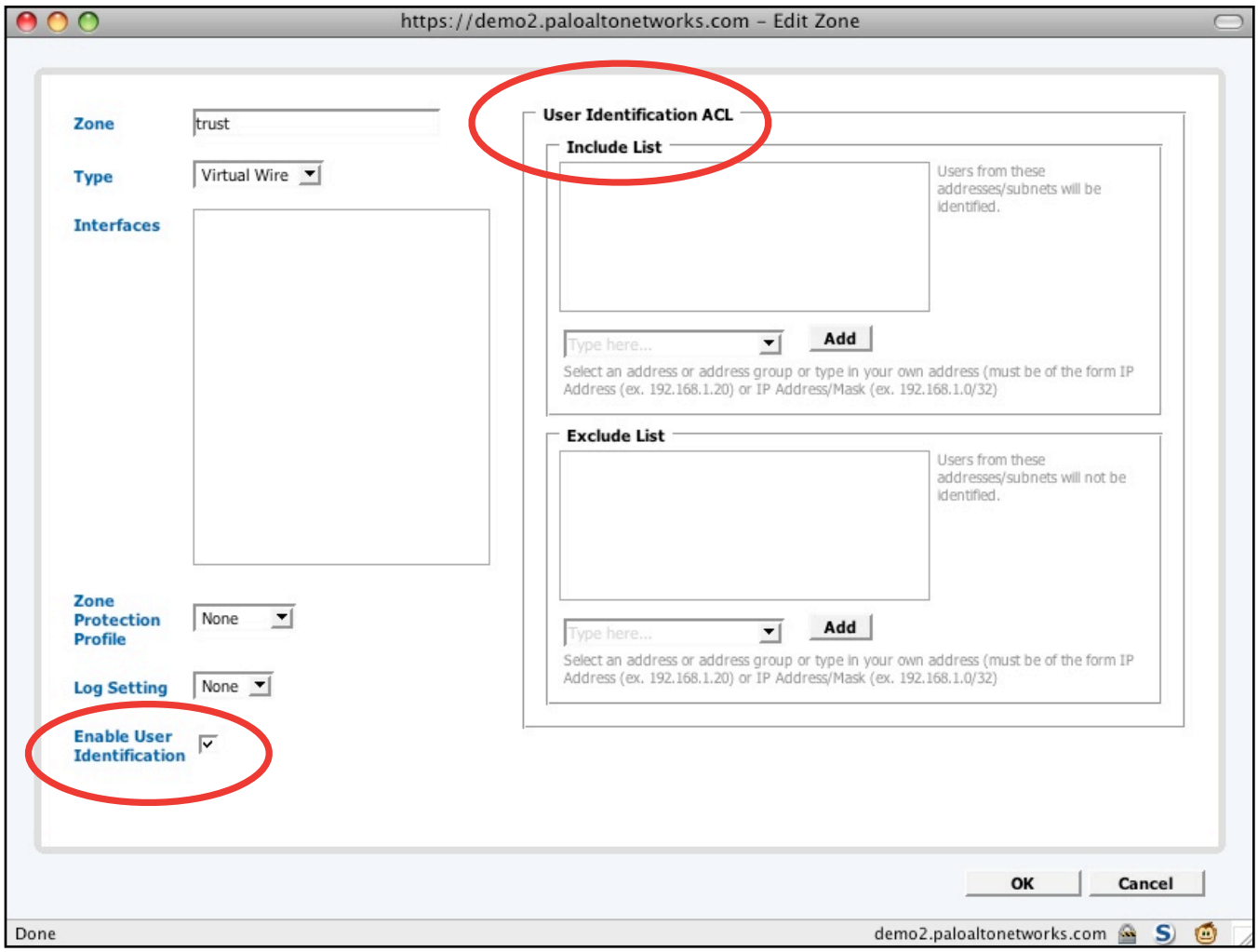
Aside from the firewall configuration, make sure:

- a DNS hostname entry for the inline management IP address exists and resolves
- user traffic has a route to the management IP address

Enable Security Zone for User Identification

By default, user identification is disabled. Once enabled, rules with user identification can be committed to the device.

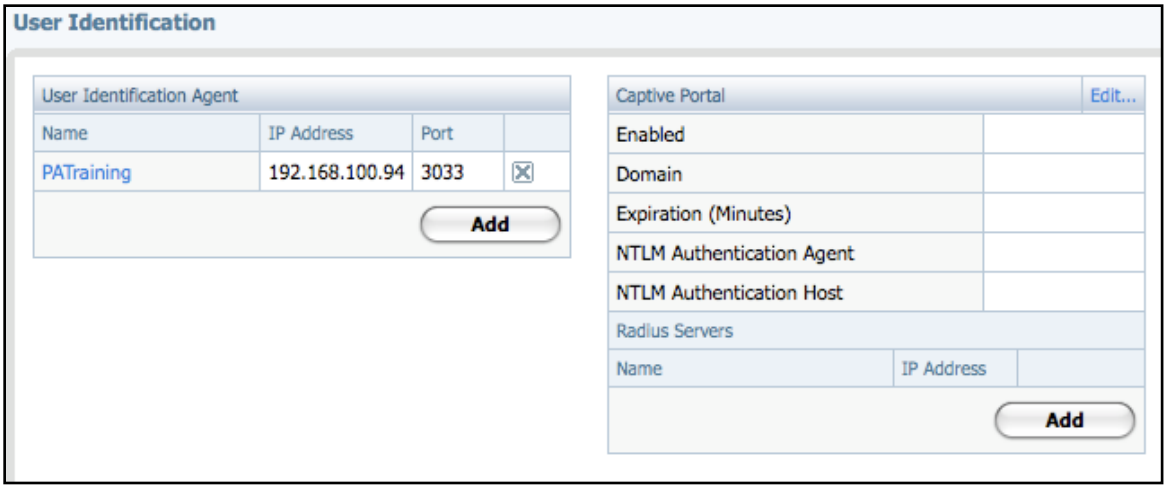
To use any form of user identification as discussed in this document, the source security zone for rules must have user identification enabled. This can be done through the web interface via **Network → Zones**. Select a given zone, and a screenshot as on the next page will appear. User Identification **must** been enabled here. To further limit the subnets or addresses checked for user identification, ACLs (access control lists) can also be enabled, as seen on the right side of the graphic below. Servers are commonly added to the exclude list.



UIA and Radius Server Setup

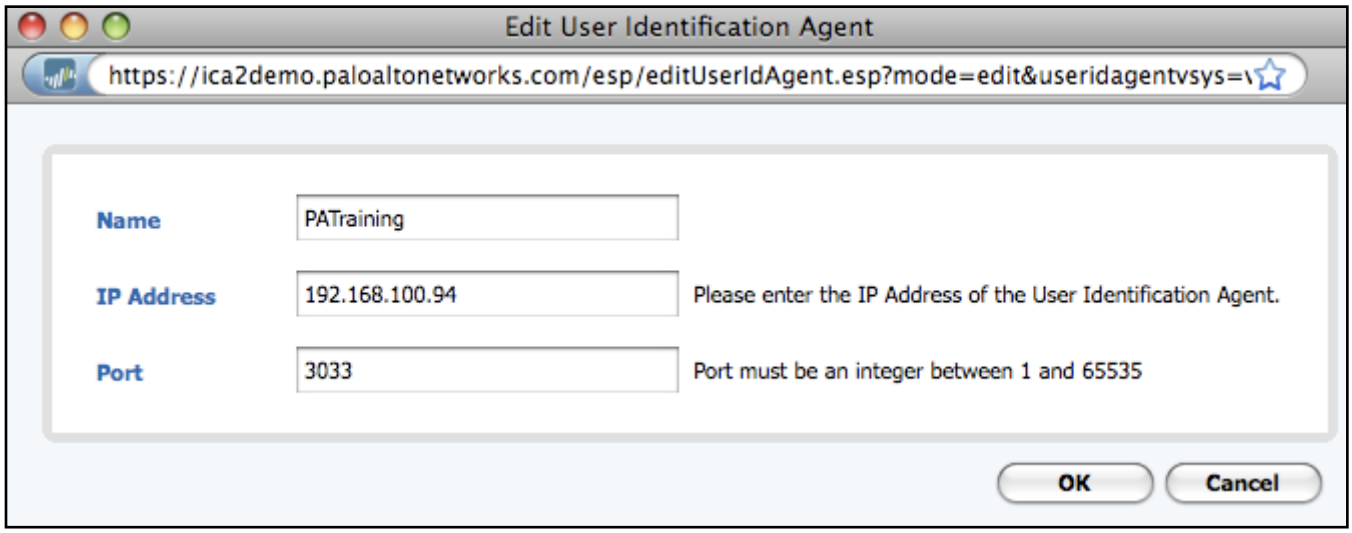
To configure the PAN device to communicate with the UIA, follow the directions below for the applicable method via the web interface.

- Click on the **Device** tab (rightmost tab).
- Click the **User Identification** option on the left. You should see the User Identification information, as on the next page, but with no agents defined.



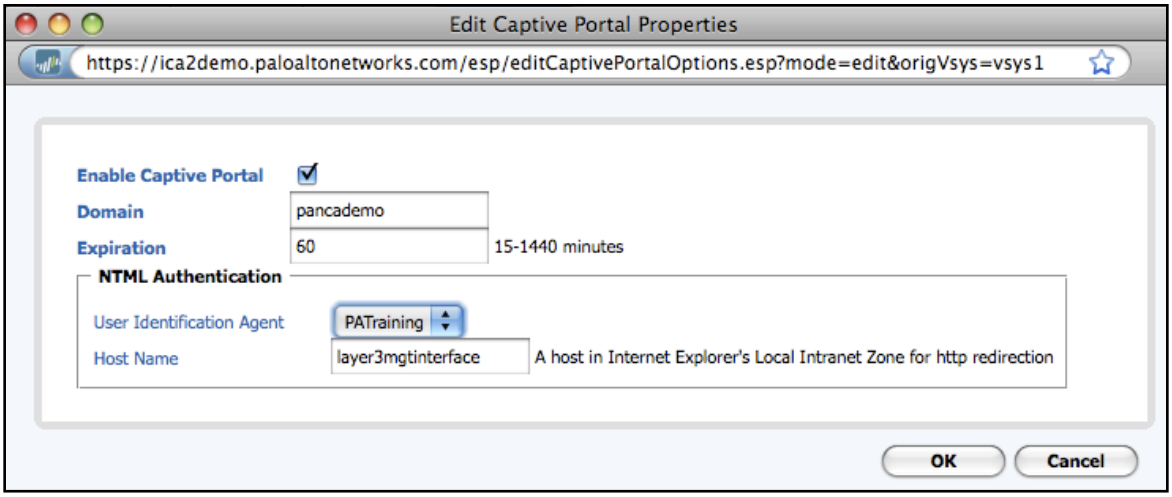
Agent with Active Directory

- Under the User Identification Agent box, select **Add** and a screen like the one below will appear. Enter the agent name, IP address, and port number to use. The name can be any name, but the IP address and port number must match the agent configuration.



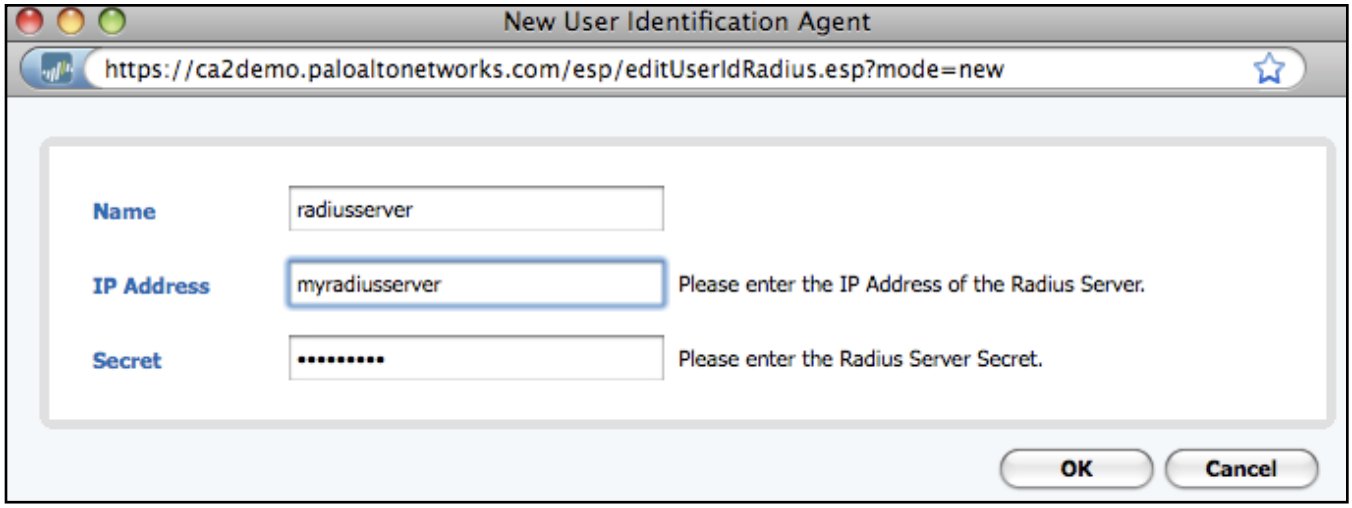
Captive Portal with NTLM

- Define the UIA as in the entry above.
- Under the Captive Portal section, click **Edit** and a screen like the one on the next page appears. Click the **Enable Captive** Portal box, select the previously defined (above) User Identification Agent, and enter in the DNS-resolveable hostname (no periods!) into the Host Name field.



Captive Portal with Web Forms

- If using an AD, define the UIA as on the previous page.
- Under the Captive Portal section, click **Add** to add a Radius Server. Fill in a name for the server, the IP address for the RADIUS interface of the AD server, and the RADIUS server secret.



HA Considerations

If deploying the Palo Alto Networks device in a high availability pair, no additional steps are required to configure the user identification agent and Captive Portal. The configuration is synchronized; the HA protocol will manage the synchronization of user information

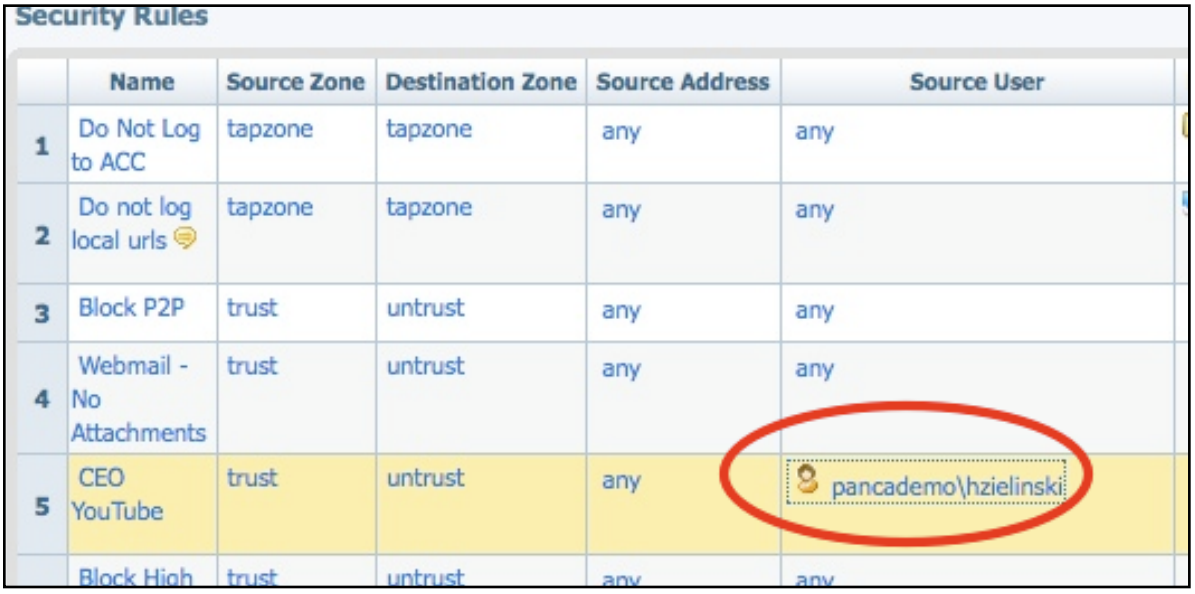
Policy Configuration

Once the associated servers, interfaces, and zones have been configured, policy can be written for user identification. The table below lists the required rules per method.

Method	Rules Required
Agent with AD	• Security Policy Rule
Captive Portal with NTLM	• Security Policy Rule • Captive Portal Rule
Captive Portal with Web Forms	• Security Policy Rule • Captive Portal Rule

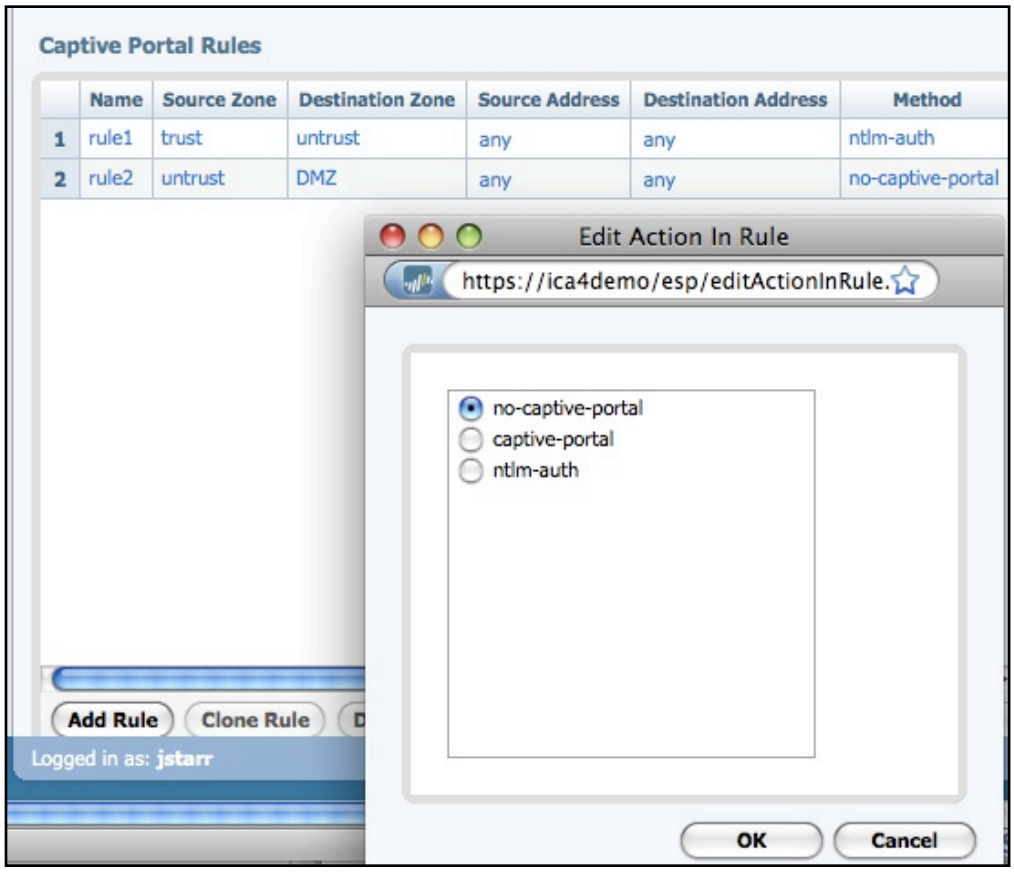
Security Rules

As long as the zone (below named trust) has been enabled for user identification, rule number 5 below is valid. Just define users the applicable user and the desired action.



Captive Portal Rules

With Captive Portal, rules must be added to the Captive Portal rulebase **before** Security Policy rules pertaining to those users go into effect. This step is not necessary when using the Agent with AD method.



Only the last column, Method, is unique to the Captive Portal rulebase. It is possible to control which users on different networks and zones will see the different Captive Portal methods in effect.

With Captive Portal defined, the firewall will be able to apply security policies to these users.

Browser Configuration

If Captive Portal with Web Forms is used, the certificate from the firewall web management interface should be installed or signed by a CA (certificate authority) the browser trusts.

When using Captive Portal with NTLM on Windows Firefox, the attribute *network.automatic-ntlm-auth.trusted-uris* should be filled in with the webserver hostname that will be requesting NTLM authentication. To set this hostname, type in **about:config** into the URL window of the browser and type **ntml** into the filter window to find this attribute. If the attribute above is not set, an authentication pop-up will appear, prompting the user for their domain\username and password.

Part III : Maintenance &Troubleshooting

Verifying Correct Operation

With the above steps complete on both the device and the agent, **IP address → user → user group** information will now be populating in the Palo Alto Networks device. There will be a period of time while the identification gets primed before complete identification results are seen. Upon startup, the agent will connect to the Domain Controller and download the security log. This log can be as large as 4GB but the default size is 16MB on Windows Server 2003. When the agent is installed on a separate machine, network transfer time will add to the initial processing time. Once the agent has the log, it can analyze approximately 2 MB/sec on an average PC. User identification results in the logs will be sparse until this process has completed.

As an example, 100MB log file might take 15 seconds to transfer from DC to agent, followed by 50 seconds to process the data. This results in no significant identification being available for at least a minute after the agent service started and connected to the Domain Controller. If the log file is set to the maximum size, it could take over 40 minutes to prime.

Even after the log file has been processed and the agent has been primed, there will likely be a number of existing sessions that were started before the agent was ready which will not have a user associated with them. These sessions could end seconds, minutes, or hours after the agent was setup. After startup, if there are a number of long lived sessions in the logs that have no user identification, do not be alarmed - this is normal.

Once primed, the agent should be in a steady state where the logs accurately report users and session active in the domain. Addresses without users associated with them after this point will be due to:

- non-Windows machines
- Windows machines that do not respond to NetBIOS queries
- Windows machines not on the Domain

To verify that the system is operating properly, login to the CLI on the device and execute the `show pan-agent statistics` command. This command will list each User Identification Agent and its current state. Make sure the **State** column shows connected. The **Users** and **Grps** columns show how many users and groups were retrieved from Active Directory that are available for use in policy configuration. The **IPs** column indicates how many IP addresses have been linked to a specific user.

```
> show pan-agent statistics
IP Address     Port    Vsys        State            Users  Grps IPs       Received Pkts
-------------------------------------------------------------------------------------
10.0.0.230     2009    vsys1       connected        122    33   60        34706
```

Once the **Users** and **Grps** columns show data, the users and groups from Active Directory will be available for use in the Security and SSL Decryption Rulebases. Once the **IPs** column shows data, the logs should begin to show user information (subject to the priming mentioned above). After a 15 minute interval has elapsed, the user information should begin appearing in ACC and App-Scope as well.

Ongoing Operations

Adding new Users and Groups

New AD groups will be recognized by the UIA once a day, or whenever the UIA is restarted.

New AD users will be visible for selection in the security policy once an hour, when group membership and new user information is updated from the UIA to the PA-series firewall.

Common Errors and Pitfalls

Windows Server

Default settings have been changed

UIA does not have permissions to read the Domain Controller security log

UIA

No networks listed in Allow list

Domain name not fully qualified

PAN-OS

User identification not enabled per zone on the fire

Cannot access UIA

Browser

3rd party firewalls and Anti-Virus block NetBIOS probes and alert on attempted probes

Captive Portal with NTLM

NLTM hostname does not resolve

NLTM hostname does not map to an L3 interface

L3 interface does not have HTTP management enabled

Captive Portal with Web Forms

Some device on the network is blocking port 6080

Appendix A: Implementation Checklists

Windows Member Server

Disable NTLMv1

Read Security Log

User Identification Agent

Install agent software

Enable/Disable NetBIOS probes?

Set age-out timer set to 10 hours (or to the same as what the AD server has) if NetBIOS is disabled. Shorter is OK is NetBIOS is enabled.

Consider installing a second UIA on anther member server for redundancy

If group membership is relatively static, lengthen group timeout

PAN Firewall Configuration

Agent to firewall management interface IP connectivity

Enable source zone for user identification

If Captive Portal with NTLM, define Interface Management Profile

If Captive Portal with NTLM, define inline management IP address

Configure UIA / Radius Server / NTLM hostname in Device tab

If needed, create Captive Portal Rule

If only using a RADIUS server, manually add users to rulebase

Write security policy rules for user/group information

Browser

Install firewall management interface SSL certificate for Captive Portal with Web Forms to avoid Untrusted Issuer SSL browser warnings

If using 3rd party security products and NetBIOS probes, allow access of NetBIOS probes on the UIA server and user desktops