Palo Alto Integration Guide

This guide covers the full integration between a **Palo Alto firewall** and Useroam Cloud: zone and interface configuration, RADIUS authentication, certificates, the Authentication Portal, DNS, log forwarding, and the firewall rules.

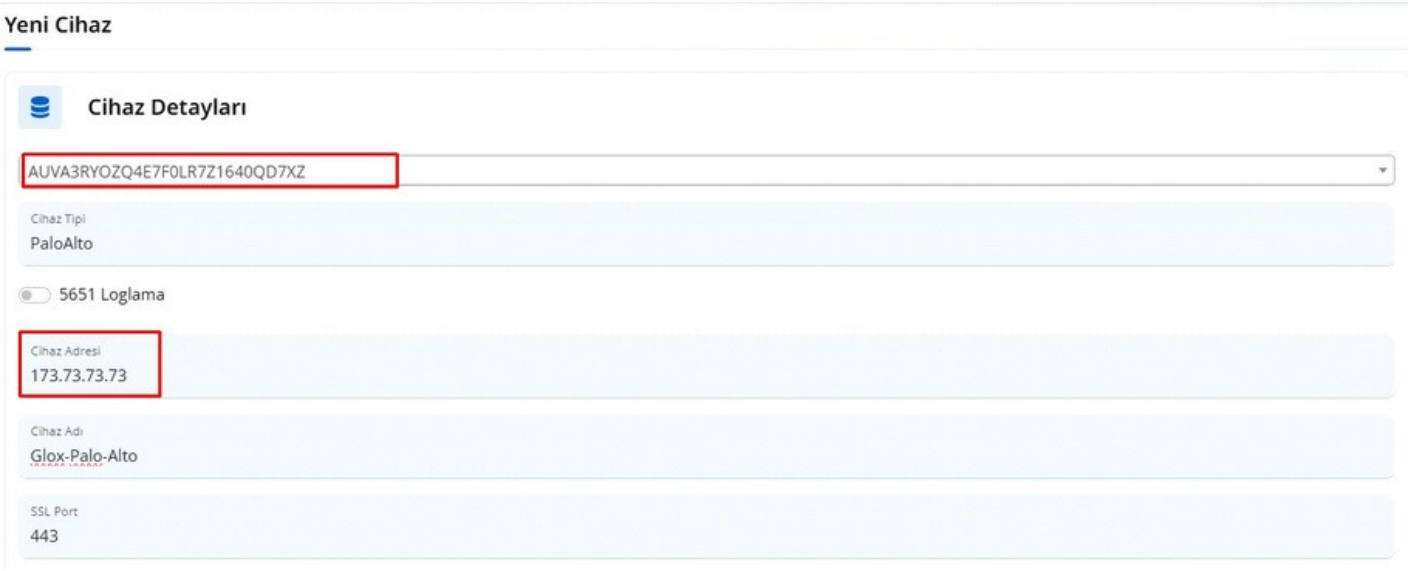
> **Before you start:** you need administrator access to the Palo Alto web interface, the external interface IP address the firewall will use to talk to Useroam, and your SSL certificate together with its key file and password.

---

1 - Adding the firewall to the panel

First sign in to your panel at **panel.useroam.com** and add a **New Device**. In the **Device Address** field, enter the external interface IP address the firewall will use to communicate.

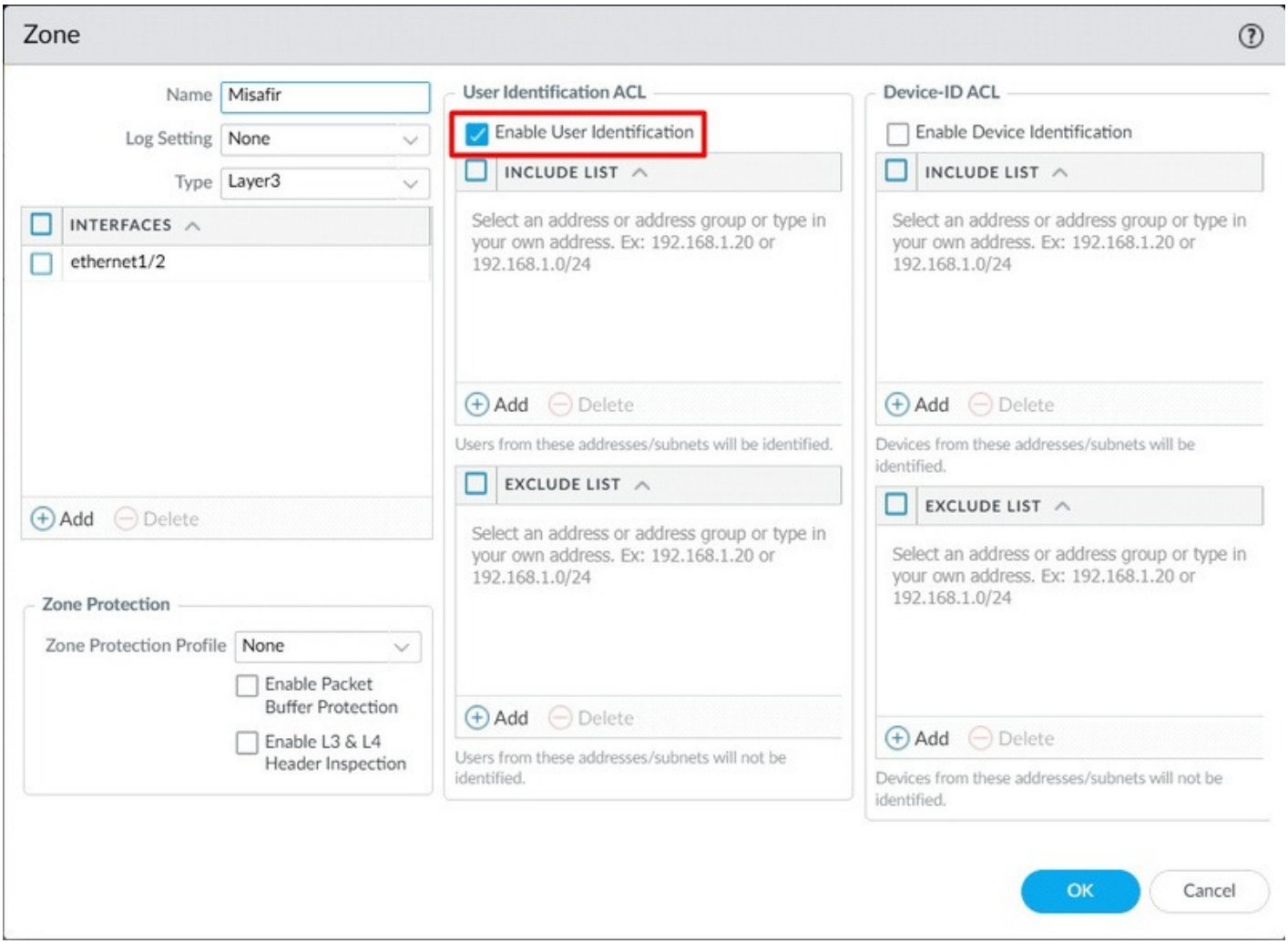
- **Device type:** select **PaloAlto**.
- **5651 Logging:** tick the 5651 Logging checkbox.



---

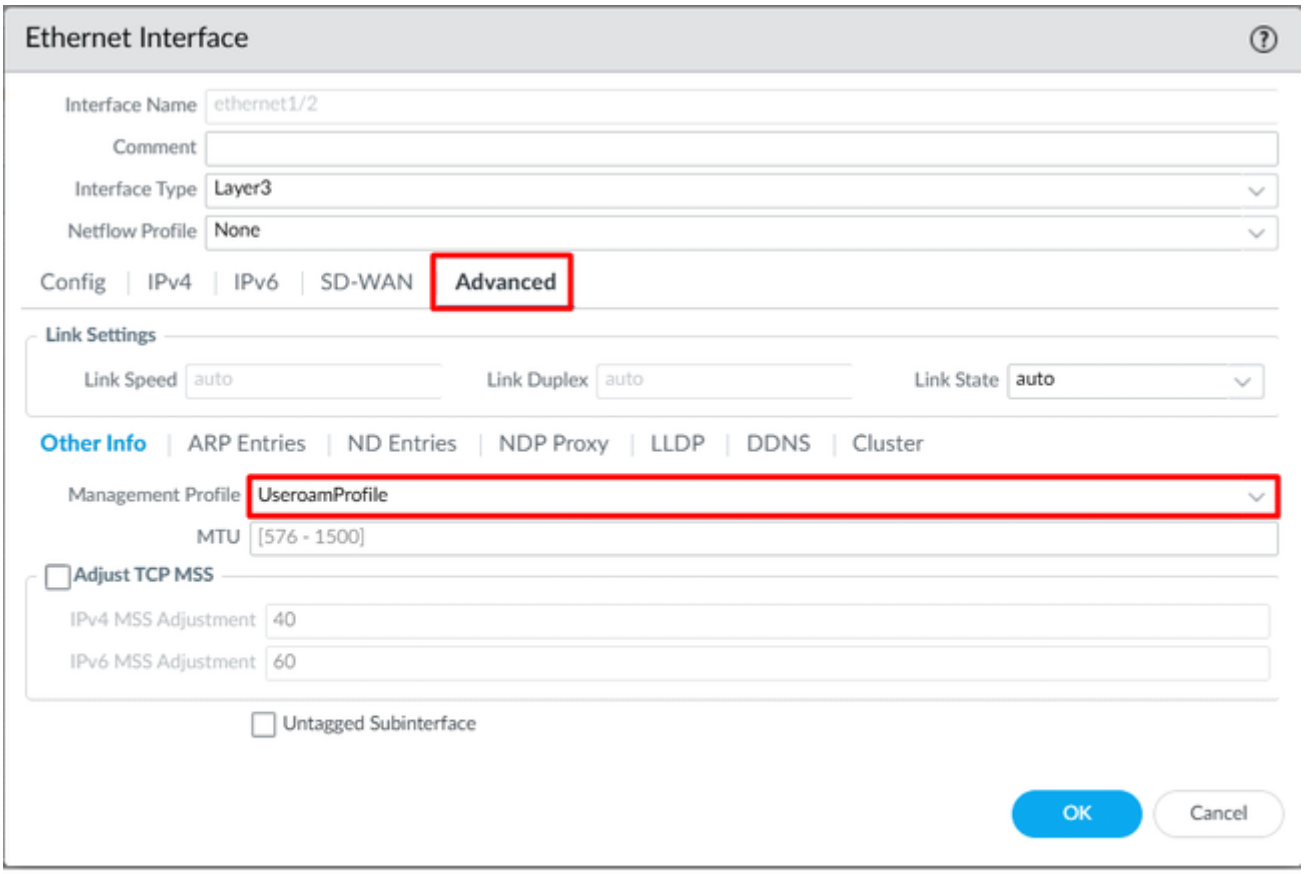
2 - Zone settings

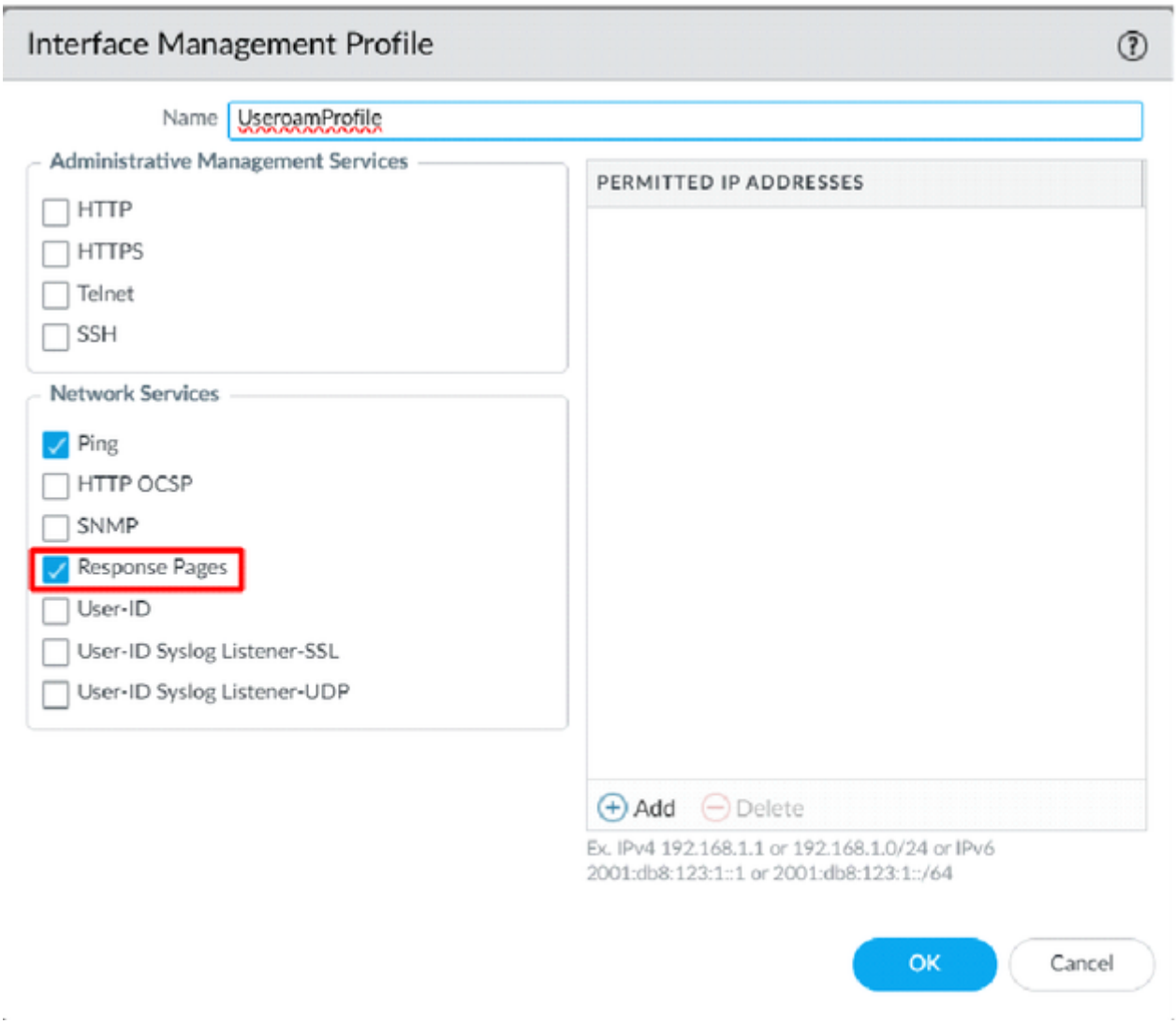
For the interface where Useroam will be enabled, create a new zone under **Network > Zone** and tick **Enable User Identification**.



3 - Interface and profile settings

On the interface where Useroam will be enabled, create a new profile from the **Advanced** section. While doing so, tick the **Response Pages** checkbox.

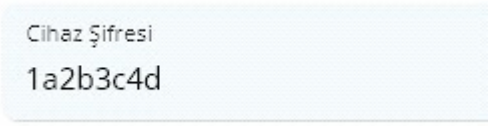

Ethernet Interface
Interface Name
ethernet1/2
Comment
Interface Type
Layer3
Netflow Profile
None
Config
IPv4
IPv6
SD-WAN
Advanced
Link Settings
Link Speed
auto
Link Duplex
auto
Link State
auto
Other Info
ARP Entries
ND Entries
NDP Proxy
LLDP
DDNS
Cluster
Management Profile
UseroamProfile
MTU
[576 - 1500]
Adjust TCP MSS
IPv4 MSS Adjustment
40
IPv6 MSS Adjustment
60
Untagged Subinterface
OK
Cancel


Interface Management Profile
Name
UseroamProfile
Administrative Management Services
HTTP
HTTPS
Telnet
SSH
Network Services
Ping
HTTP OCSP
SNMP
Response Pages
User-ID
User-ID Syslog Listener-SSL
User-ID Syslog Listener-UDP
PERMITTED IP ADDRESSES
Add
Delete
Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64
OK
Cancel

4 - RADIUS settings

Apply the settings below under **Device > Server Profiles > RADIUS**:

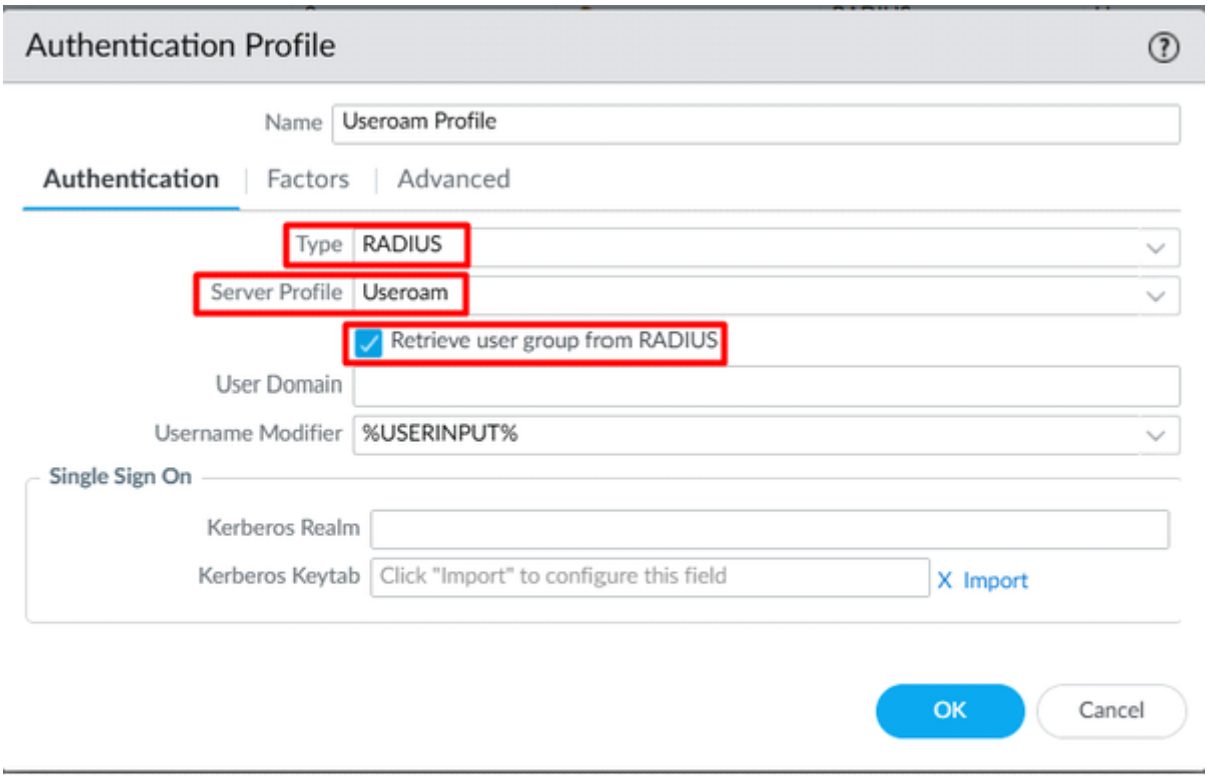
- **Authentication Protocol:** PAP
- **RADIUS Server / FQDN:** `panel.useroam.com`
- **Secret:** the device password you obtained from **Settings > Device Settings** in panel.useroam.com

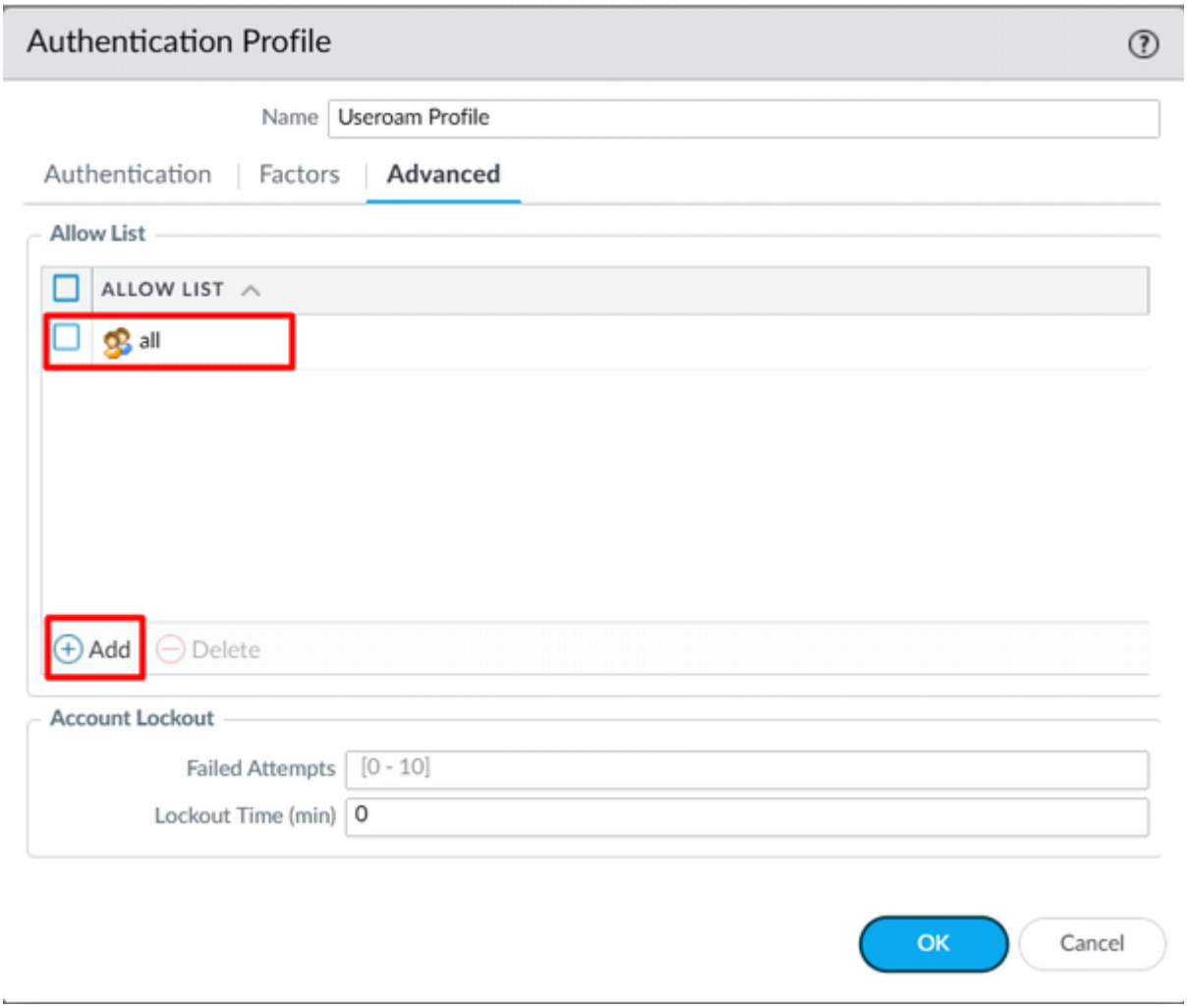


5 - Authentication Profile

Define the new profile under **Device > Authentication Profile**.

- **Type:** RADIUS
- **Server Profile:** select the RADIUS server profile you created.
- **Retrieve user group from RADIUS:** make sure this checkbox is ticked.
- **Advanced:** add the `all` object to the Allow List.


Authentication Profile
Name
Useroam Profile
Authentication
Factors
Advanced
Type
RADIUS
Server Profile
Useroam
Retrieve user group from RADIUS
User Domain
Username Modifier
%USERINPUT%
Single Sign On
Kerberos Realm
Kerberos Keytab
Click "Import" to configure this field
X Import
OK
Cancel

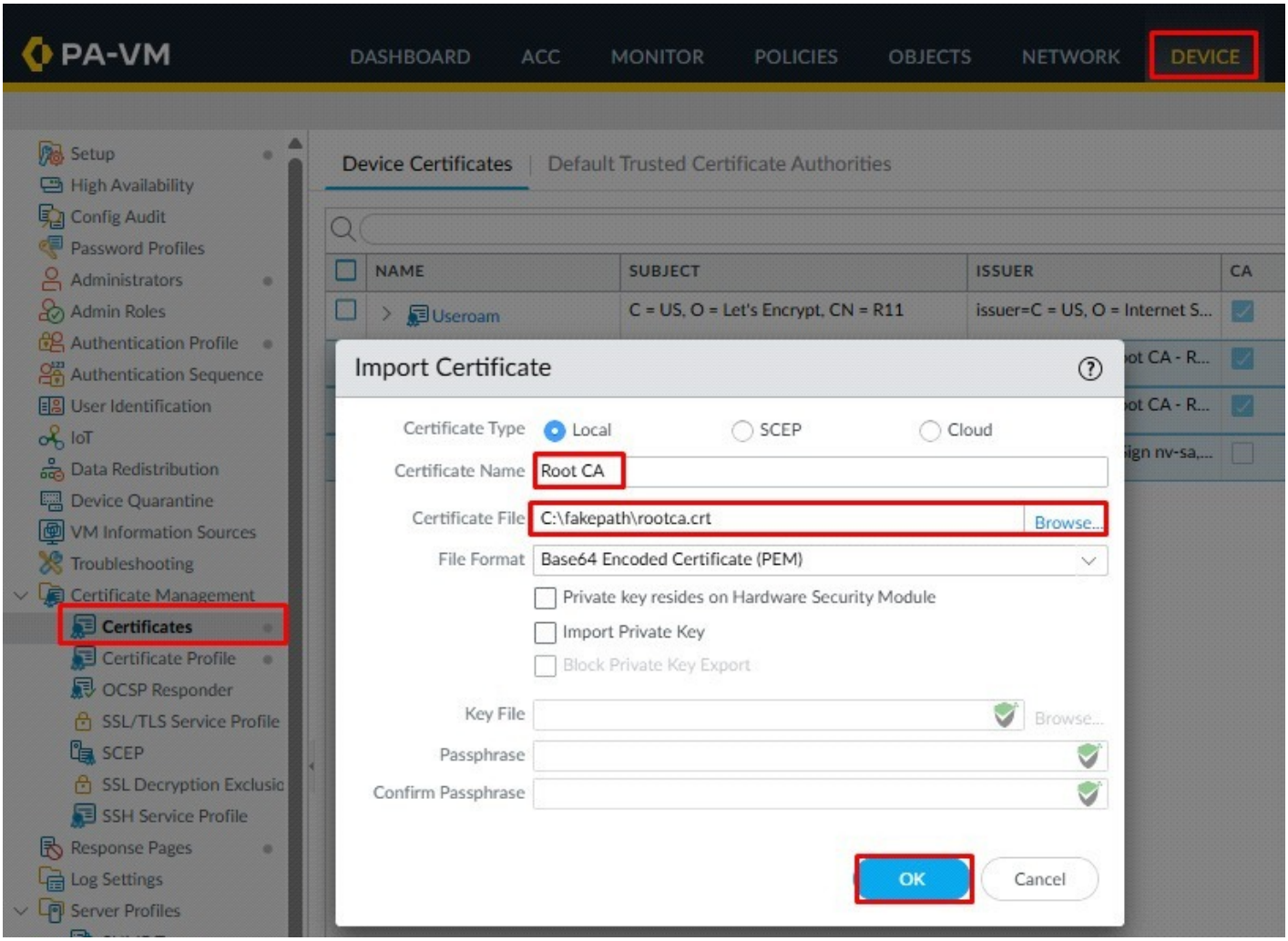

Authentication Profile
Name
Useroam Profile
Authentication
Factors
Advanced
Allow List
ALLOW LIST
all
Add
Delete
Account Lockout
Failed Attempts
[0 - 10]
Lockout Time (min)
0
OK
Cancel

6 - Certificate configuration

Before the certificates are installed on the device, the relevant root certificates (Root CA or Intermediate) must already be added to the system. This completes the certificate trust chain and prevents SSL/TLS errors on the client devices that connect.

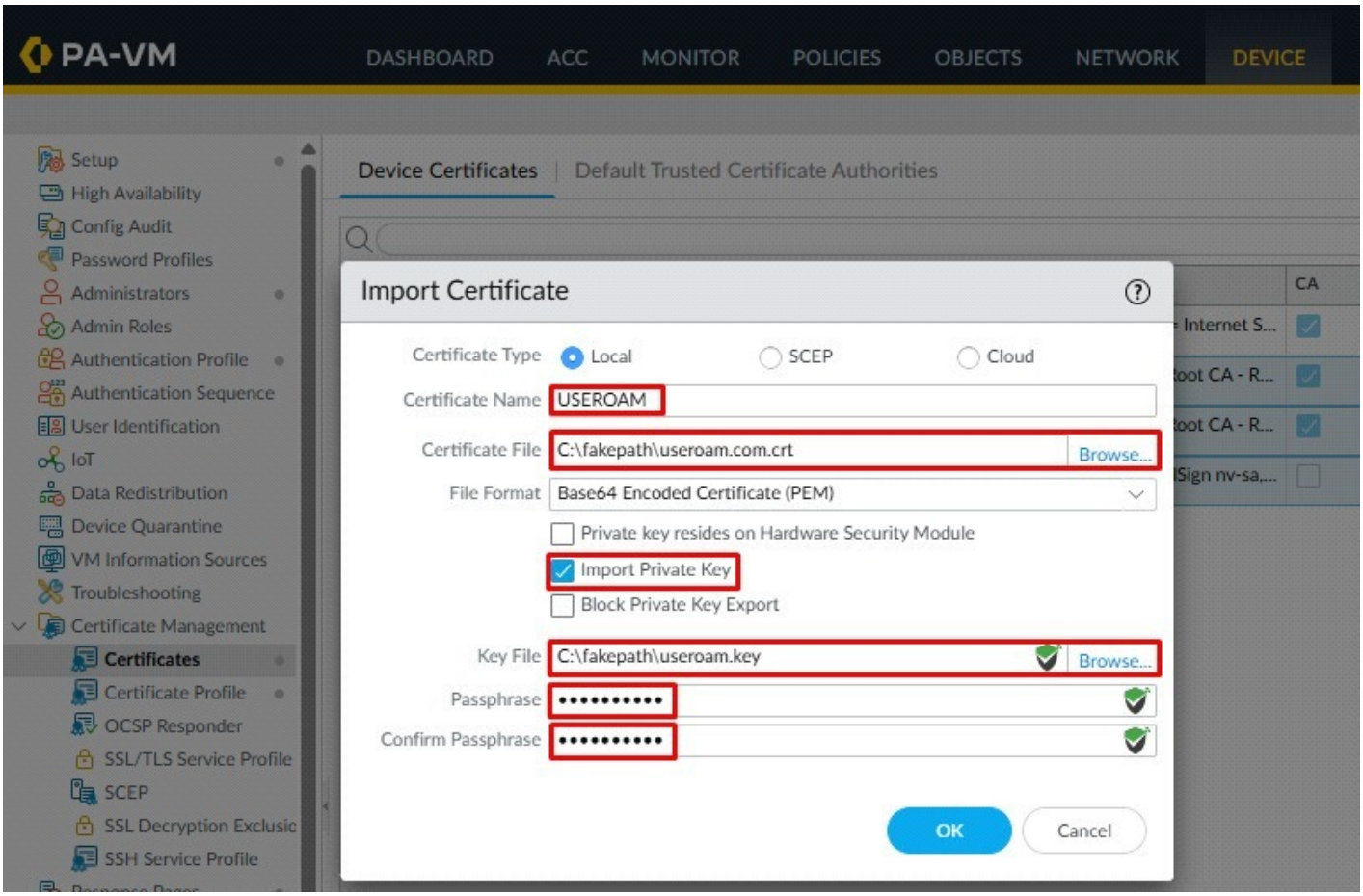
6A - Importing the Root CA

As the first step, import the Root CA or CA certificate.



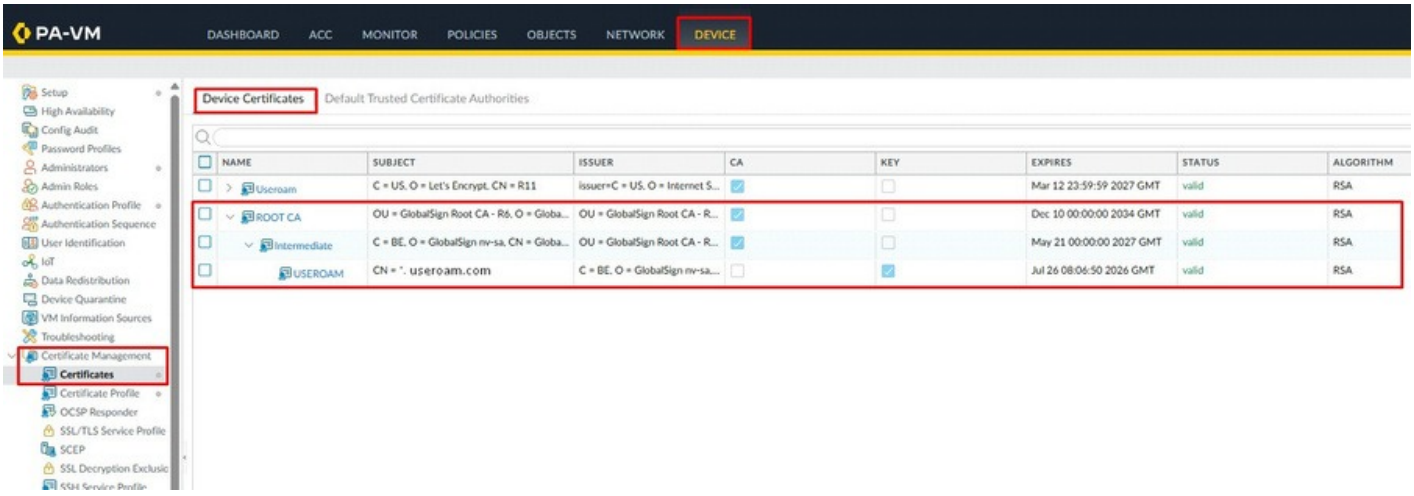
6B - Uploading the certificate and key file

Next, upload the certificate file to the firewall together with the key file and its password.



6C - Verifying the layered certificate chain

Once the upload is complete, the view should show a layered structure — a certificate chain in which the entries are linked to one another.

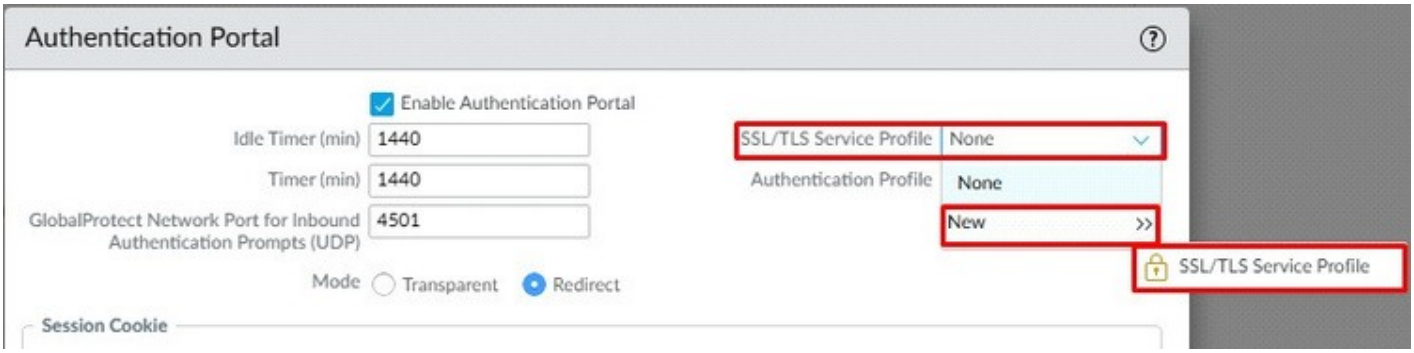


7 - Authentication Portal settings

Next, open the **Settings** section under **Device > User Identification > Authentication Portal**.

- **Enable Authentication Portal:** tick this option to activate the hotspot.

- **Idle Timer and Timer:** enter the maximum value, **1440 minutes** (24 hours), in both fields. This means a user sees the hotspot screen only once a day. We use this value because we want the hotspot screen to appear once every 24 hours; if you prefer shorter sessions, adjust it to suit your needs.
- **SSL/TLS Service Profile:** select the SSL profile you created earlier. Note that on some Palo Alto versions, previously created profiles may not appear in this field. In that case, use the **New** option to create a new SSL/TLS profile from this screen. If your system does let you select one, you can use the existing profile.



If you need to create a new profile, follow these steps:

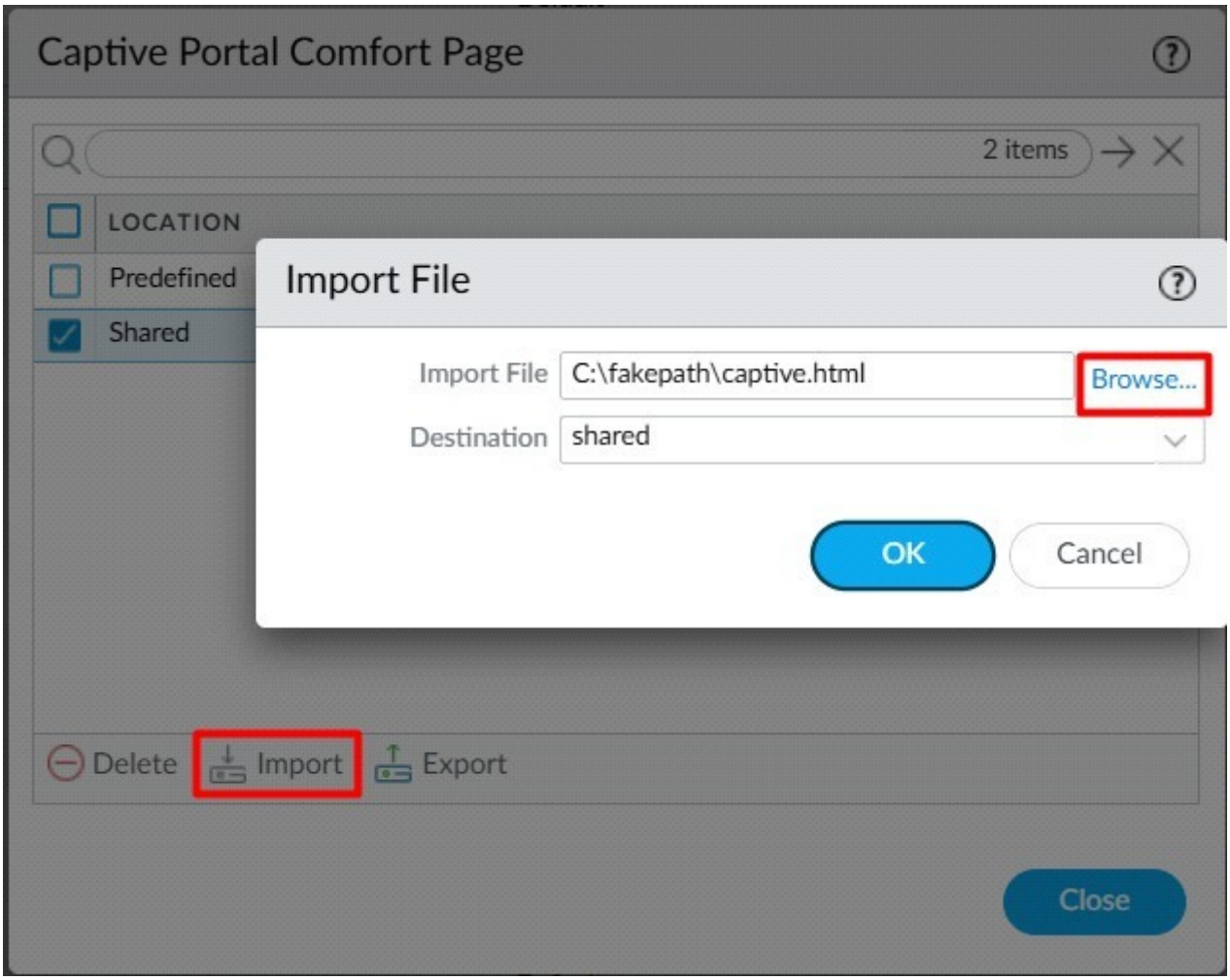
- Give the profile a name and select the SSL certificate to be used.
- Under **Protocol Settings**, choose the minimum and maximum SSL/TLS versions you want to support.
- When the settings are complete, click **OK** to save the profile.

- **Authentication Profile:** continue by selecting the Useroam profile you created.
- **Session Cookie / Timeout:** enter **1440 minutes** (24 hours) here as well, matching the value set above.
- **Redirect Host:** enter the subdomain here, since the redirect is performed over the certificate.

---

8 - Uploading the captive portal design (Comfort Page)

In panel.useroam.com, go to **Settings > Device Settings** and copy the entire code block that starts with `<html>`. Paste it into a text editor and save it in HTML format under a name such as `captive.html`. Then upload that document on the firewall via **Device > Response Pages > Captive Portal Comfort Page**.

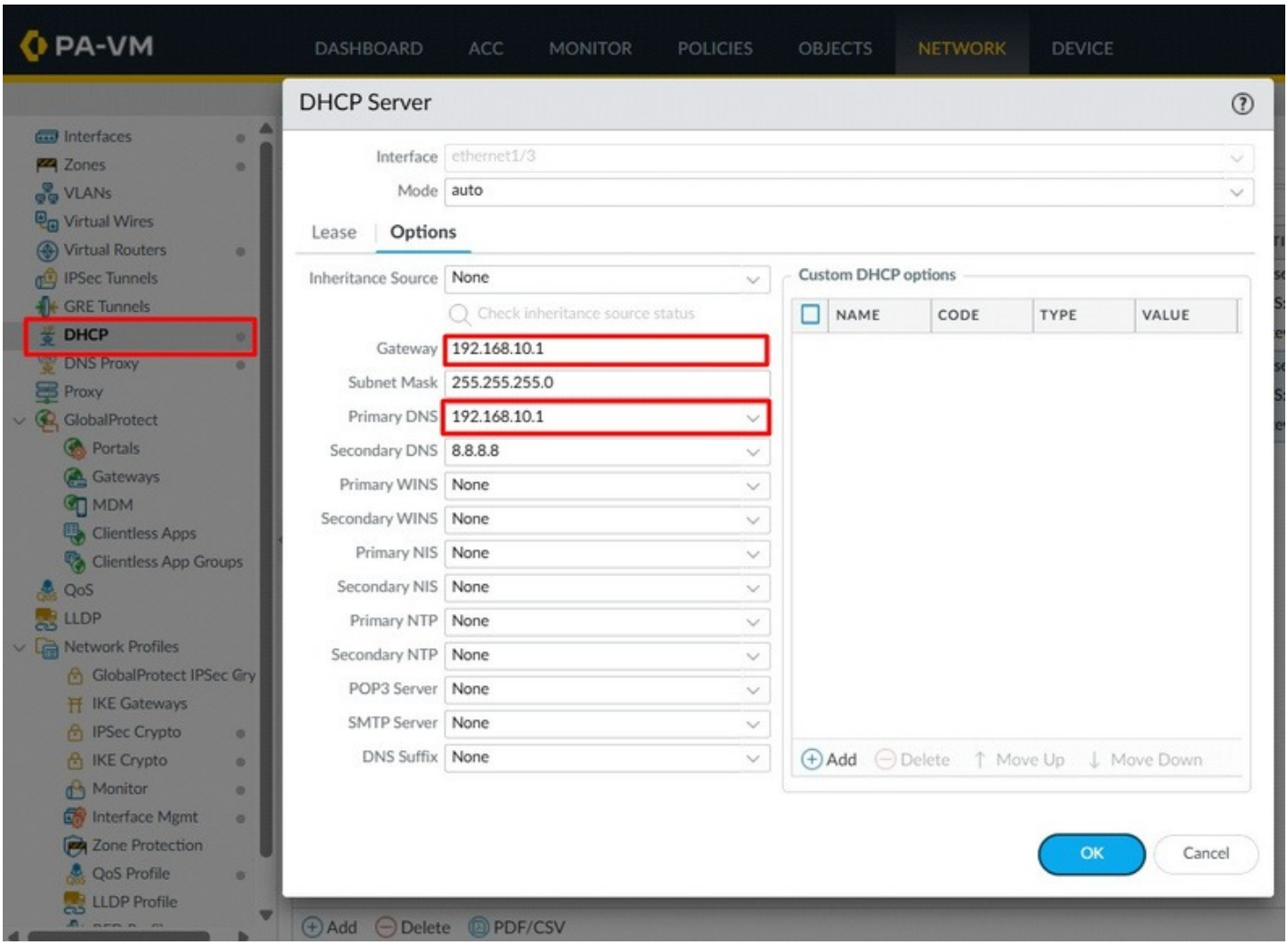


9 - DHCP settings

So that DNS queries from the internal network are handled without problems, the DHCP and DNS Proxy configuration must be updated if you do not have a separate DNS server. Go to **Network > DHCP > Options**.

- **Primary DNS:** enter the firewall's own interface IP address.
- **Secondary DNS:** you can define a global DNS server (for example `8.8.8.8` — Google DNS).

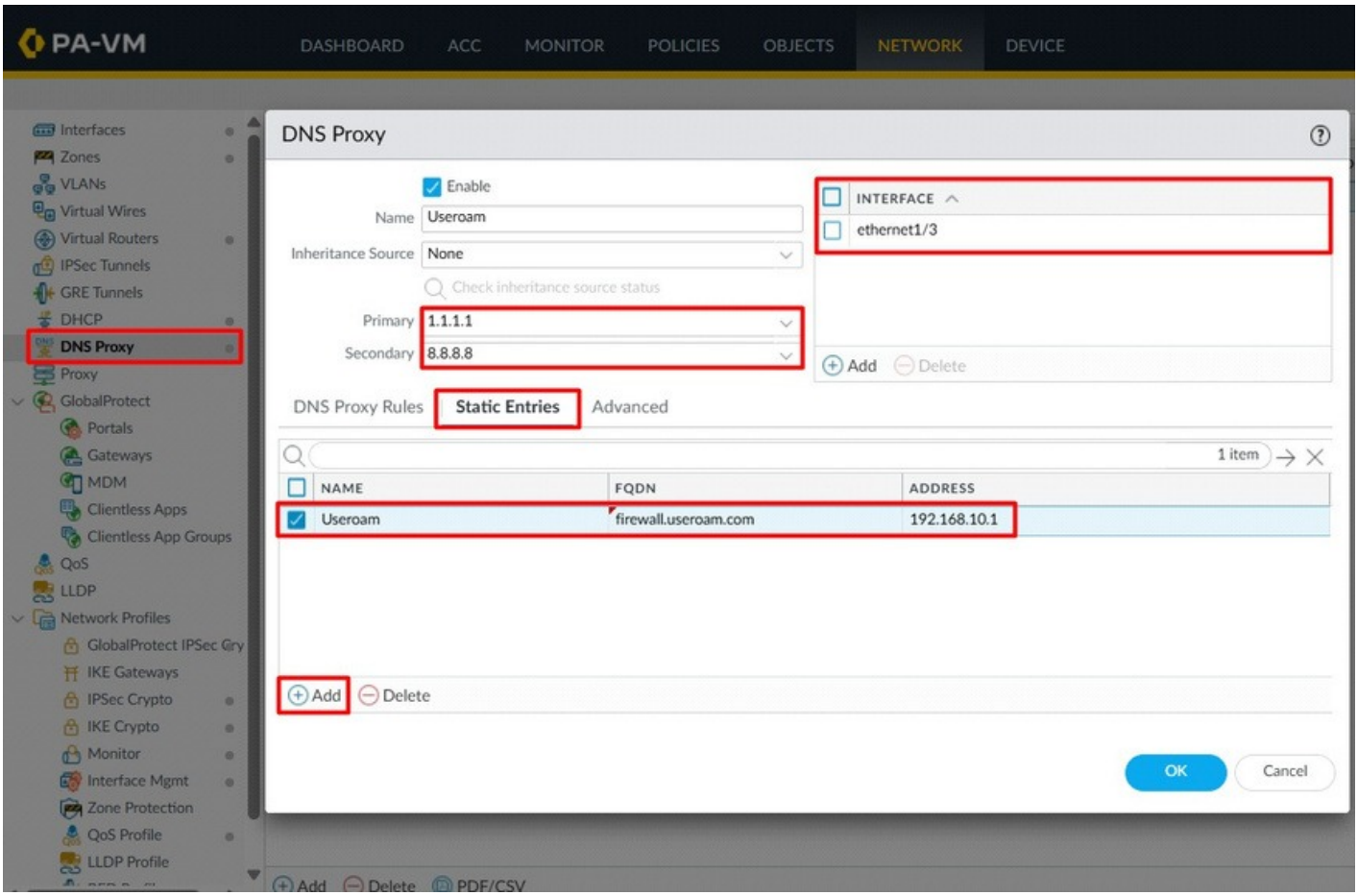
Note: if you already have an internal DNS server, add the record required for the domain redirect to your internal DNS as well (in the Static Entries section) and continue from step 11.



10 - DNS Proxy settings

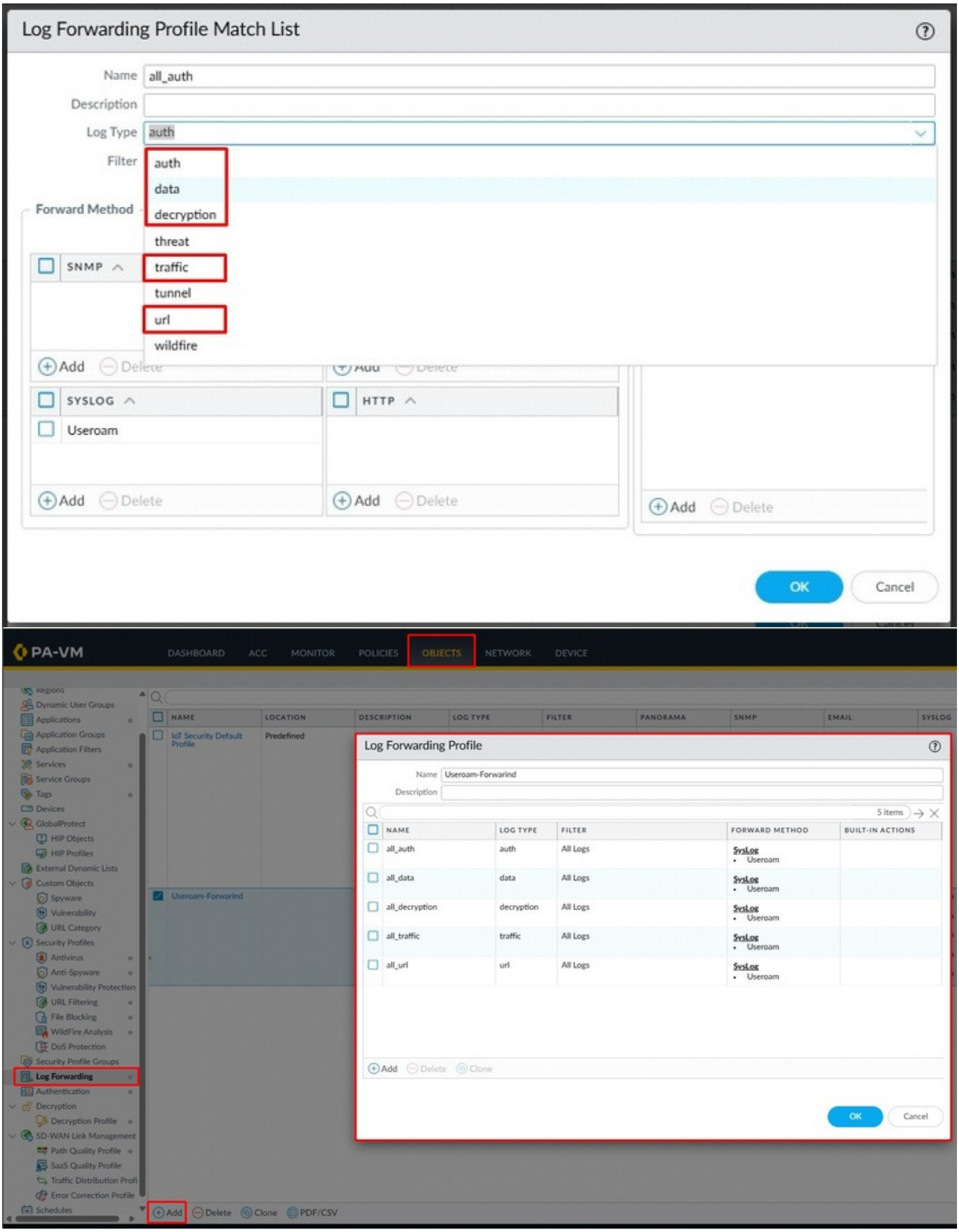
Next, define a new proxy under **Network > DNS Proxy** so DNS queries resolve correctly.

- **Interface:** select the interface(s) where Useroam will be active.
- **Primary / Secondary DNS:** enter the global DNS servers.
- **Static Entries:** click **Add** to create a new record. At this stage it is important that the IP used for the redirect is the gateway IP address of the firewall's Management Interface.



11 - Forwarding logs to Useroam (Log Forwarding)

Go to **Objects > Log Forwarding** and add a new profile with **Add**. A separate profile must be created for each of the five log types (auth, data, decryption, traffic, url). For every entry, remember to select the Useroam profile in the Syslog section.

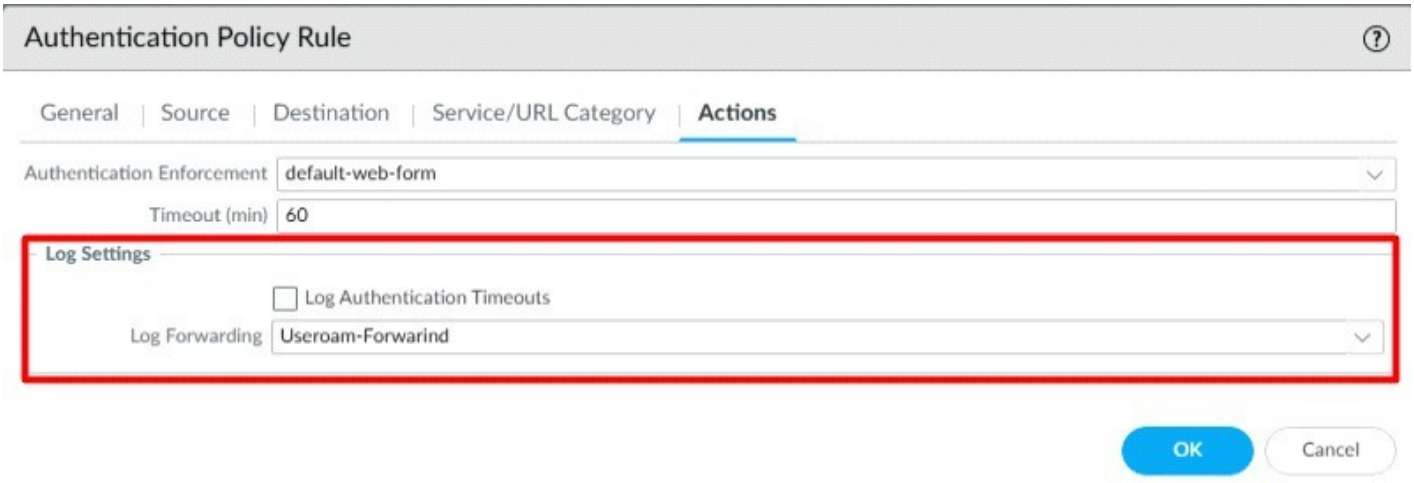

Log Forwarding Profile Match List
Name
all_auth
Description
Log Type
auth
Filter
auth
data
decryption
threat
traffic
tunnel
url
wildfire
Forward Method
SNMP
Add
Delete
SYSLOG
Useroam
HTTP
OK
Cancel
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Log Forwarding
Authentication
Decryption
Log Forwarding Profile
Name
Useroam-Forwarind
Description
5 items
NAME
LOG TYPE
FILTER
FORWARD METHOD
BUILT-IN ACTIONS
all_auth
auth
All Logs
SysLog
Useroam
all_data
data
all_decryption
decryption
all_traffic
traffic
all_url
url
Clone
PDF/CSV

Creating the firewall rules

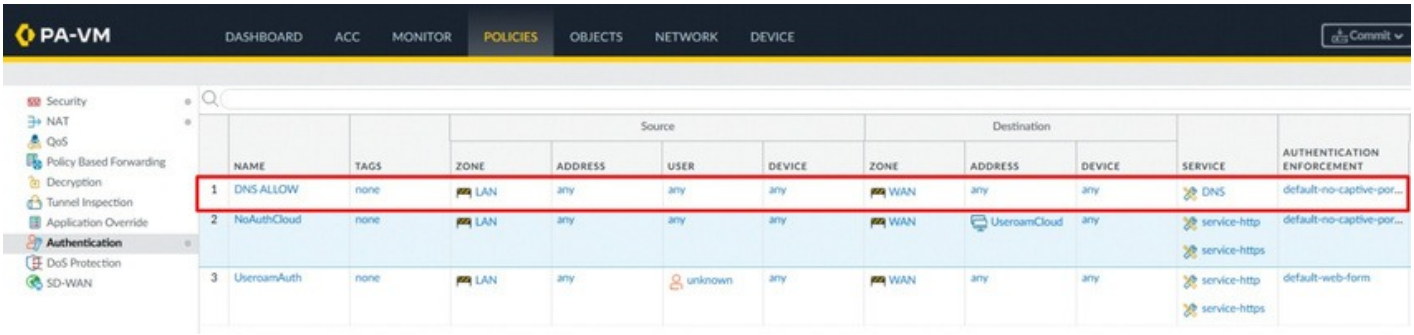
Two sets of rules are needed for the Palo Alto integration. When you first create the rules, Palo Alto needs to learn the traffic — so set **Service** to `Any` at first and change it to `application-default` afterwards.

12A - RULE SET 1: Authentication rules

Go to **Policies > Authentication** and define the three rules below. **Useroam** must be selected in the Log Forwarding field on every rule.

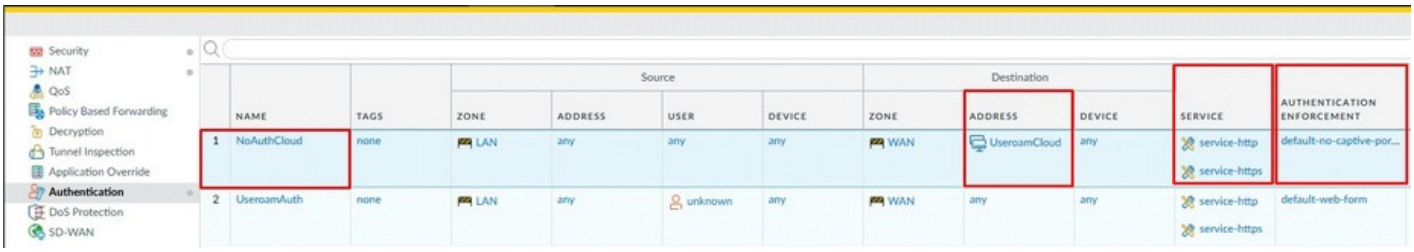


- **RULE 1 (Allow DNS):** created so DNS queries pass through the authentication stage without problems. All DNS queries towards the WAN are allowed by selecting `default-no-captive-portal` under Authentication Enforcement.
- **RULE 2 (Allow Useroam Cloud):** this rule provides trouble-free access to Useroam Cloud. In the Destination Address field, select the `UseroamCloud` (panel.useroam.com) FQDN address object you created.
- **RULE 3 (Captive redirect):** the main rule that redirects HTTP and HTTPS traffic of users who have not yet signed in — or who are joining the network for the first time — to `default-web-form`, i.e. the captive portal screen.



12B - RULE SET 2: Security rules

Go to **Policies > Security**. On every rule, **Log at Session End** must be selected under Log Settings and **Useroam** must be assigned in Log Forwarding.



- **RULE 1 (Allow WAN DNS):** lets every device run DNS queries over the WAN without being caught by the captive portal. It is required so the device can reach its own global captive-detection domain (for example `captive.apple.com`), conclude that internet access exists, and then trigger the hotspot screen.
- **RULE 2 (Allow Useroam access):** defined so devices in the captive portal zone can reach panel.useroam.com through the firewall without problems.
- **RULE 3 (Allow internet access):** the final rule that gives your guest network internet access. On this rule, the **Source User** value in the Source section must be set to `known-user`.

> **Additional technical note (disconnecting a signed-in user):** to end an active guest session or clear its cache, sign in to the Palo Alto CLI and run the following commands in order.
>
> To list all signed-in active users and their IP addresses:
> `show user ip-user-mapping all`
>
> To drop the relevant IP address from the network, run:
> `clear user-cache ip <ip-address>`
> `debug user-id reset captive-portal ip-address <ip-address>`

Important — integration complete

That's it — your Palo Alto integration and server change are complete. If you run into any technical problems during the process, contact our support team at **destek@useroamteknoloji.com**.

Login with WhatsApp — firewall allowlist (walled garden)

For the **Login with WhatsApp** flow to work while the guest is still behind the captive portal (before internet access is granted), the following addresses **must be allowed** in your firewall or walled-garden configuration. Without these rules the WhatsApp login screen will not open and the automatic login based on delivery confirmation will not work.

Domains to allow (FQDN)

- `*.wa.me`
- `*.whatsapp.com`
- `*.whatsapp.net`
- `g.whatsapp.net`
- `mmg.whatsapp.net`
- `fbsbx.com`
- `*.useroam.com`

IP addresses to allow

- `157.240.0.0` — Meta / Facebook network block
- `31.13.0.0` — Meta / Facebook network block
- `104.247.174.120` — Useroam panel

Note: `157.240.0.0` and `31.13.0.0` are typically `/16` network blocks (Meta infrastructure); we recommend defining them as blocks in the firewall (`157.240.0.0/16`, `31.13.0.0/16`). `104.247.174.120` is the Useroam panel IP (`/32`). Use the domain list if your firewall supports FQDN-based filtering; otherwise use the IP blocks.

Revizyon #1
tugay tarafından 10 Ağustos 2026 22:59:09 oluşturuldu
tugay tarafından 10 Ağustos 2026 22:59:09 güncellendi