Expedition

Hardening Guide

Version 1.0

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 28, 2018

Contents

What is Expedition?

Expedition is the fourth evolution of the Palo Alto Networks Migration Tool. The main purpose of this tool was help reducing the time and efforts to migrate a configuration from one of the supported vendors to Palo Alto Networks.

By using the Migration Tool everyone can convert a configuration from Checkpoint or Cisco or any other vendor to a PanOS and give you more time to improve the results. Migration Tool 3 added some functionalities to allow our customers to enforce security policies based on App-ID and User-ID as well.

With Expedition we have gone one step further, not only because we want to continue helping to facilitate the transition of a security policy from others vendors to PanOS but we want to ensure the outcome it's the best as possible, there is why we added a **Machine Learning module** who can help you to generate new security policies based on real log traffic and the introduction of the **Best Practices Assessment Tool** to check the configuration complies with the Best Practices recommended by our security experts.

With all these huge improvements we expect the next time you use Expedition the journey to the excellence will be easier.

How to harden Expedition

Expedition is delivered as a whole VM where a preinstalled OS is in place. Palo Alto Networks is not the responsible of any OS security related there is why you have full root privileges to keep it up to date. This guide will help you in case you don't know how to maintain your server up to date and guide you in what best practices you should look at before starting using it in production environments.

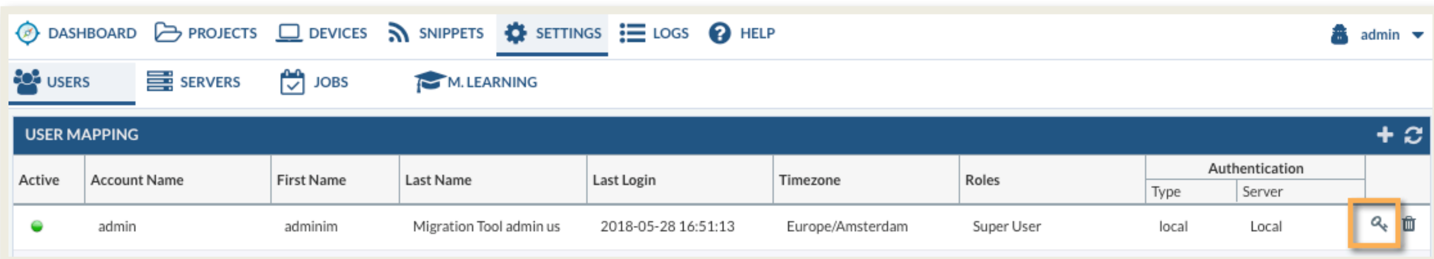
Change default Passwords

Change the password for the expedition user from the cli by typing

```
passwd expedition
```

Use at least 10 characters and mix with some numeric and especial characters to make it hard to brute force it.

From the GUI change it from the SETTINGS -> USERS at least to the admin user.



Re-generate SSH Keys

First time you download the Expedition image we encourage you to re-generate a new pair of ssh keys to avoid have man in the middle attacks.

Connect to your Expedition instance via SSH and type these commands:

```
sudo rm /etc/ssh/ssh_host_*
sudo dpkg-reconfigure openssh-server
sudo systemctl restart sshd
```

After you disconnect from the server and try to connect again you will receive an error because now the key you trusted before for the Expedition IP address won't match with the new certificate so we have to remove the entry from our ssh desktop

In case you are using Mac OS this will be the error:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
```

```
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:M9N1zOs1zwZEhUt5r+0vV/olH67P8Jveaf15vxk7JOw.
Please contact your system administrator.
Add correct host key in /Users/xxxxx/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/xxxxx/.ssh/known_hosts:135  ←EDIT THIS FILE LINE 135 on this EXAMPLE
ECDSA host key for 1.1.4.8 has changed and you have requested strict checking.
Host key verification failed.
```

To Remove the Key edit from your User's folder the file under .ssh/known_hosts and remove the entry from that file and try it again.

Re-generate SSL certificate

Apache SSL is already configured on Expedition and it comes by default with a private and public certificates to its recommended to create them once your instance is up and running

From the CLI and after run the first command you will be prompted for some information for the new certificate like Country, company, etc, fill under your requirements.

```
sudo openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout /etc/ssl/private/ssl-cert-snakeoil.key -out /etc/ssl/certs/ssl-cert-snakeoil.pem
sudo systemctl restart apache2
```

After restart Apache you can restart your browser session to see the new certificate

You can use a Let's Encrypt valid certs as well, this is one User guide you can find on Internet
https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-16-04

Revision History

Date	Revision	Comment
May 28, 2018	A	First release of this document.