



STORMSHIELD

LAB 7 :
Authentification

Réseau A :

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Places System

09K0639A9@19 x +

⚠ Not secure | <https://192.168.1.254/admin/admin.html#ldapmodule>

Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

USERS / DIRECTORIES CONFIGURATION

CONFIGURED DIRECTORIES (MAXIMUM 5)

+ Add a directory Action

Domain name: a.net

Configuration

Enable user directory

Organization: a

Domain: net

ID: cn=NetasqAdmin

Password:

Confirm:

Password strength

Access to the internal LDAP

Enable unencrypted access (PLAIN)

Enable SSL access

SSL certificate issued by the server: No certificate

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 x AUTHENTICATION +

⚠ Not secure | <https://192.168.1.254/auth/>

Apps Debian.org Latest News Help

STORMSHIELD Network Security

LOGIN / LOGOUT NEW USER

Username

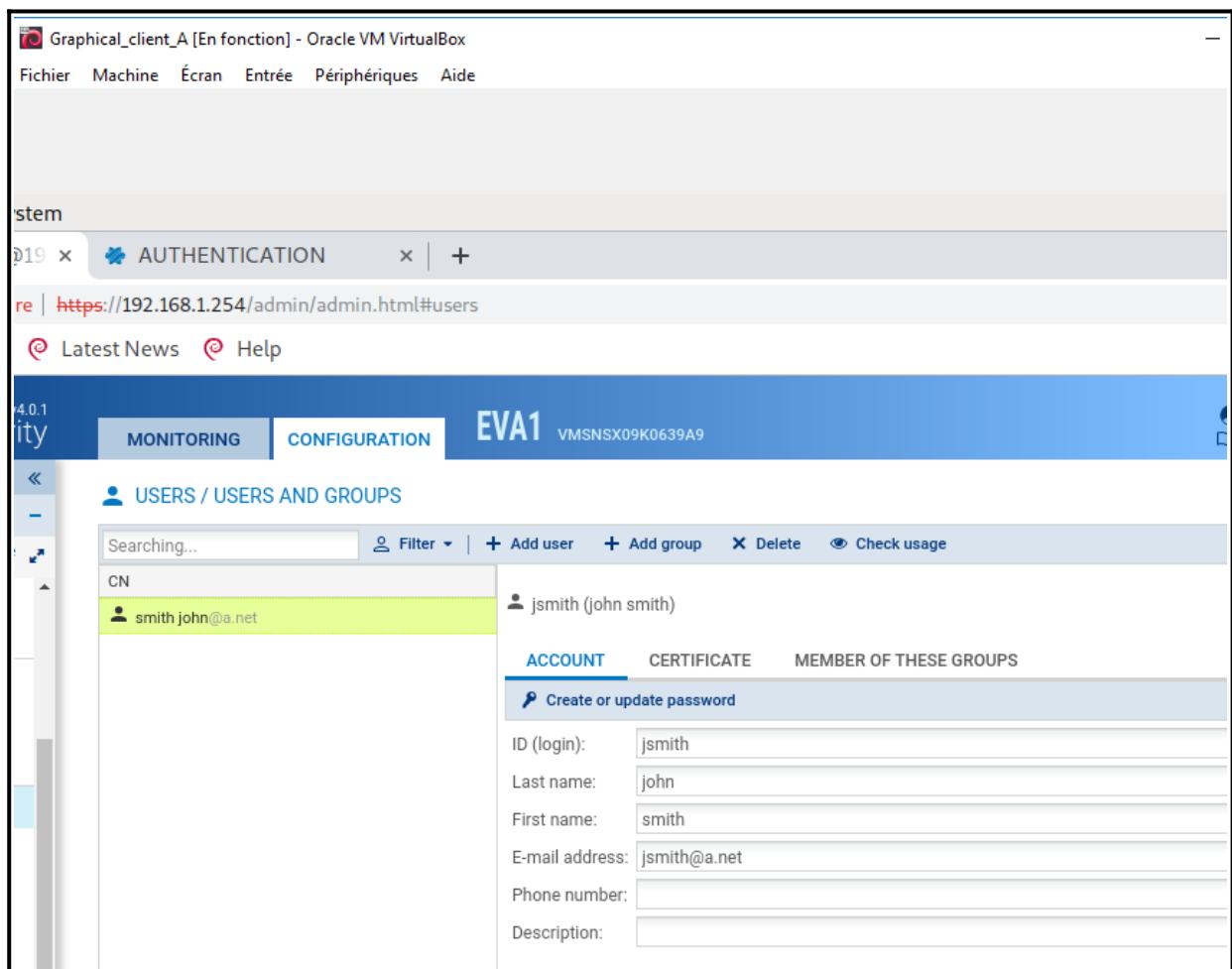
Authentication duration 4 hours

Logout Login

If you are already authenticated, clicking on connect will extend the authentication by the

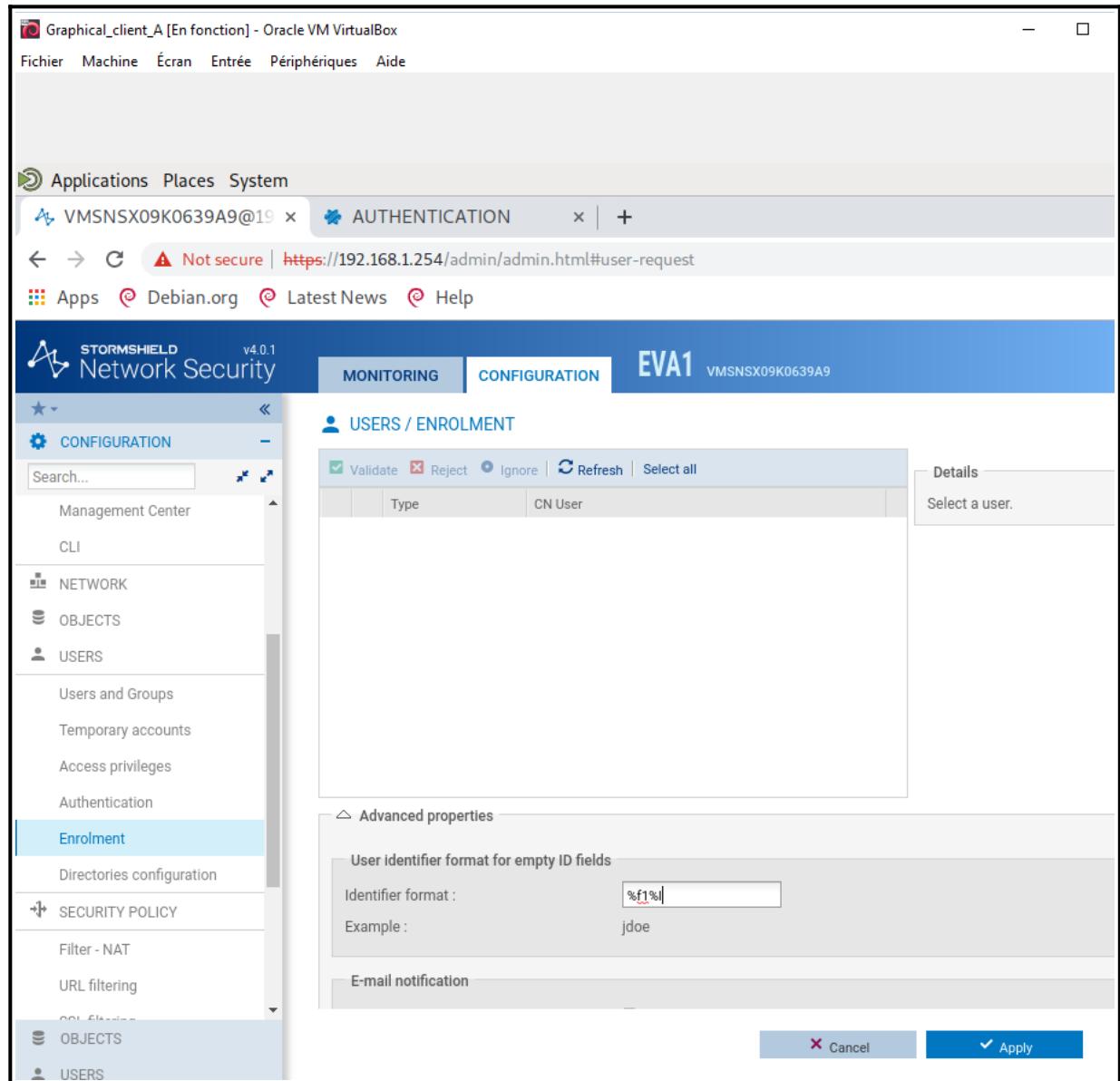
1ère étape : Crédation d'une base LDAP interne :

- Organisation A, domaine « net ».
- Activation du profil d'authentification, ainsi que l'enrôlement des utilisateurs.
- Test du portail captif.



The screenshot shows a web browser window titled 'Graphical_client_A [En fonction] - Oracle VM VirtualBox'. The address bar shows 'https://192.168.1.254/admin/admin.html#users'. The page is titled 'USERS / USERS AND GROUPS'. A table lists a single user entry: 'jsmith (john smith)' with 'CN' 'smith john@a.net'. The right panel shows the 'ACCOUNT' tab of the user's profile, with fields for 'ID (login): jsmith', 'Last name: john', 'First name: smith', 'E-mail address: jsmith@a.net', 'Phone number: ', and 'Description: '.

2ème étape : Crédation de l'utilisateur John Smith.



Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 ✘ AUTHENTICATION ✘ +

Not secure | <https://192.168.1.254/auth/newuser.html>

Apps Debian.org Latest News Help

STORMSHIELD Network Security

LOGIN / LOGOUT **NEW USER**

Please enter all the required information

Last Name *

First name *

E-mail address *

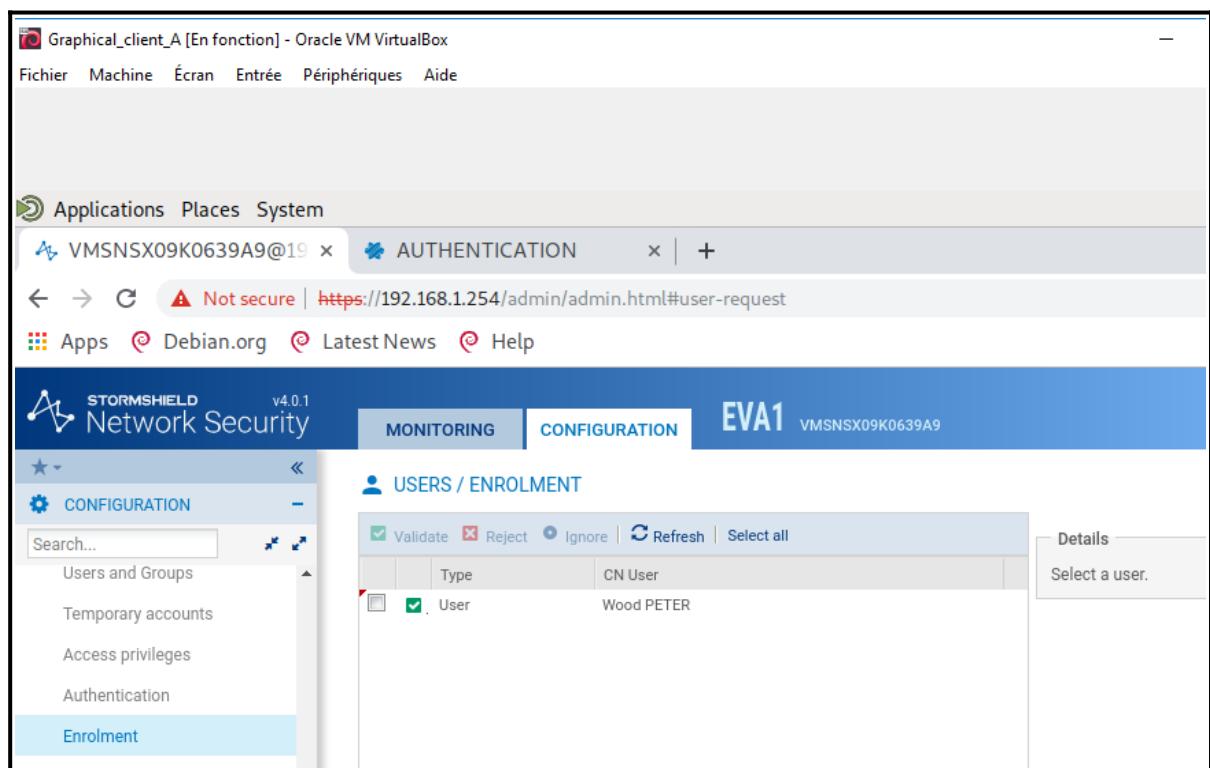
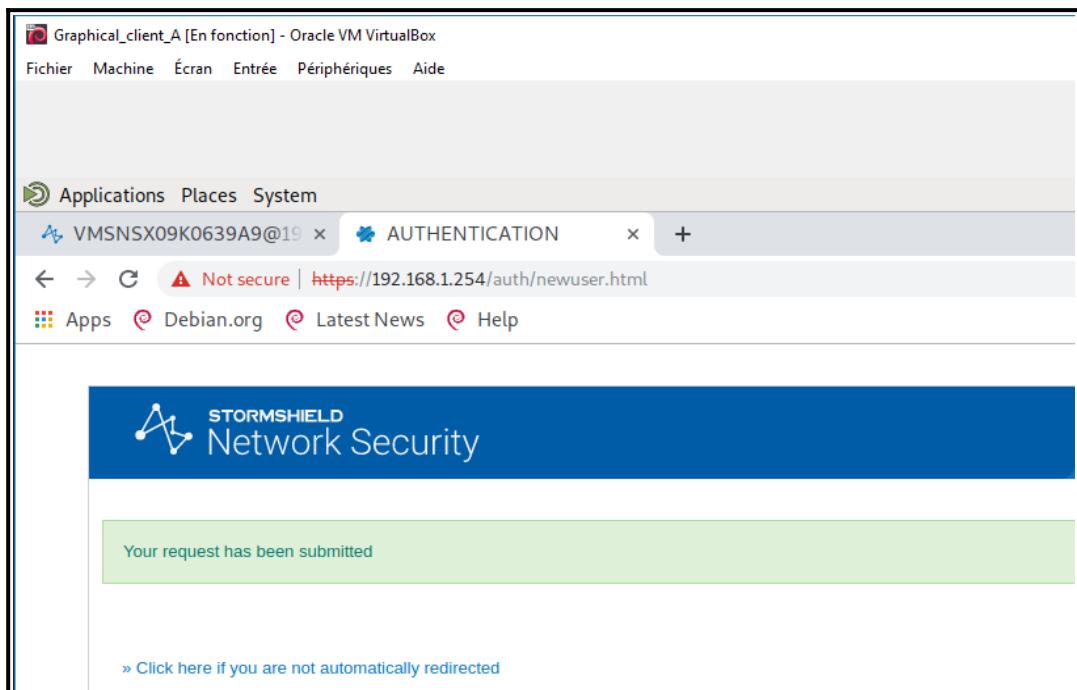
Description

Telephone number

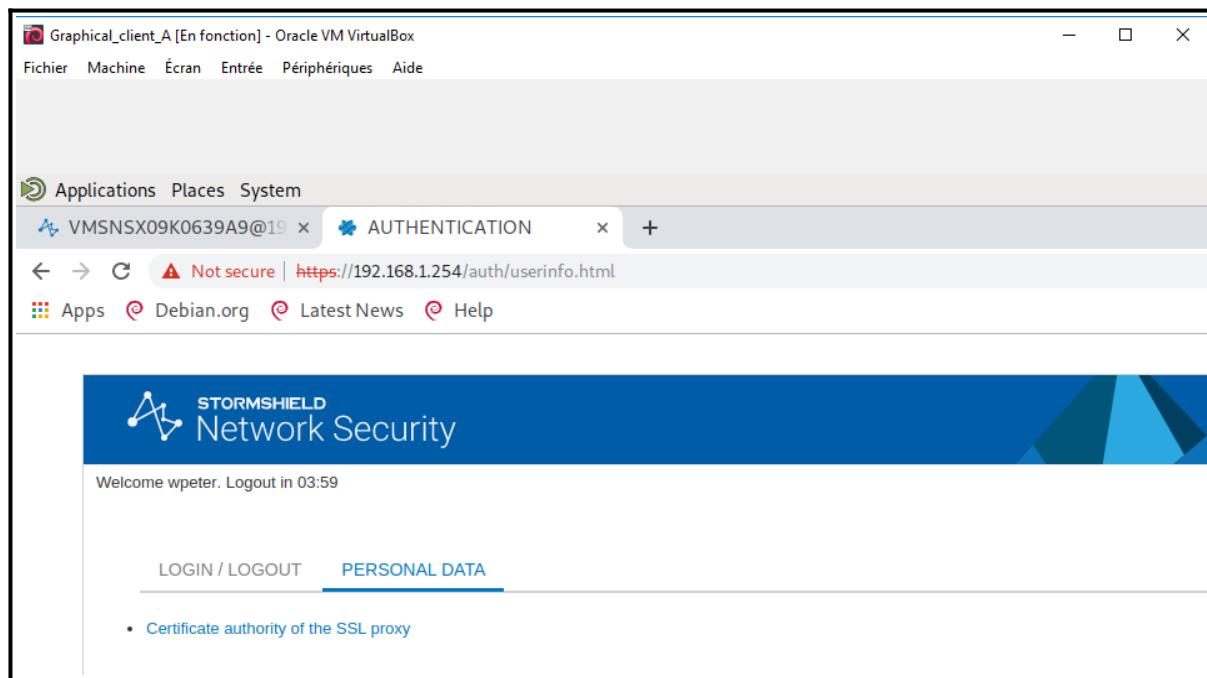
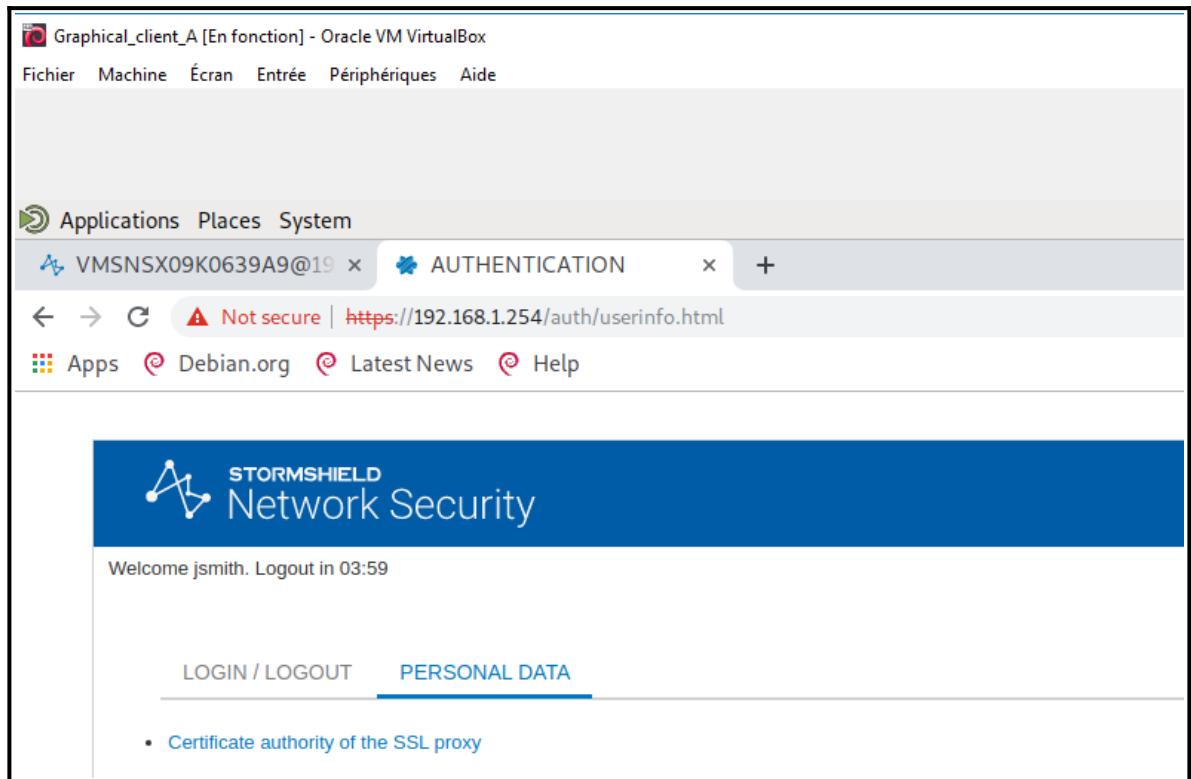
Password **

Confirm password **

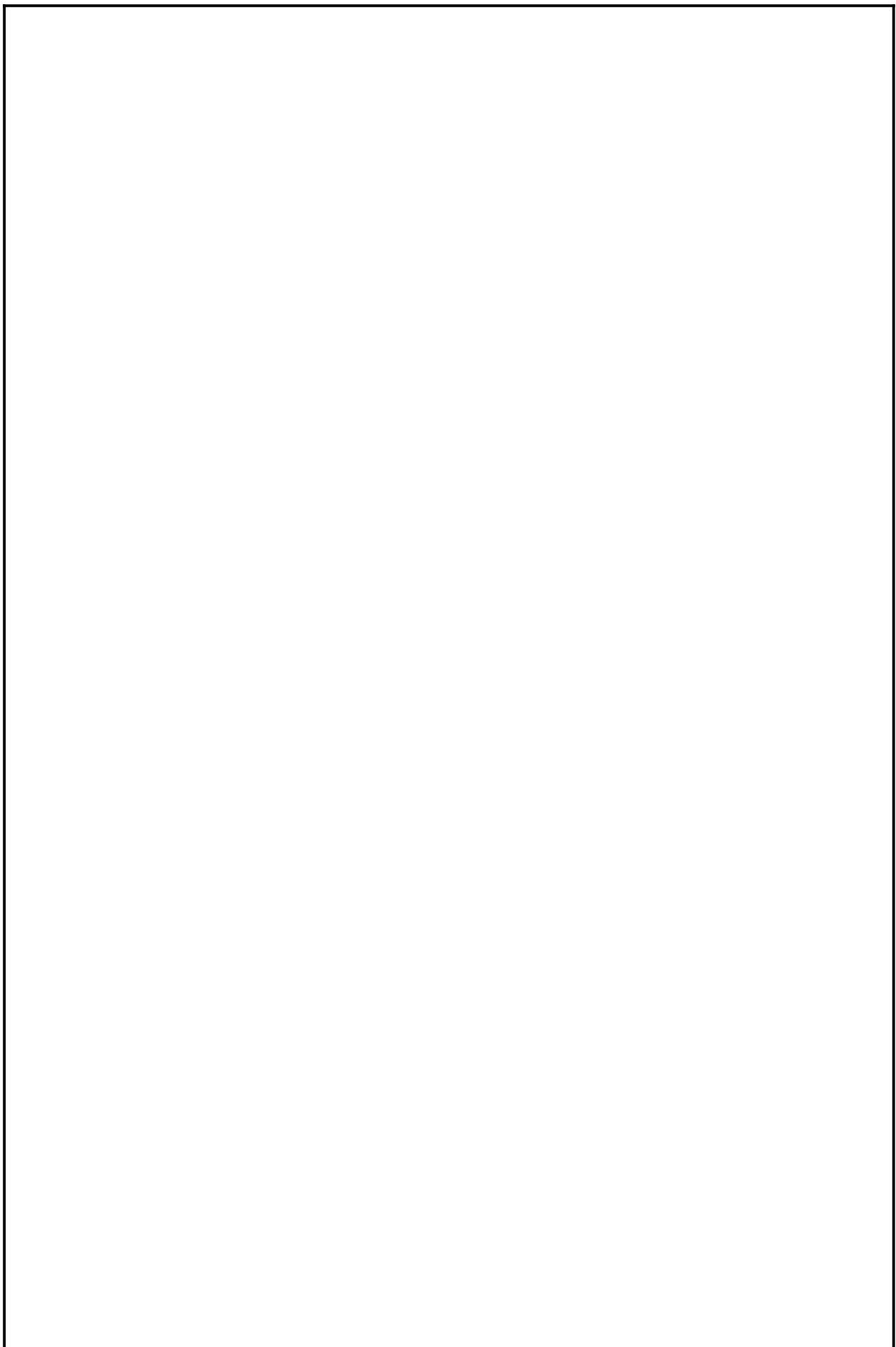
Submit request...



3ème étape : En utilisant la fonction d'enrôlement, création de l'utilisateur Peter Wood et tests.



4ème étape : Test de connexion avec l'utilisateur John Smith et Peter Wood.



Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 ✎ AUTHENTICATION ✎ +

← → C Not secure | https://192.168.1.254/admin/admin.html#securitypolicy/local/7/filter/25

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

EVA1 VMSNSX09K0639A9

MONITORING CONFIGURATION

AUTHENTICATION WIZARD

Objective: Redirect unauthenticated users to the captive portal.
For example, during the initial authentication or after the expiry of the session.

SOURCE

Who: Unauthenticated users
From: Network_internals

DESTINATION

Destination: Internet
Except for URLs: authentication_bypass

Graphical_client_A [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 ✎ AUTHENTICATION ✎ +

← → C Not secure | https://192.168.1.254/admin/admin.html#securitypolicy/local/7/filter

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

EVA1 VMSNSX09K0639A9

MONITORING CONFIGURATION

SECURITY POLICY / FILTER - NAT

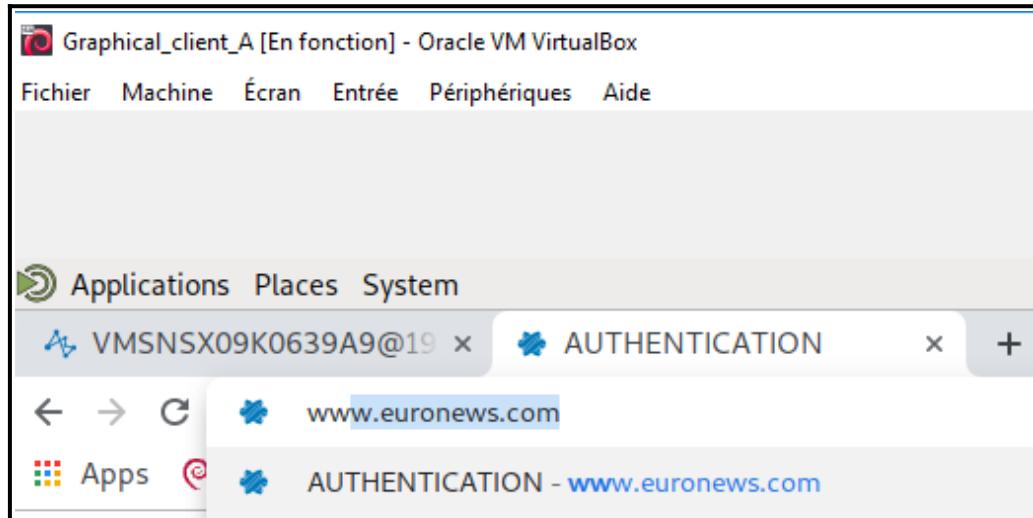
Lab_7 Edit Export

FILTERING NAT

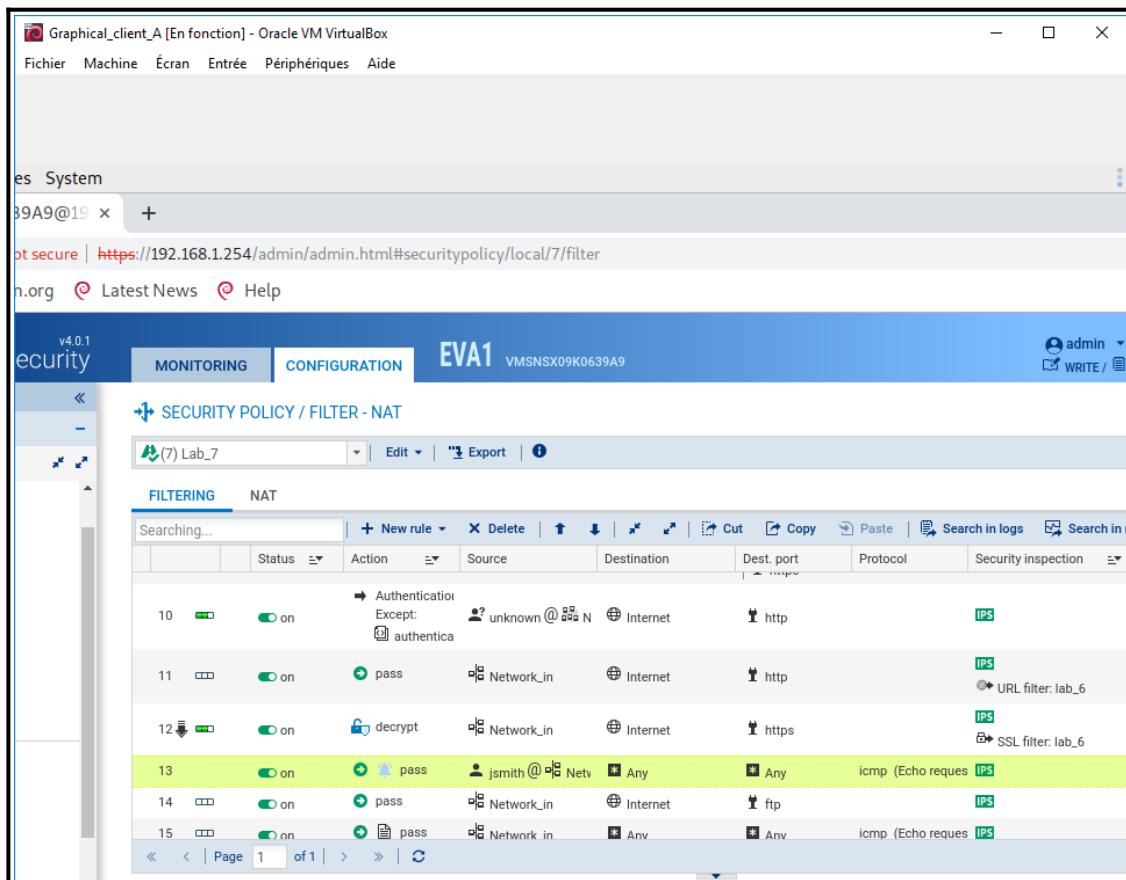
TRAFFIC SORTANT - Updated on 2022-09-22 13:53:53 by admin (192.168.1.2) - Updated on 2022-09-29 11:10:41 by admin (192.168.1.2)

	Status	Action	Source	Destination	Dest. port	Protocol
8	on	block	Network_in	Internet		http https
9	on	block	Network_in	www.edition.cnn.co		http https
10	on	Authentication	unknown @	Internet		http

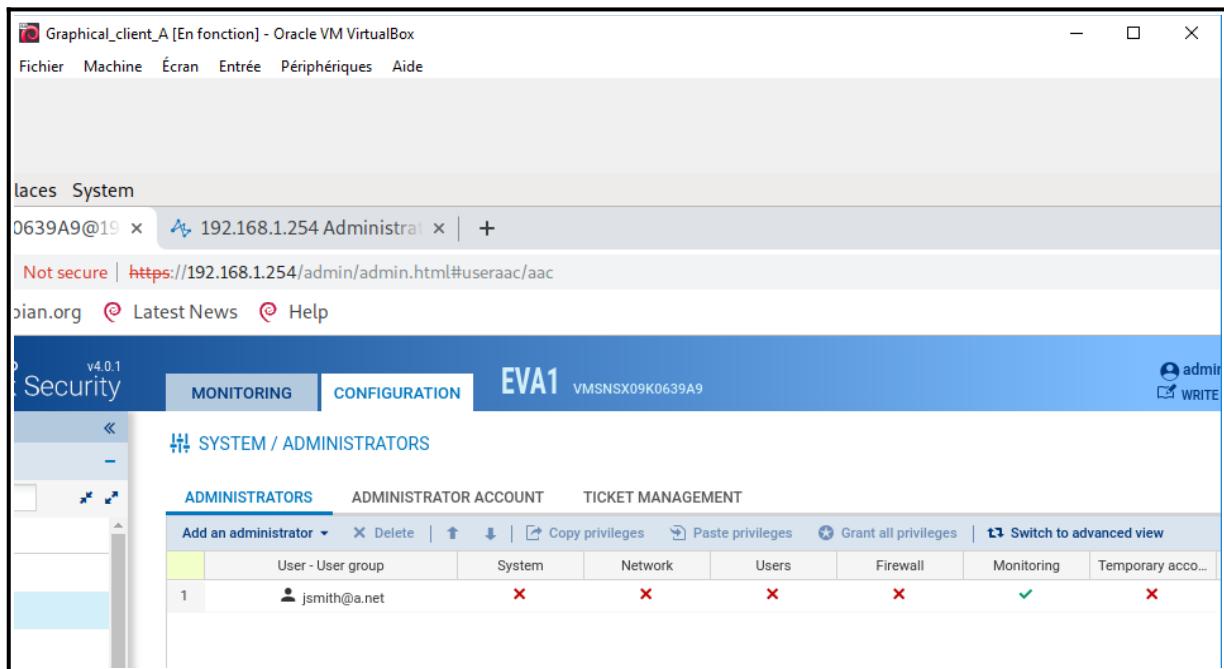
Except: unknown @ Internet authentication_bypass



5ème étape : Après avoir adapté la politique de filtrage afin que les utilisateurs voulant accéder à un site web en HTTP soit redirigé vers le portail captif. Nous effectuons les tests.



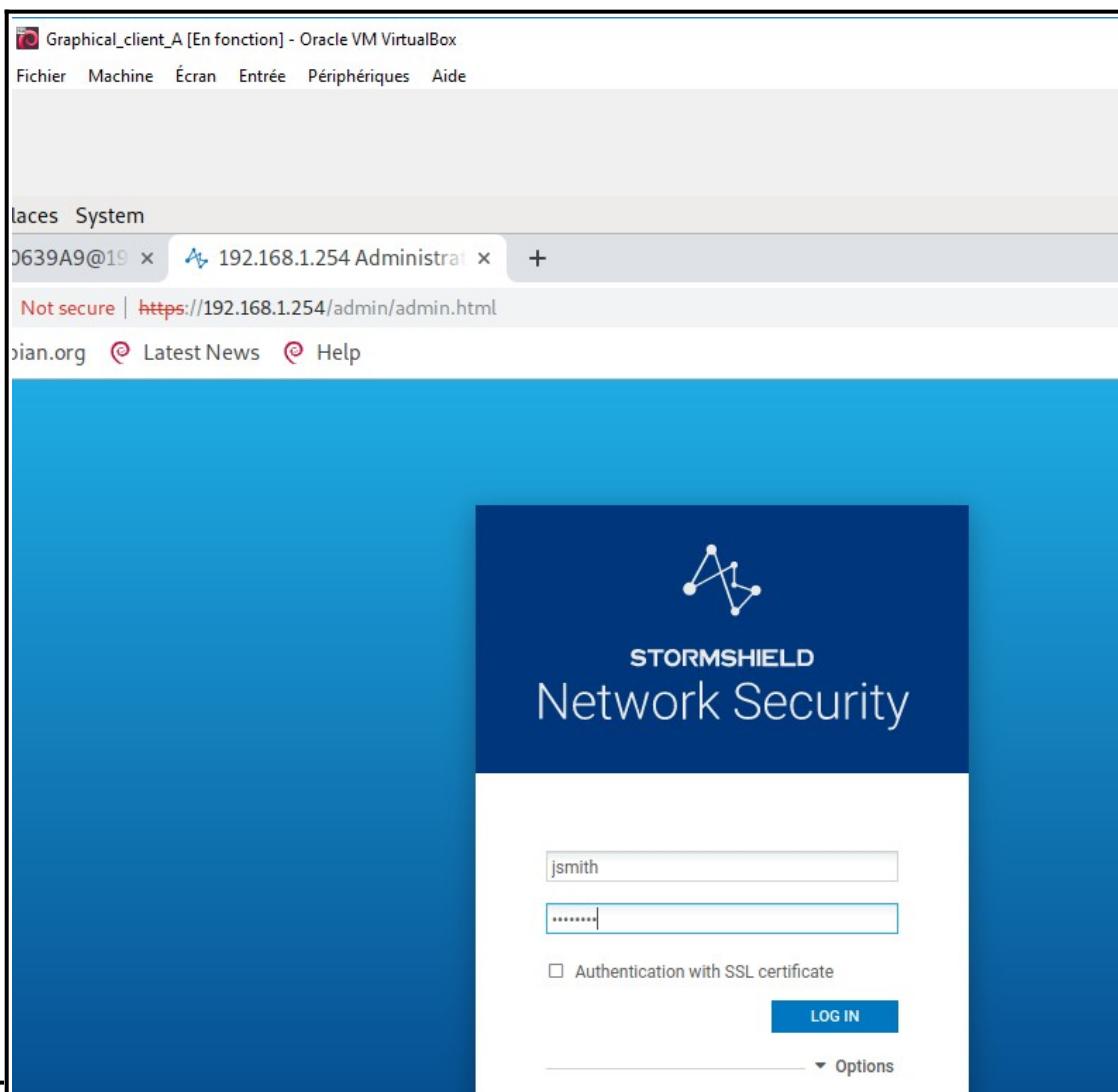
6ème étape : Nous mettons en place une règle de filtrage pour l'utilisateur John Smith.



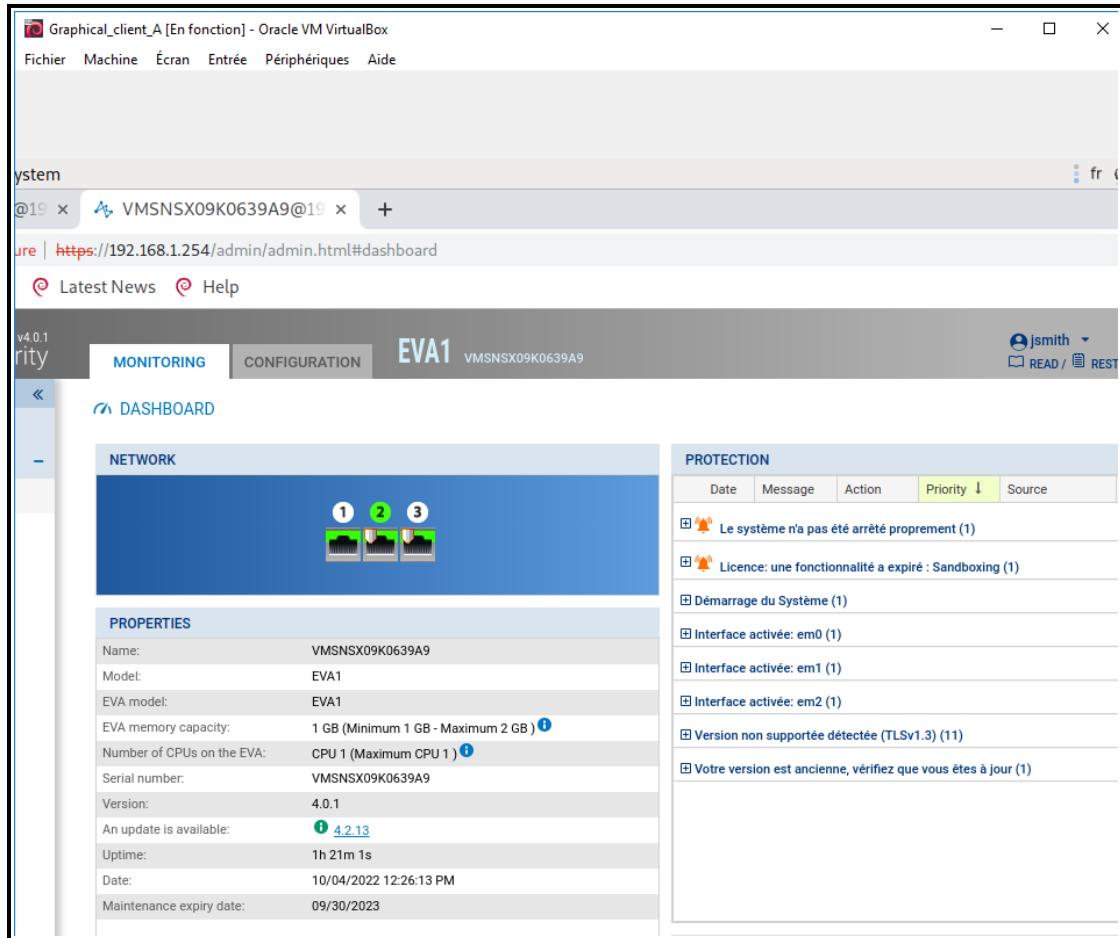
The screenshot shows the EVA1 web interface. The top navigation bar includes 'Fichier', 'Machine', 'Écran', 'Entrée', 'Périphériques', and 'Aide'. Below this is a sub-navigation bar with 'Places', 'System', and a connection status '0639A9@19 x 192.168.1.254 Administral x | +'. A message 'Not secure | https://192.168.1.254/admin/admin.html#useraac/aac' is displayed. The main content area has tabs 'MONITORING' (selected), 'CONFIGURATION', and 'EVA1 VMSNSX09K0639A9'. On the right, a user 'admin' with 'WRITE' privileges is shown. The central part of the screen is titled 'SYSTEM / ADMINISTRATORS' with sub-tabs 'ADMINISTRATORS', 'ADMINISTRATOR ACCOUNT', and 'TICKET MANAGEMENT'. A table lists one administrator:

User - User group	System	Network	Users	Firewall	Monitoring	Temporary acco...
1 jsmith@a.net	✗	✗	✗	✗	✓	✗

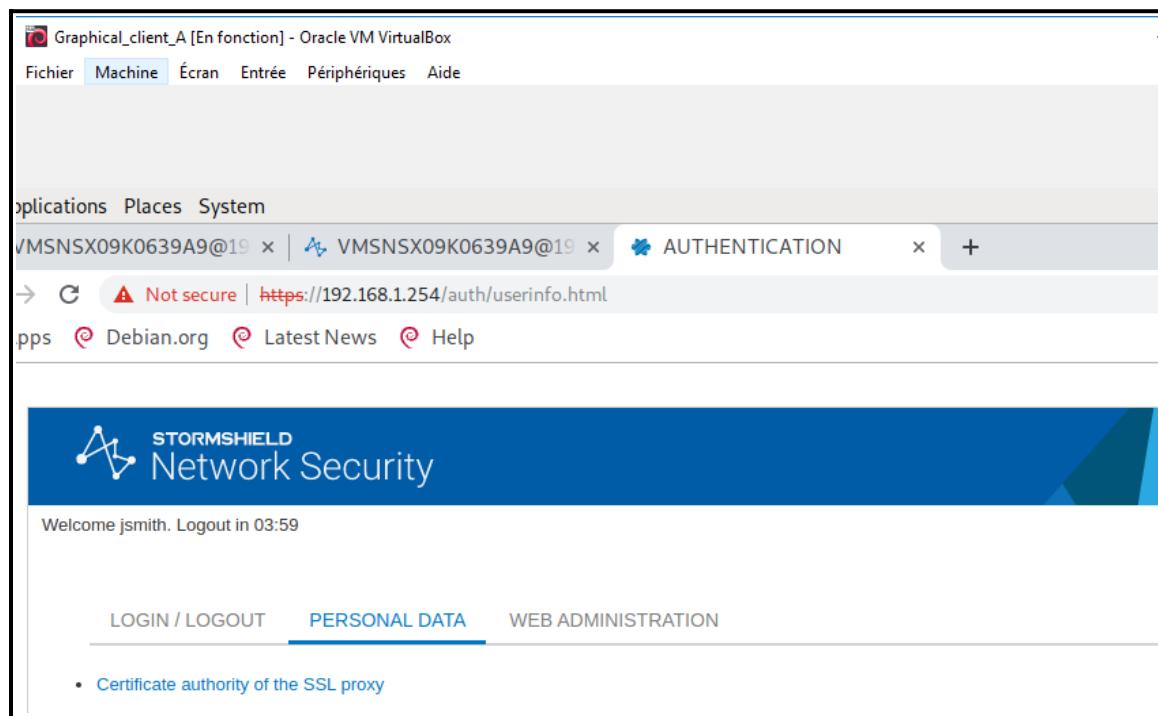
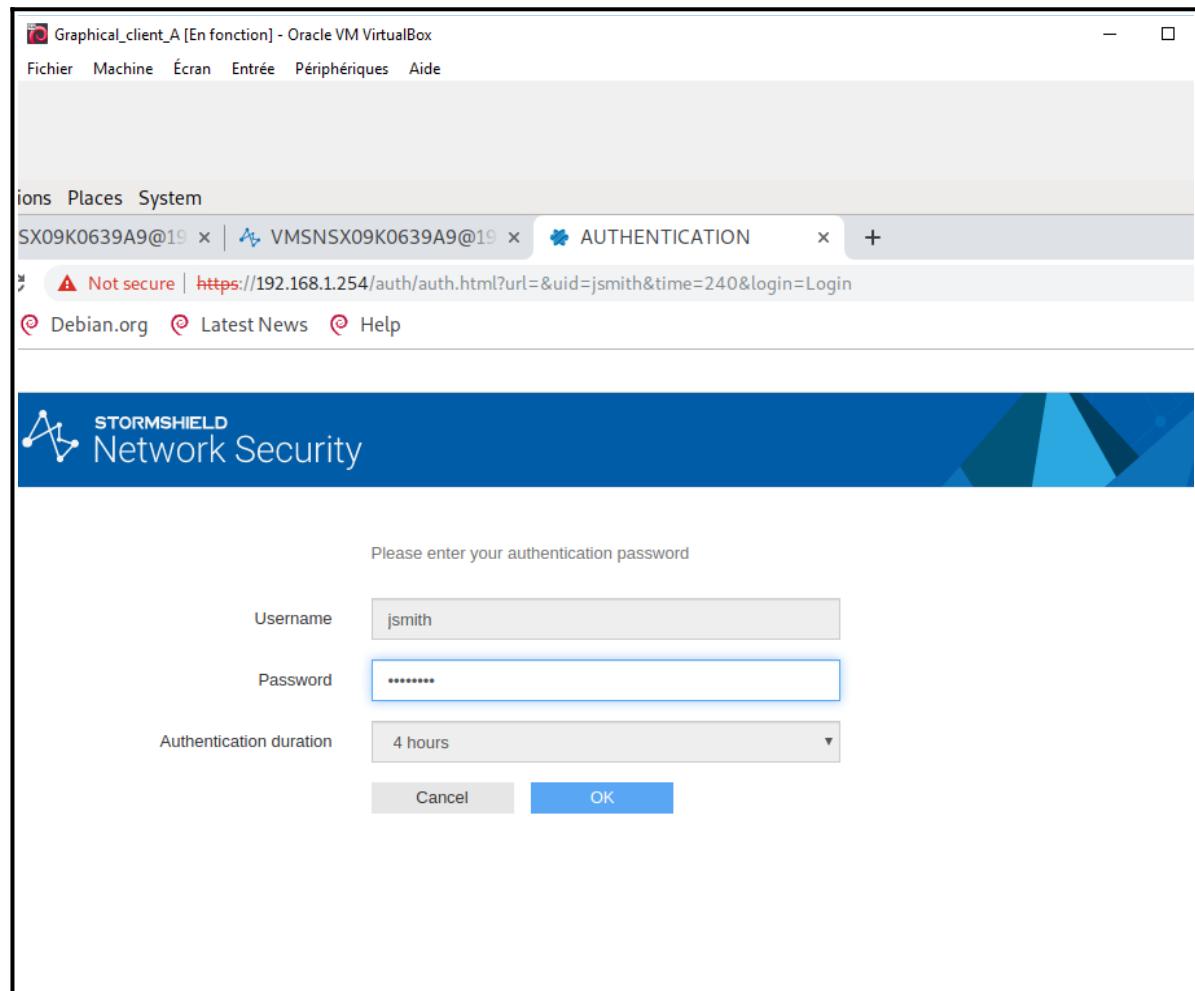
7ème étape : Nous accordons les droits de supervision à l'utilisateur John Smith.



The screenshot shows a web browser window with the address bar showing '0639A9@19 x 192.168.1.254 Administral x | +'. The page content is a login screen for 'STORMSHIELD Network Security'. It features a logo of a network of lines and dots, the text 'STORMSHIELD Network Security', and a login form with fields for 'jsmith' and '.....'. A checkbox for 'Authentication with SSL certificate' is present, along with 'LOG IN' and 'Options' buttons.

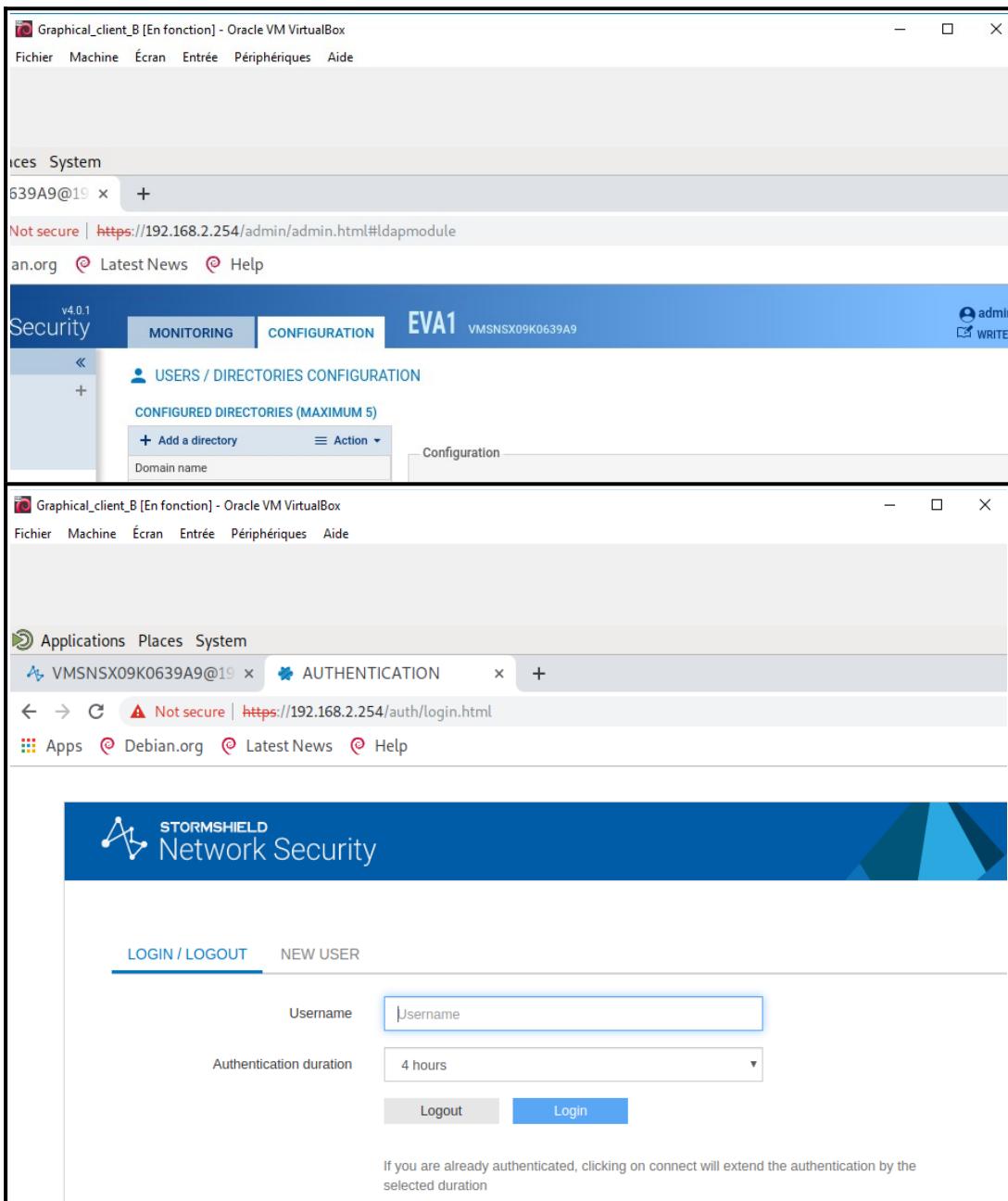


8ème étape : Connexion au firewall avec l'utilisateur John Smith, nous constatons que celui-ci possède seulement les droits de supervision.



9ème étape : Test de connexion au portail captif avec l'utilisateur John Smith.

Réseau B :

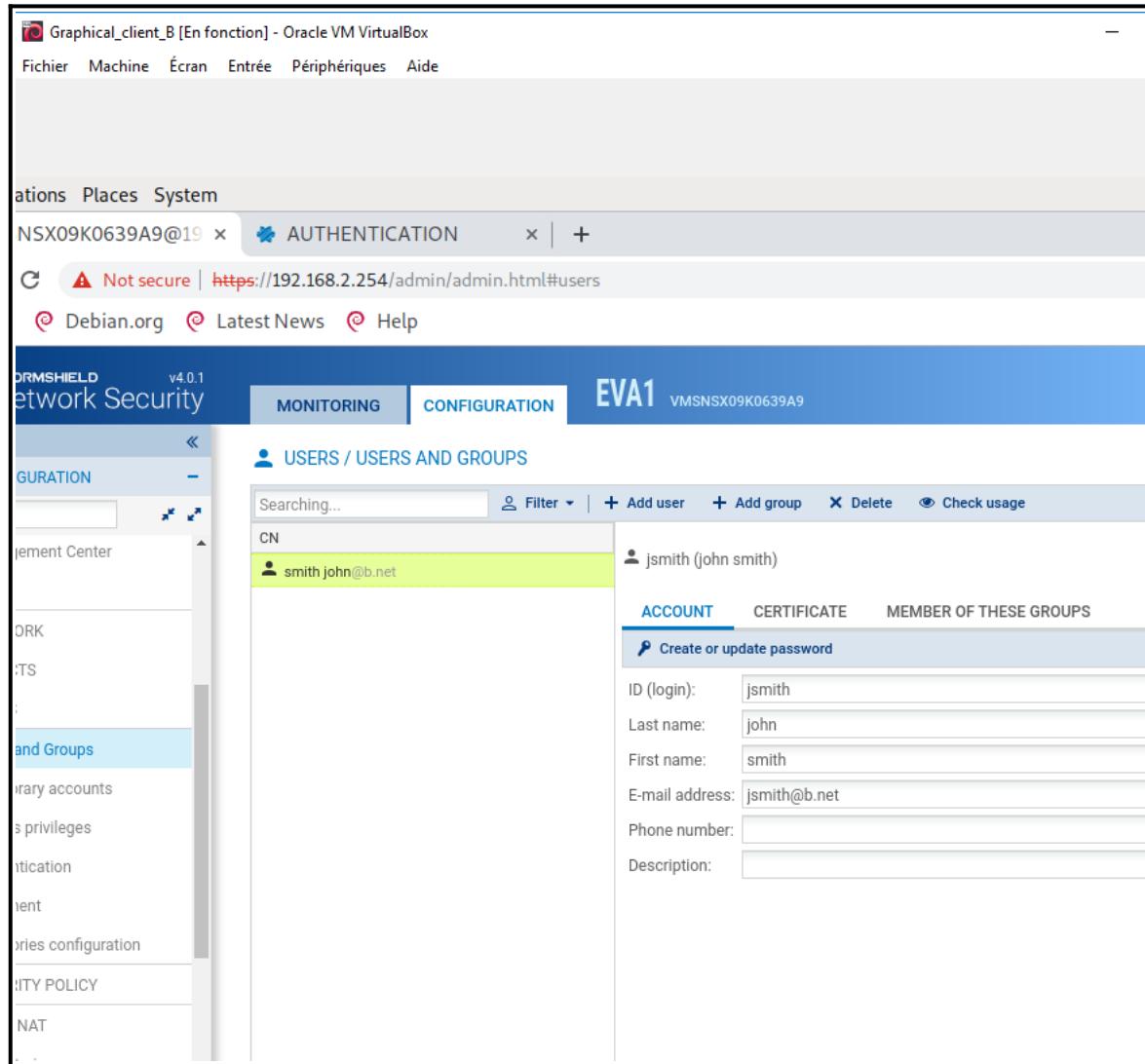


The screenshot shows a Linux desktop environment with two windows open:

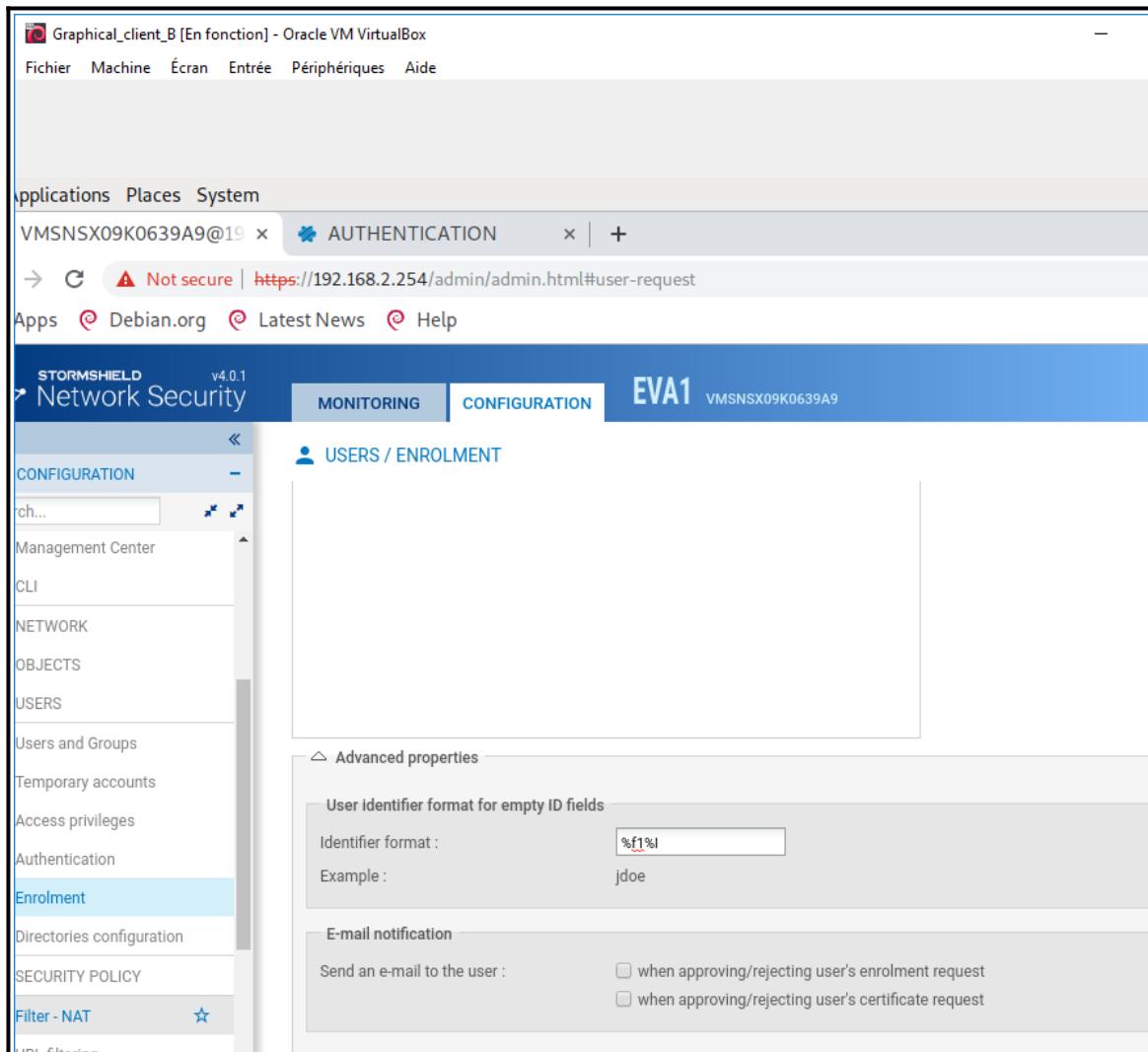
- Top Window:** A web browser window titled "Graphical_client_B [En fonction] - Oracle VM VirtualBox". The address bar shows "Not secure | https://192.168.2.254/admin/admin.html#ldapmodule". The content of the page is the "USERS / DIRECTORIES CONFIGURATION" section of the EVA1 interface, showing a table with one row: "+ Add a directory" and "Domain name".
- Bottom Window:** A web browser window titled "Graphical_client_B [En fonction] - Oracle VM VirtualBox". The address bar shows "Not secure | https://192.168.2.254/auth/login.html". The content is the "STORMSHIELD Network Security" login page, featuring a "LOGIN / LOGOUT" tab and a "NEW USER" tab. It includes fields for "Username" (with a placeholder "Username") and "Authentication duration" (set to "4 hours").

1ère étape : Création d'une base LDAP interne :

- Organisation B, domaine « net ».
- Activation du profil d'authentification, ainsi que l'enrôlement des utilisateurs.
- Test du portail captif.



2ème étape : Création de l'utilisateur John Smith.



Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 ✎ AUTHENTICATION ✎ +

◀ ▶ ⏪ ⏪ Not secure | <https://192.168.2.254/auth/newuser.html>

apps Debian.org Latest News Help

 STORMSHIELD Network Security

LOGIN / LOGOUT NEW USER

Please enter all the required information

Last Name *

First name *

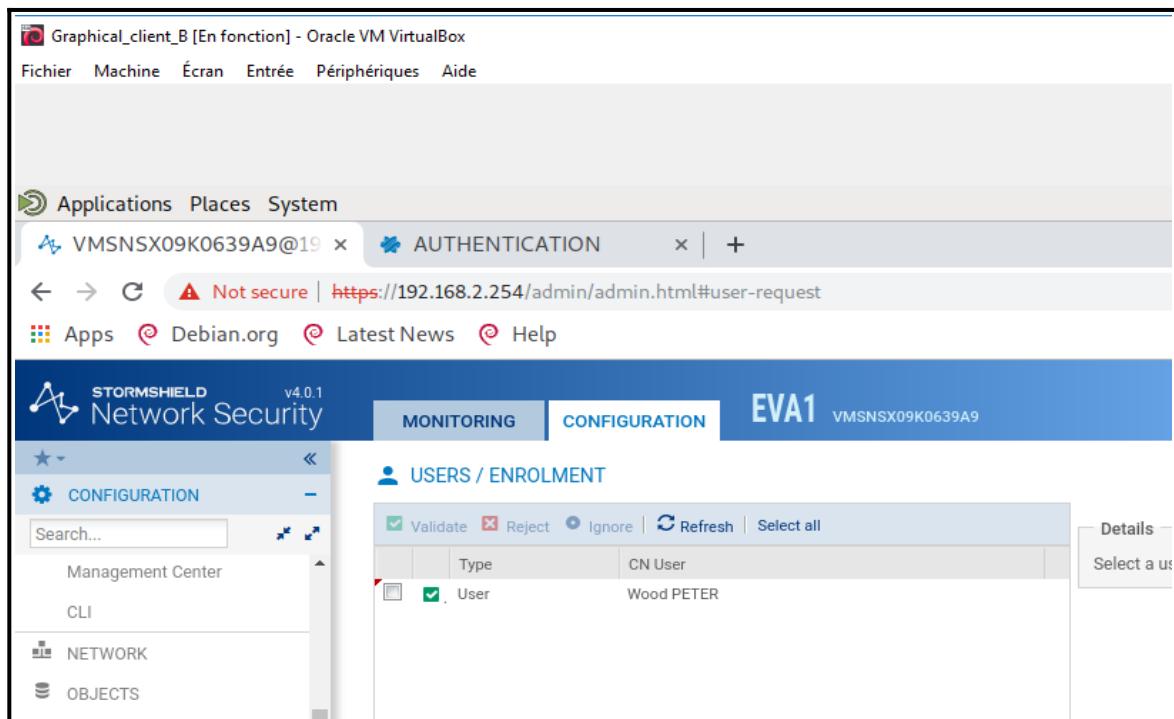
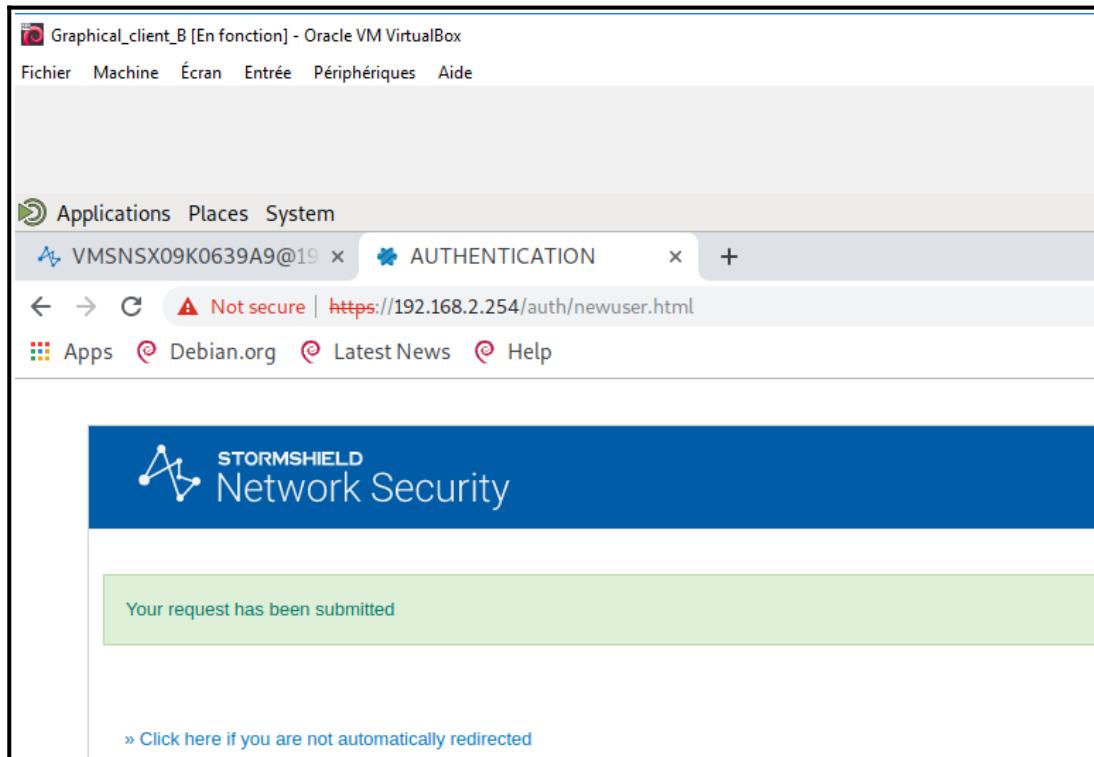
E-mail address *

Description

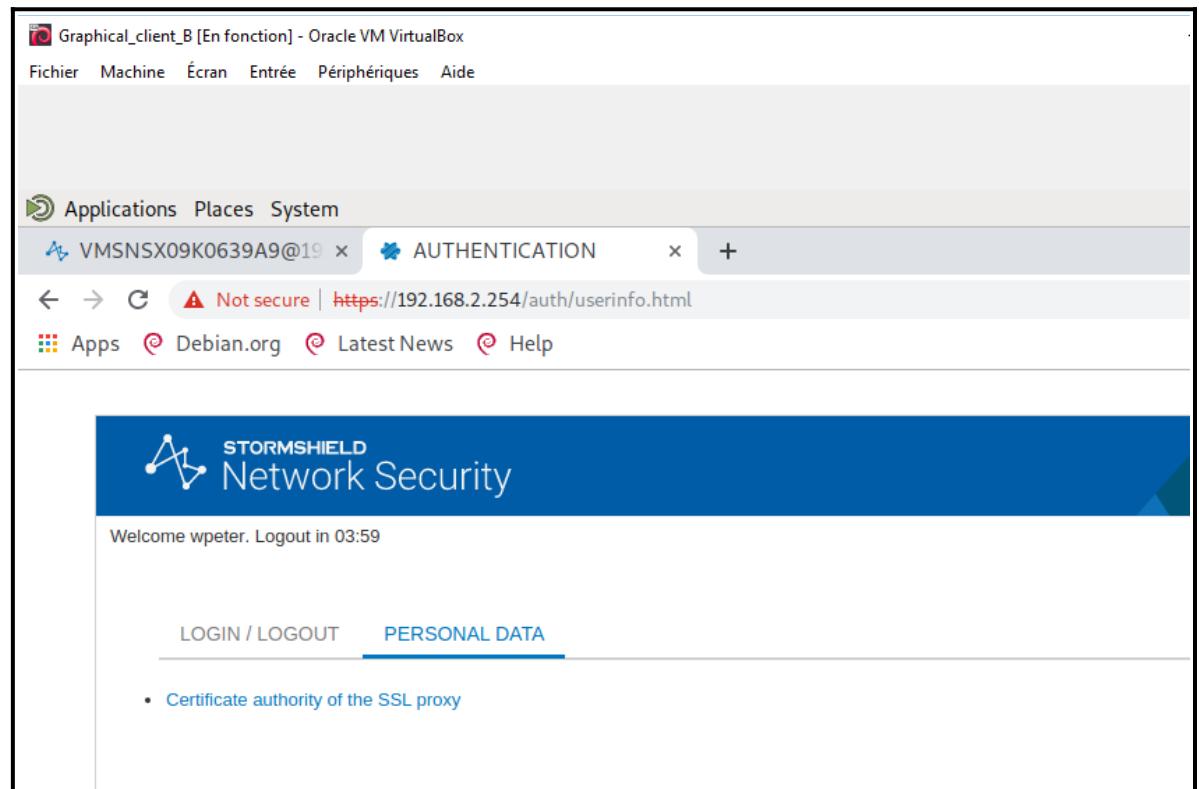
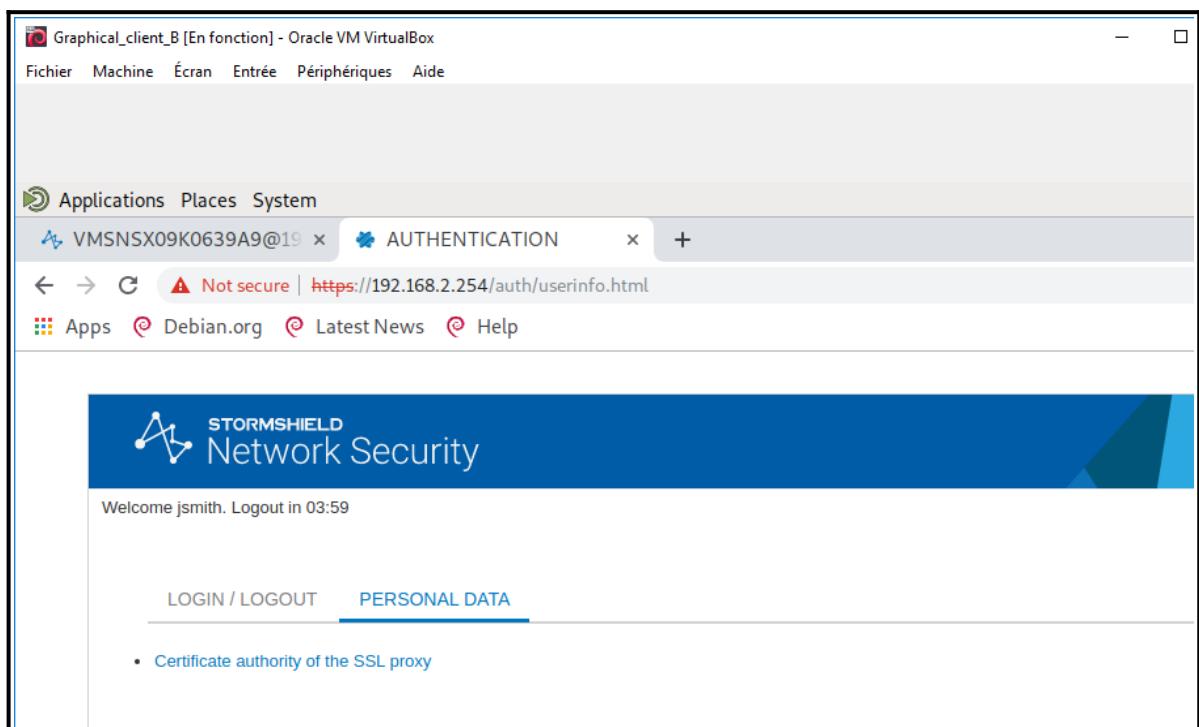
Telephone number

Password **

Confirm password **



3ème étape : En utilisant la fonction d'enrôlement, création de l'utilisateur Peter Wood et tests.



4ème étape : Test de connexion avec l'utilisateur John Smith et Peter Wood.

Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Applications Places System

VMSNSX09K0639A9@19 AUTHENTICATION x | +

← → C Not secure | <https://192.168.2.254/admin/admin.html#securitypolicy/local/7/filter/13>

Apps Debian.org Latest News Help

STORMSHIELD Network Security v4.0.1

EVA1 VMSNSX09K0639A9

MONITORING CONFIGURATION

SECURITY POLICY / FILTER - NAT

7 Lab_7 Edit Export

FILTERING NAT

Search...	Status	Action	Source	Destination	Dest. port	Prot
7	on	pass	Network_in	srv_mail_priv	smtp	
8	on	block	Network_in	Internet geo Corée du Sud	http https	
9	on	block	Network_in	www.edition.cnn.c	http https	
10	on	Authentication	Except: unknown@N	Internet	http	

TRAFFIC SORTANT - Updated on 2022-09-27 11:33:44 by admin (192.168.2.2) - Updated on 2022-09-29 11:14:55 by admin (192.168.2.2)

Management Center

CLI

NETWORK

OBJECTS

USERS

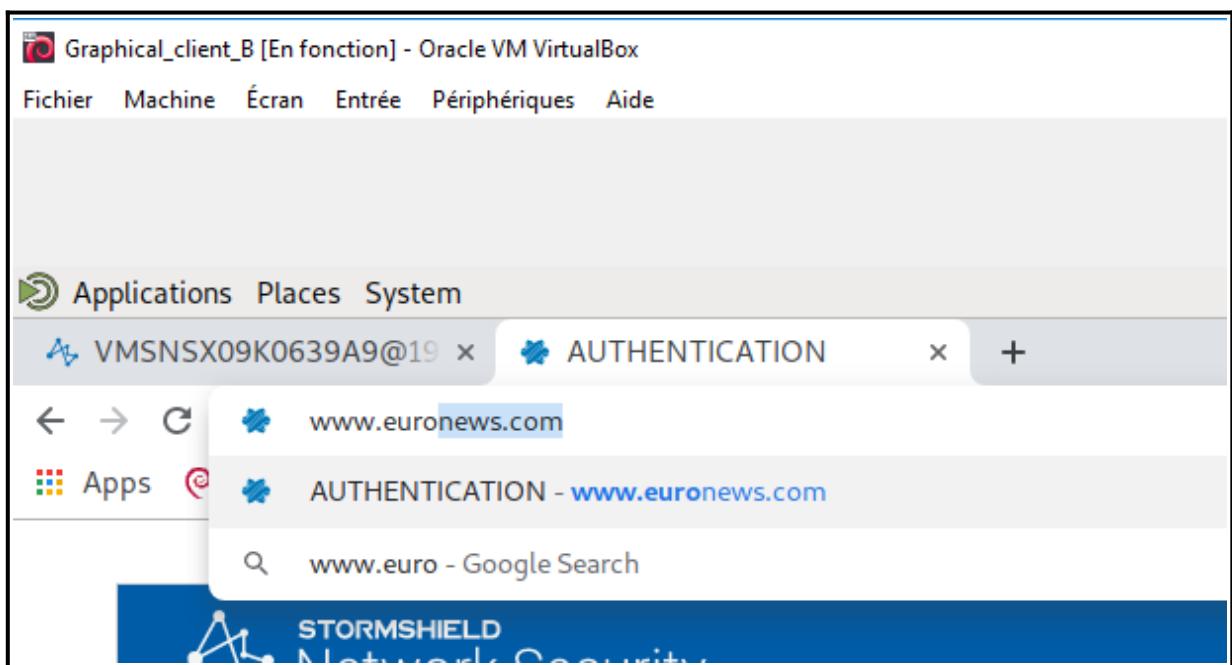
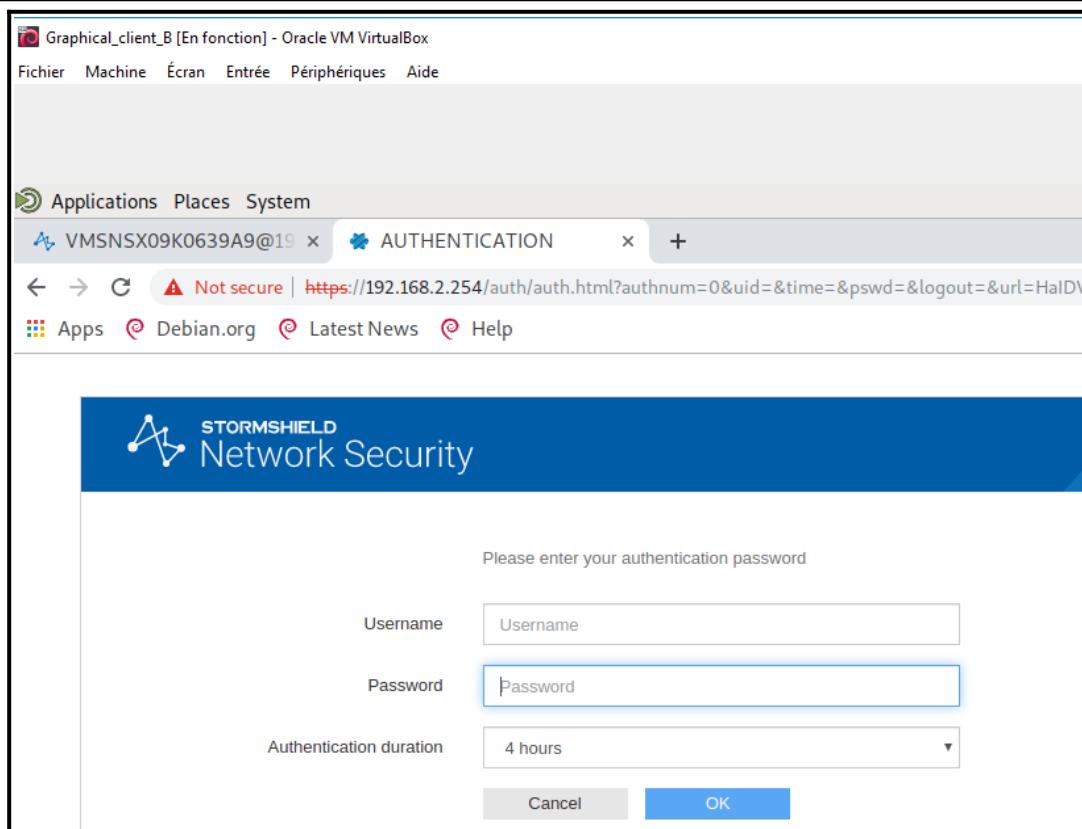
Users and Groups

Temporary accounts

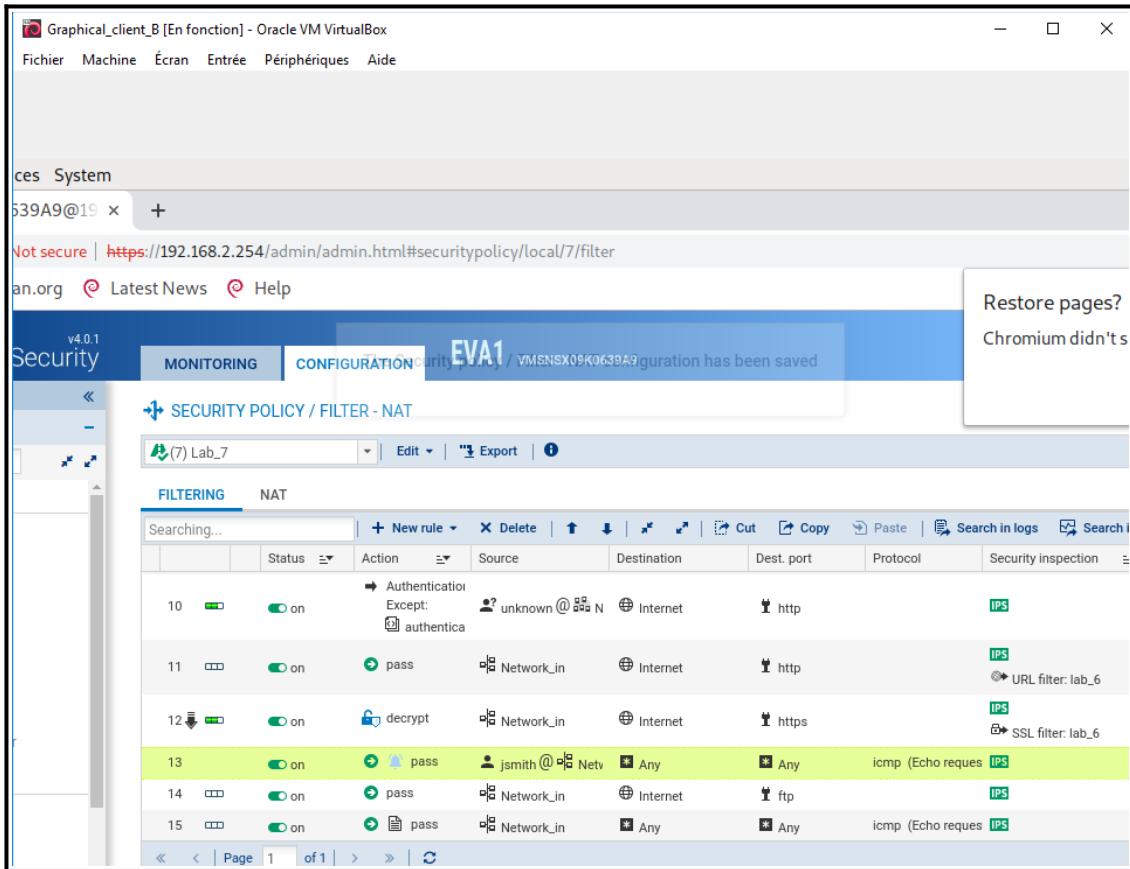
Access privileges

Authentication

Enrolment



5ème étape : Après avoir adapté la politique de filtrage afin que les utilisateurs voulant accéder à un site web en HTTP soit redirigé vers le portail captif. Nous effectuons les tests.



ces System
539A9@19 x +
Not secure | <https://192.168.2.254/admin/admin.html#securitypolicy/local/7/filter>
an.org Latest News Help

v4.0.1 Security MONITORING CONFIGURATION EVA1 / VMSNSX09K0639A9 Configuration has been saved

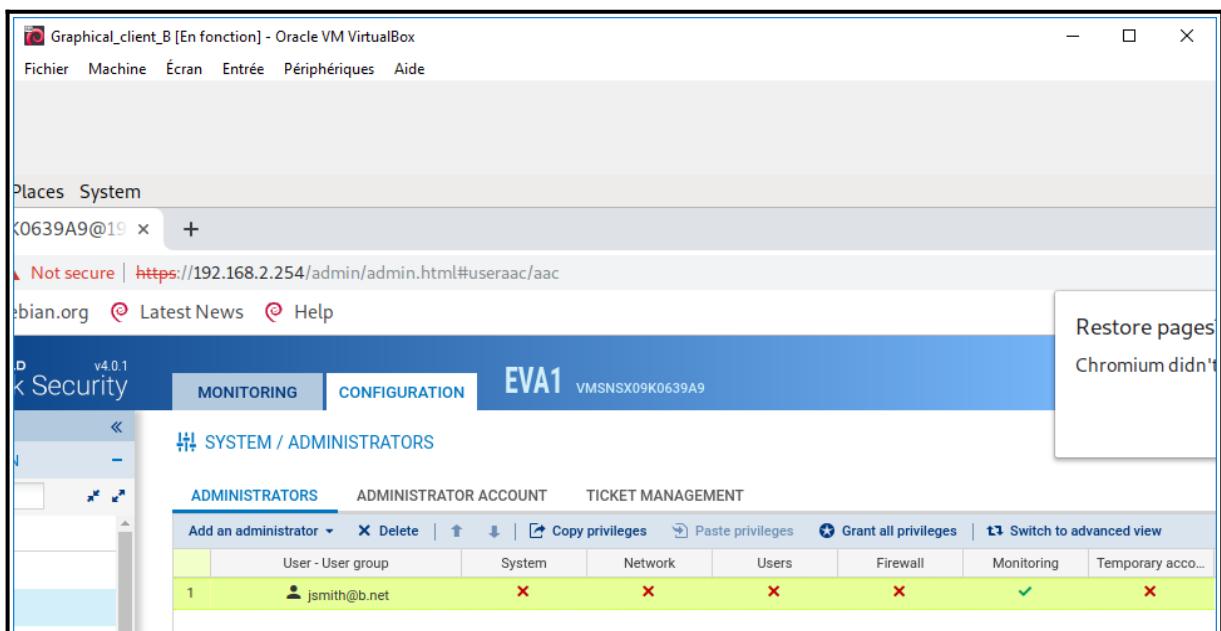
SECURITY POLICY / FILTER - NAT

Lab_7 Edit Export | i

FILTERING NAT

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
10	on	Authentication Except: unknown @ N authentication	Internet		http		IPS
11	on	pass	Network_in	Internet	http		IPS
12	on	decrypt	Network_in	Internet	https		IPS
13	on	pass	jsmith @ Net	Any	Any	icmp (Echo request)	IPS
14	on	pass	Network_in	Internet	ftp		IPS
15	on	pass	Network_in	Any	Any	icmp (Echo request)	IPS

6ème étape : Nous mettons en place une règle de filtrage pour l'utilisateur John Smith.



Places System
0639A9@19 x +
Not secure | <https://192.168.2.254/admin/admin.html#useraac/aac>
bian.org Latest News Help

v4.0.1 Security MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

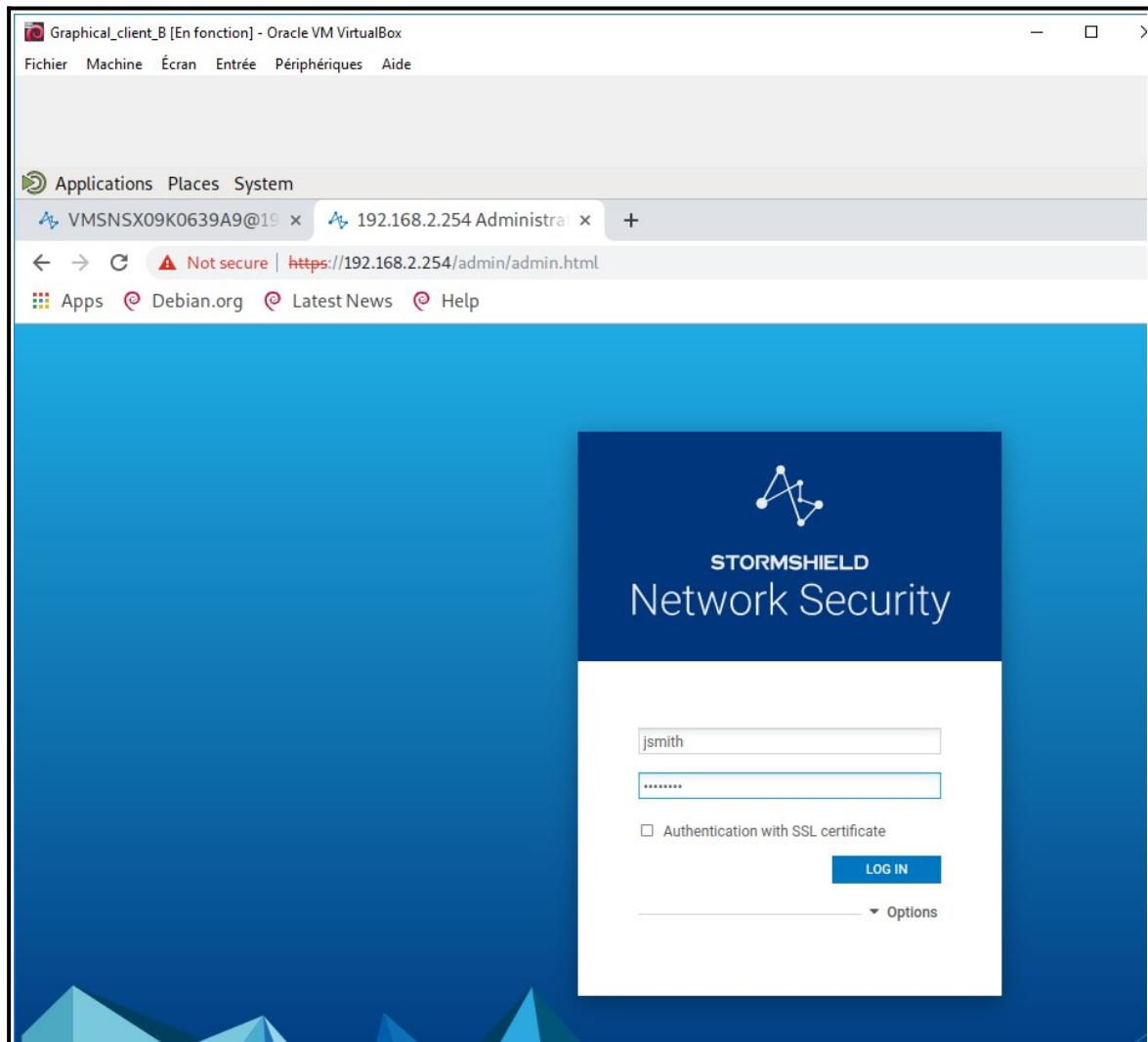
SYSTEM / ADMINISTRATORS

ADMINISTRATORS ADMINISTRATOR ACCOUNT TICKET MANAGEMENT

Add an administrator | X Delete | Copy privileges | Paste privileges | Grant all privileges | Switch to advanced view

	User - User group	System	Network	Users	Firewall	Monitoring	Temporary acco...
1	jsmith@b.net	X	X	X	X	✓	X

7ème étape : Nous accordons les droits de supervision à l'utilisateur John Smith.



Graphical_client_B [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

System A9@19 x VMSNSX09K0639A9@19 x +

secure | <https://192.168.2.254/admin/admin.html#dashboard>

org Latest News Help

v4.0.1 Curity MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 jsmith READ / R

DASHBOARD

NETWORK

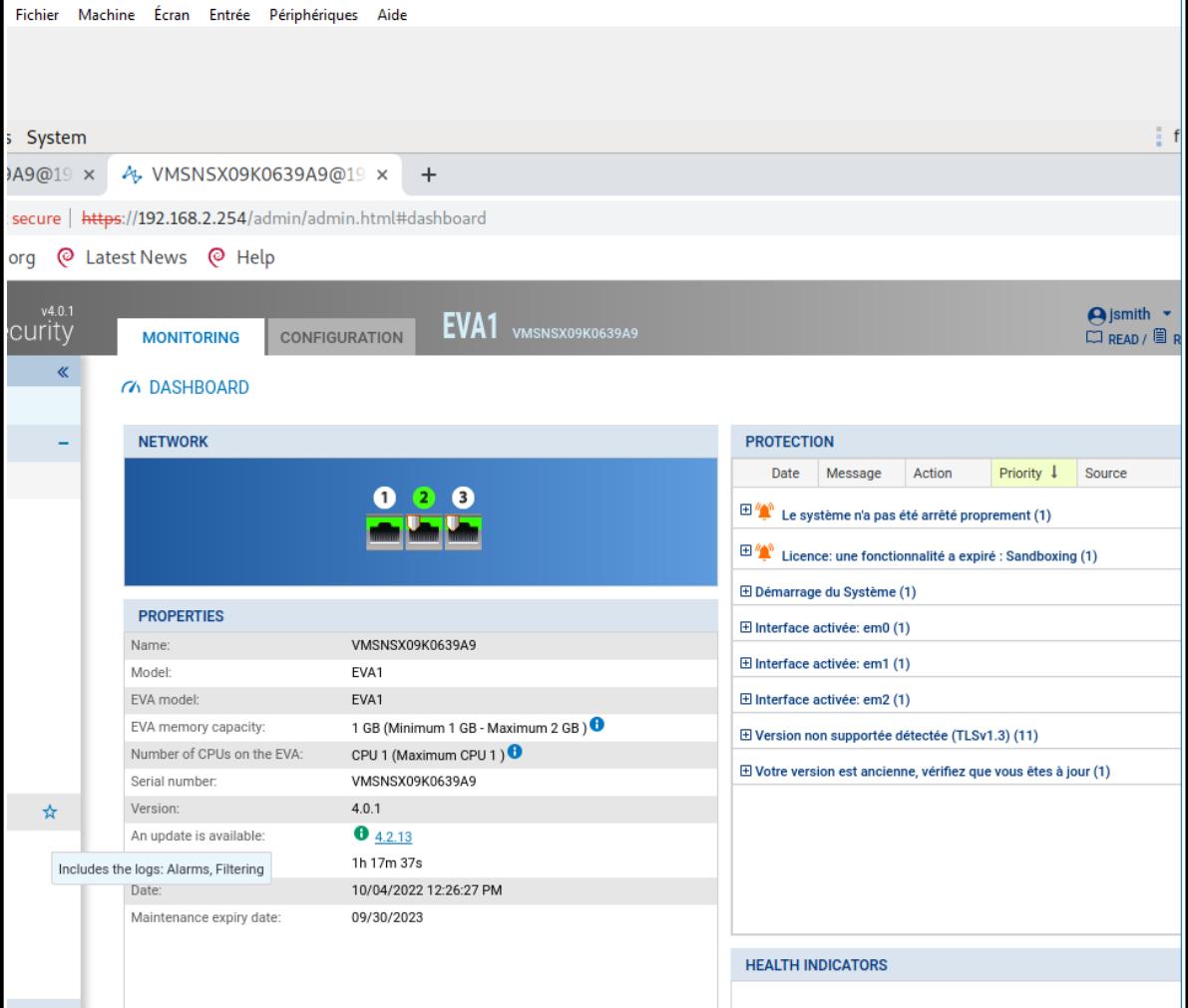
PROTECTION

Date	Message	Action	Priority ↓	Source
Le système n'a pas été arrêté proprement (1)				
Licence: une fonctionnalité a expiré : Sandboxing (1)				
Démarrage du Système (1)				
Interface activée: em0 (1)				
Interface activée: em1 (1)				
Interface activée: em2 (1)				
Version non supportée détectée (TLSv1.3) (11)				
Votre version est ancienne, vérifiez que vous êtes à jour (1)				

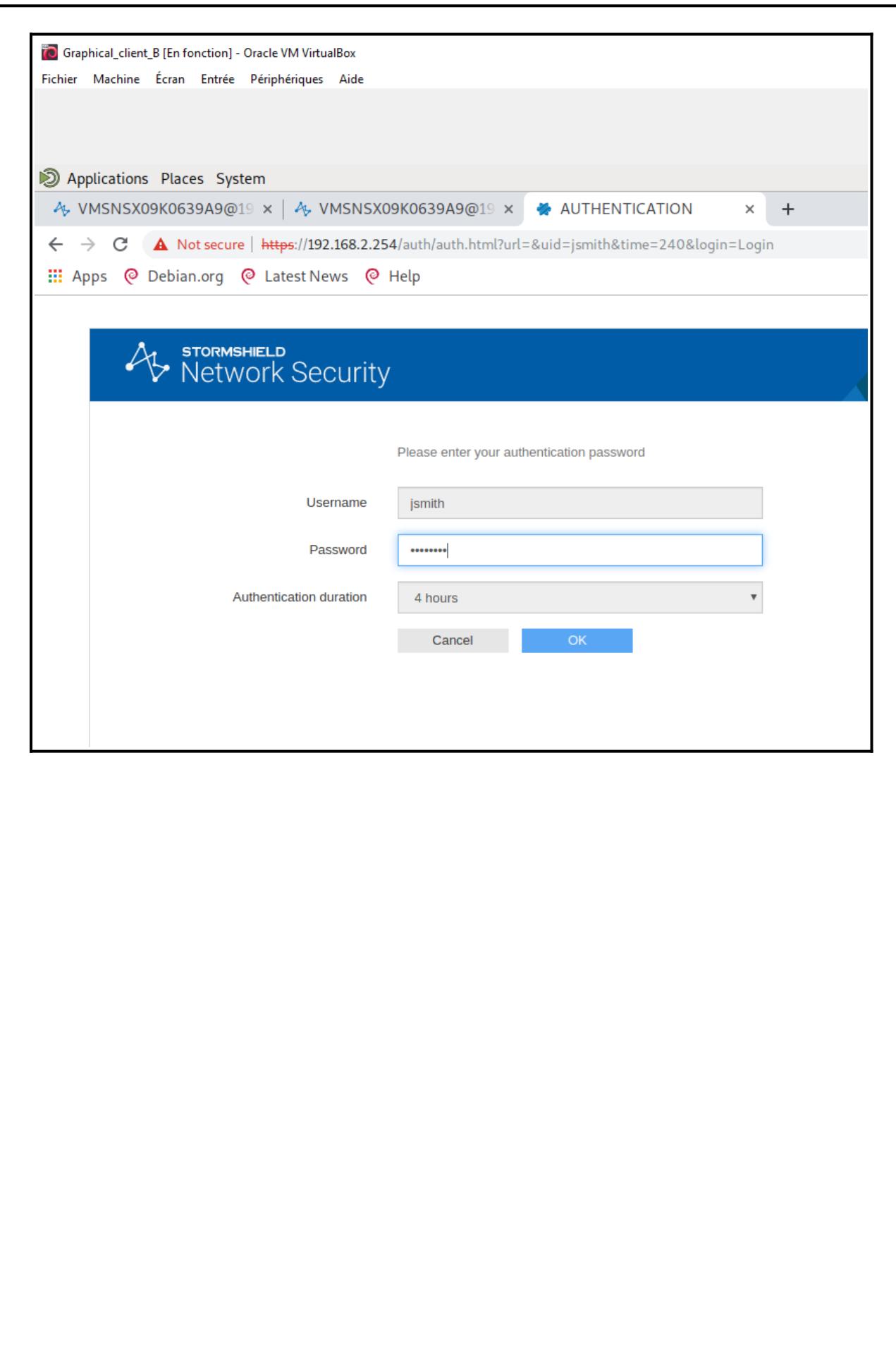
PROPERTIES

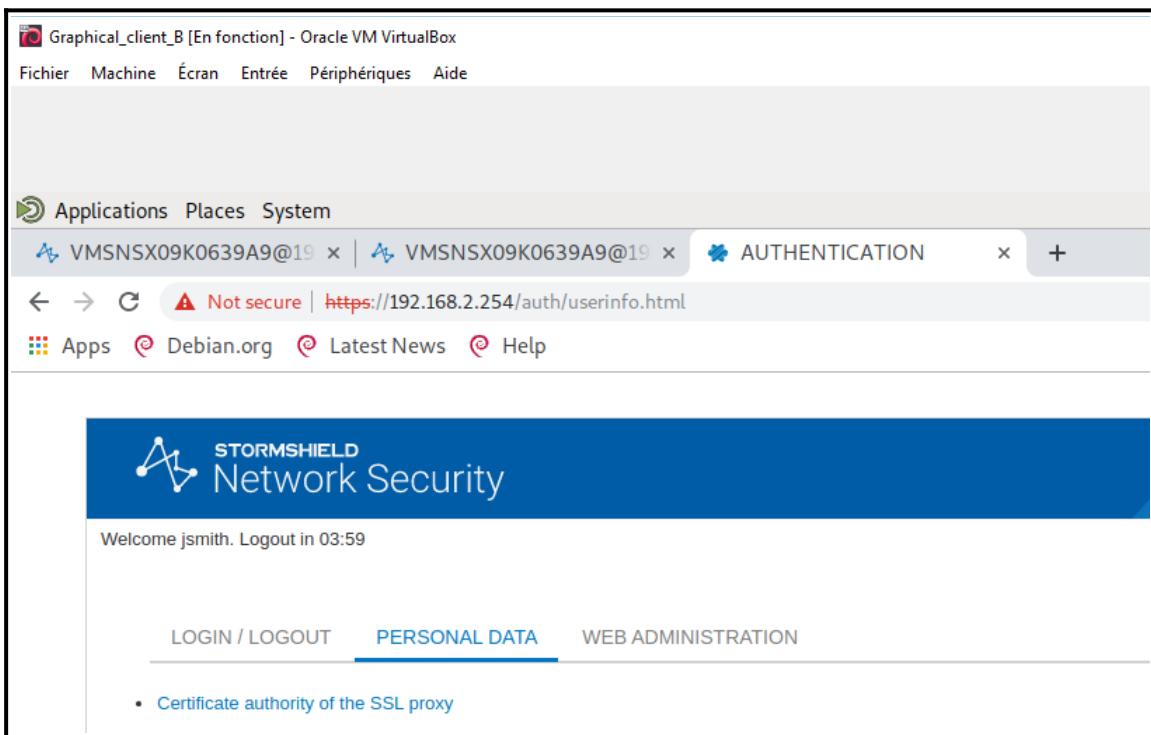
Name:	VMSNSX09K0639A9
Model:	EVA1
EVA model:	EVA1
EVA memory capacity:	1 GB (Minimum 1 GB - Maximum 2 GB) i
Number of CPUs on the EVA:	CPU 1 (Maximum CPU 1) i
Serial number:	VMSNSX09K0639A9
Version:	4.0.1
An update is available:	i 4.2.13
Includes the logs: Alarms, Filtering	1h 17m 37s
Date:	10/04/2022 12:26:27 PM
Maintenance expiry date:	09/30/2023

HEALTH INDICATORS



8ème étape : Connexion au firewall avec l'utilisateur John Smith, nous constatons que celui-ci possède seulement les droits de supervision.





9ème étape : Test de connexion au portail captif avec l'utilisateur John Smith.