WatchGuard Integration

Integration Overview

March 2020

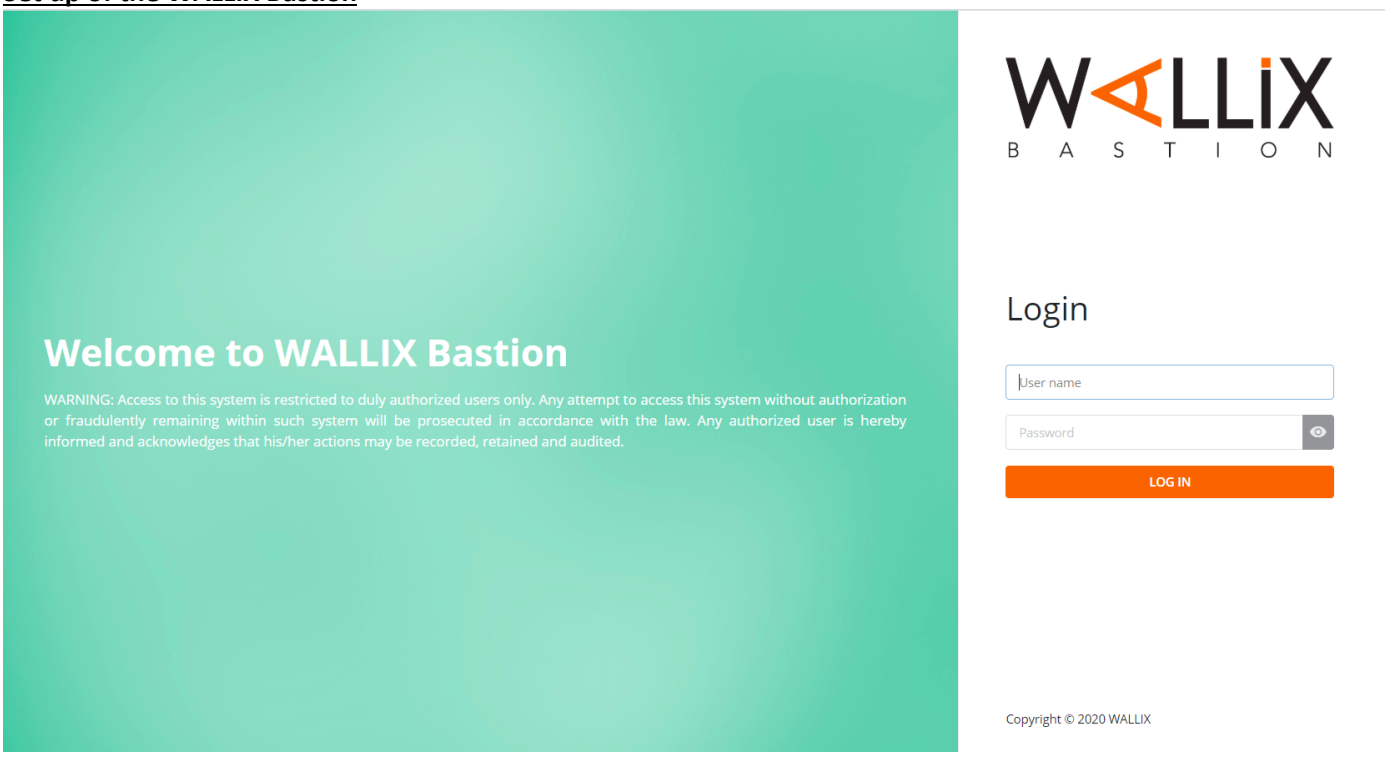
WALLIX
250 bis rue du Faubourg Saint-Honoré 75008 Paris
Tel : +33 1 53 42 12 90 - Fax : +33 1 43 87 66 38
SARL au capital de 50 000 Euros – RCS PARIS B 450 401 153 – FBR67 450 401 153

Integration of WALLIX and WatchGuard

Paris-based WALLIX a software company providing cyber security solutions, WALLIX Group is a European specialist in privileged account governance. In response to recent regulatory change (NIS/GDPR in Europe and OVIs in France) and the cyber security threats affecting all companies today, Bastion helps users protect their critical IT assets: data, servers, terminals and connected objects. It is the first market solution to have been awarded first-level security certification (CSPN) by France's National Cybersecurity Agency (ANSSI) and thus meet all the criteria for regulatory compliance

Seattle-based WatchGuard has deployed nearly a million of its integrated, multi-function threat management appliances worldwide, to businesses that range from SMEs to large distributed enterprises. Recognizing an unmet need for a security solution that addresses the rapidly evolving threat landscape, WatchGuard architected its high-throughput, highly scalable, and flexible Fireware® operating system to form the backbone of its products. This platform yields dramatically higher performance at a much lower cost than competitors in environments where multiple security engines are enabled.
With the ability to record all admin actions and manage passwords on the firewall WALLIX Bastion is the ideal PAM solution to partner with WatchGuard

<u>Set up of the WALLIX Bastion</u>

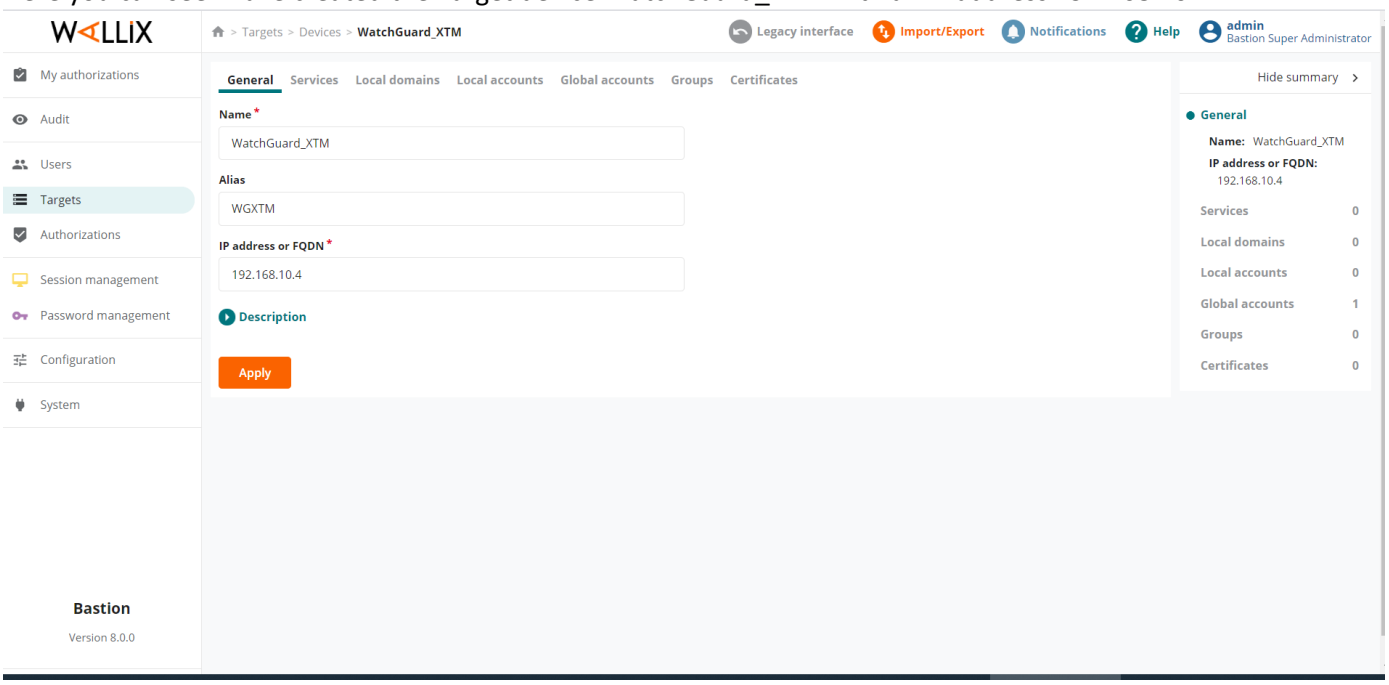


The WALLIX Bastion is setup of rules called authorisations
These authorisations tie User and Target groups together ensuring that only Authenticated and Authorised users have monitored and recorded session access.

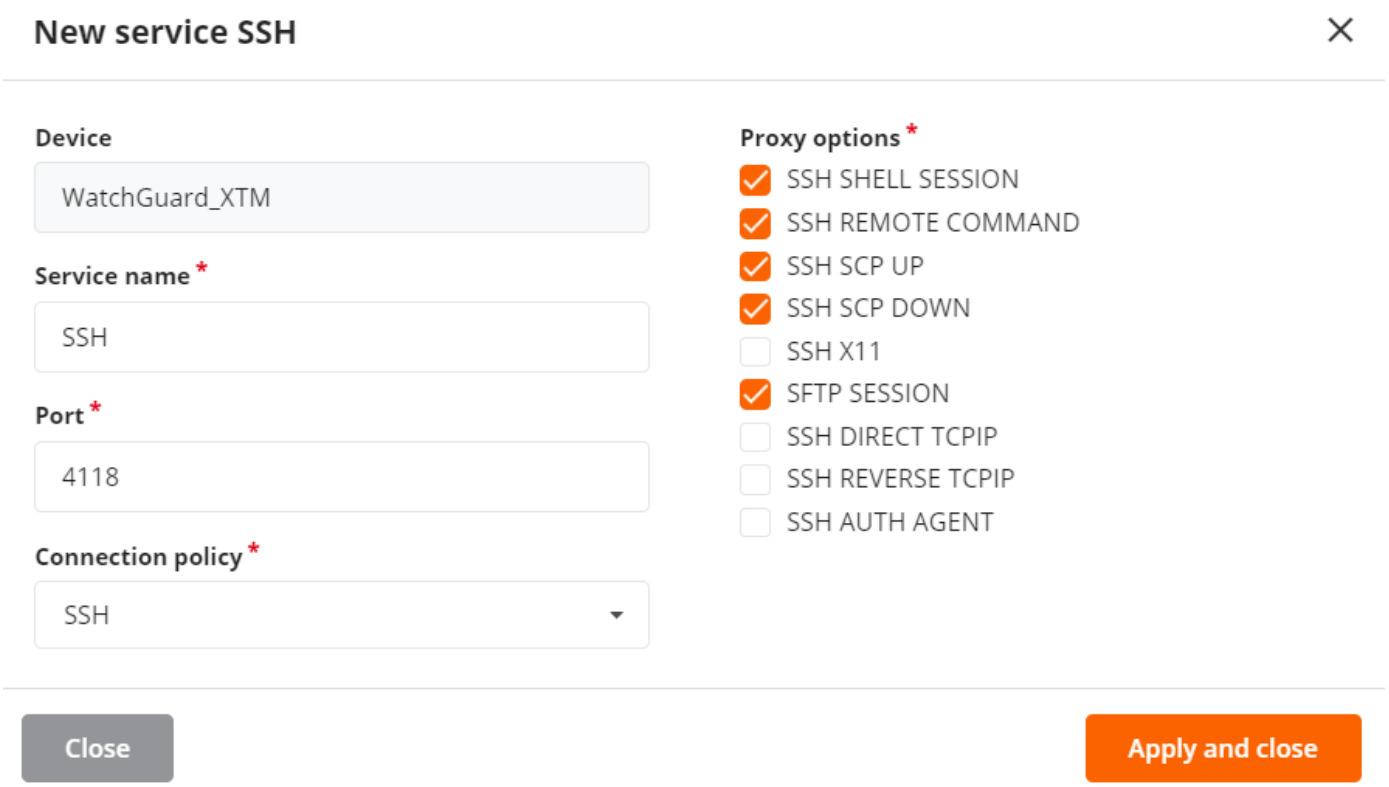
Target Groups

SSH CLI connections

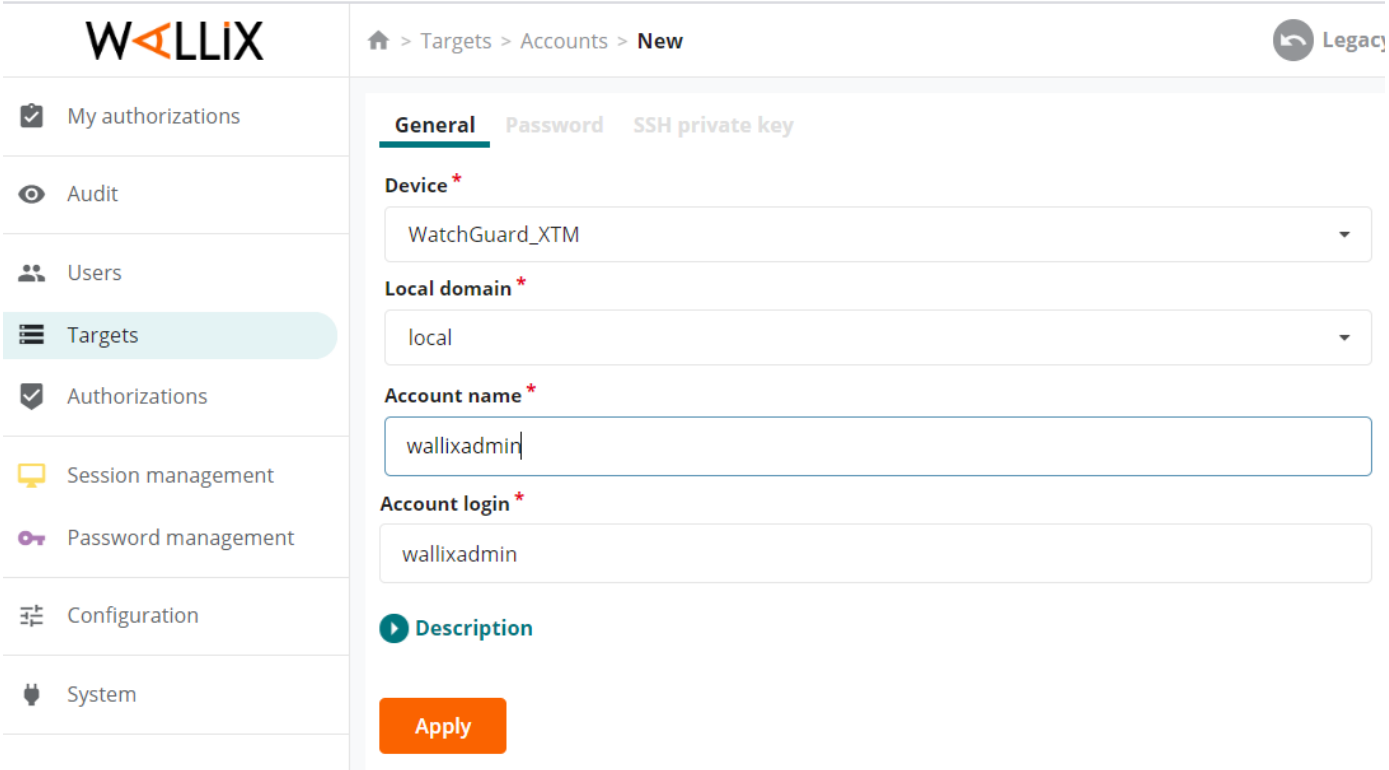
Create a device for the firewall using **SSH 4118**
Here you can see I have created the Target device WatchGaurd_XTM with an IP address 192.168.10.4



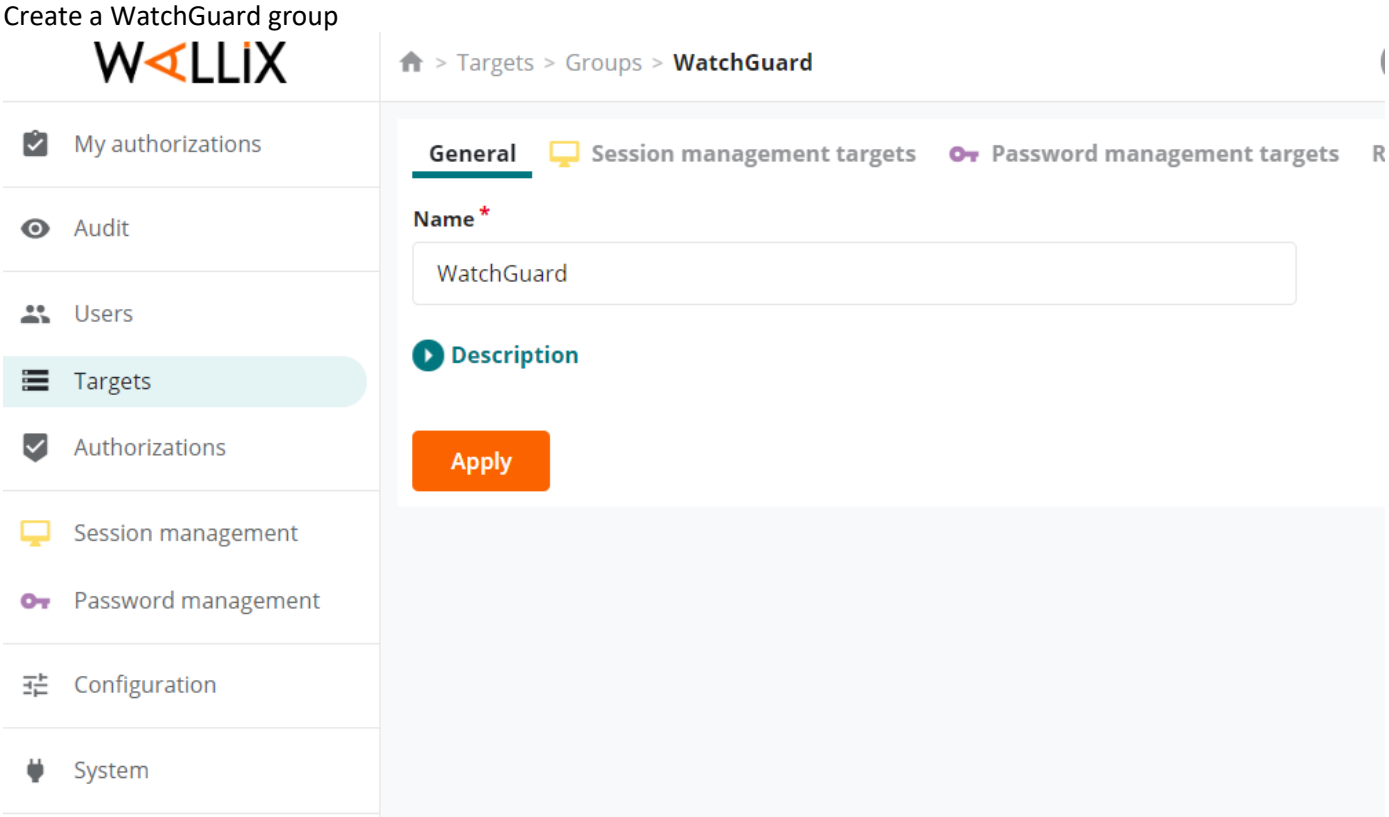
I then create the service
In this case it is SSH using port 4118 (WatchGuard Cli Admin port)



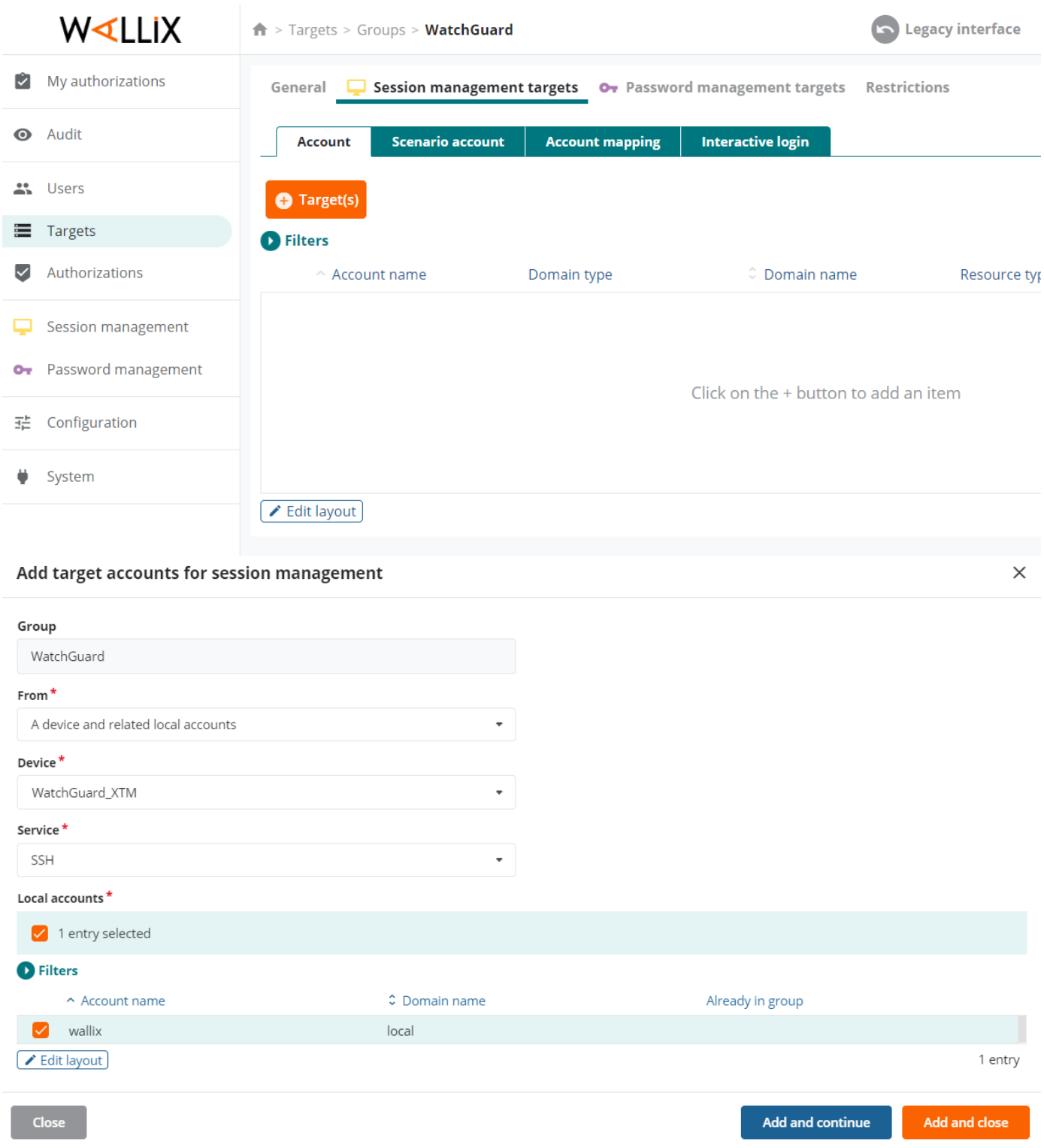
Once the resource has been created you need to create an account associated with the CLI of the firewall
The Bastion will manage the password and user / admin will not know it



A target group is then required
Create a WatchGuard group

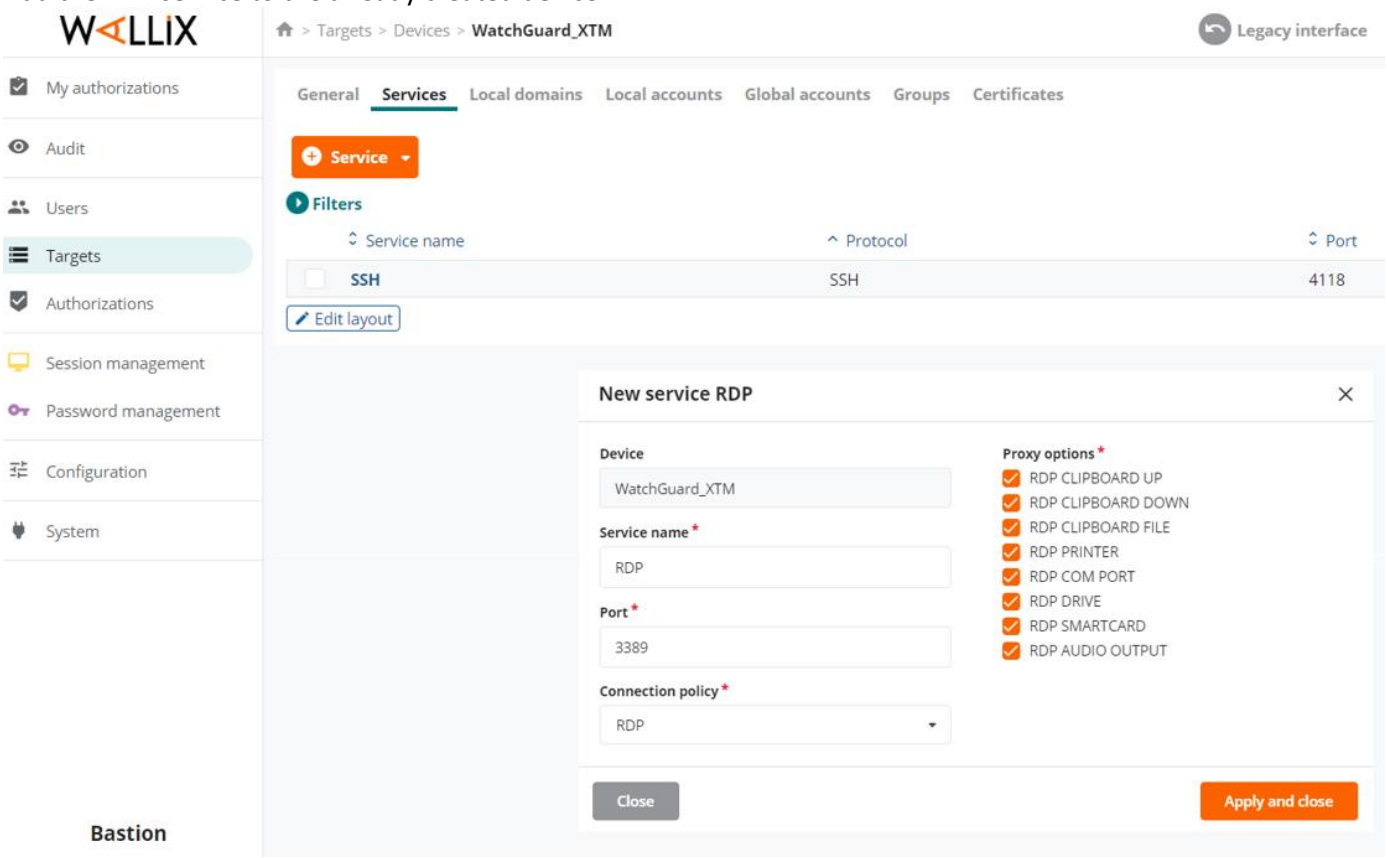


From the WatchGuard group choose the users that will be connecting to the firewall via (in this case) Session Management targets

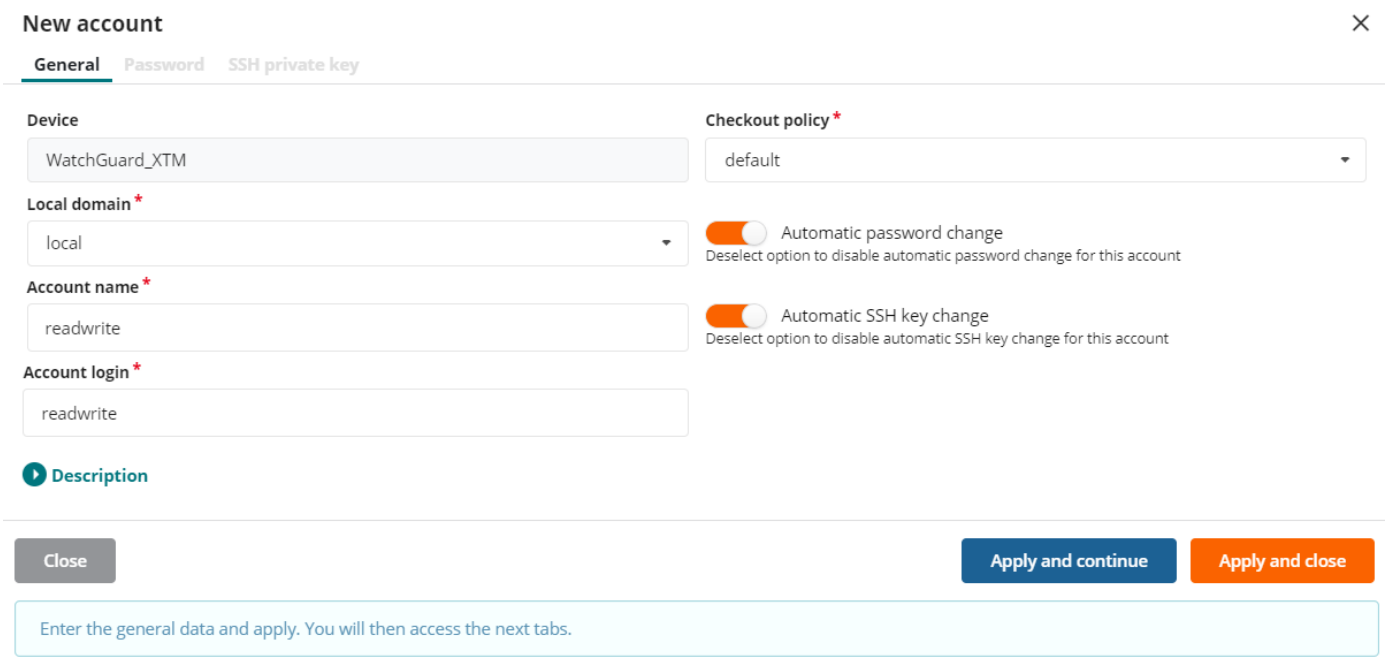


RDP HTTPS Connections

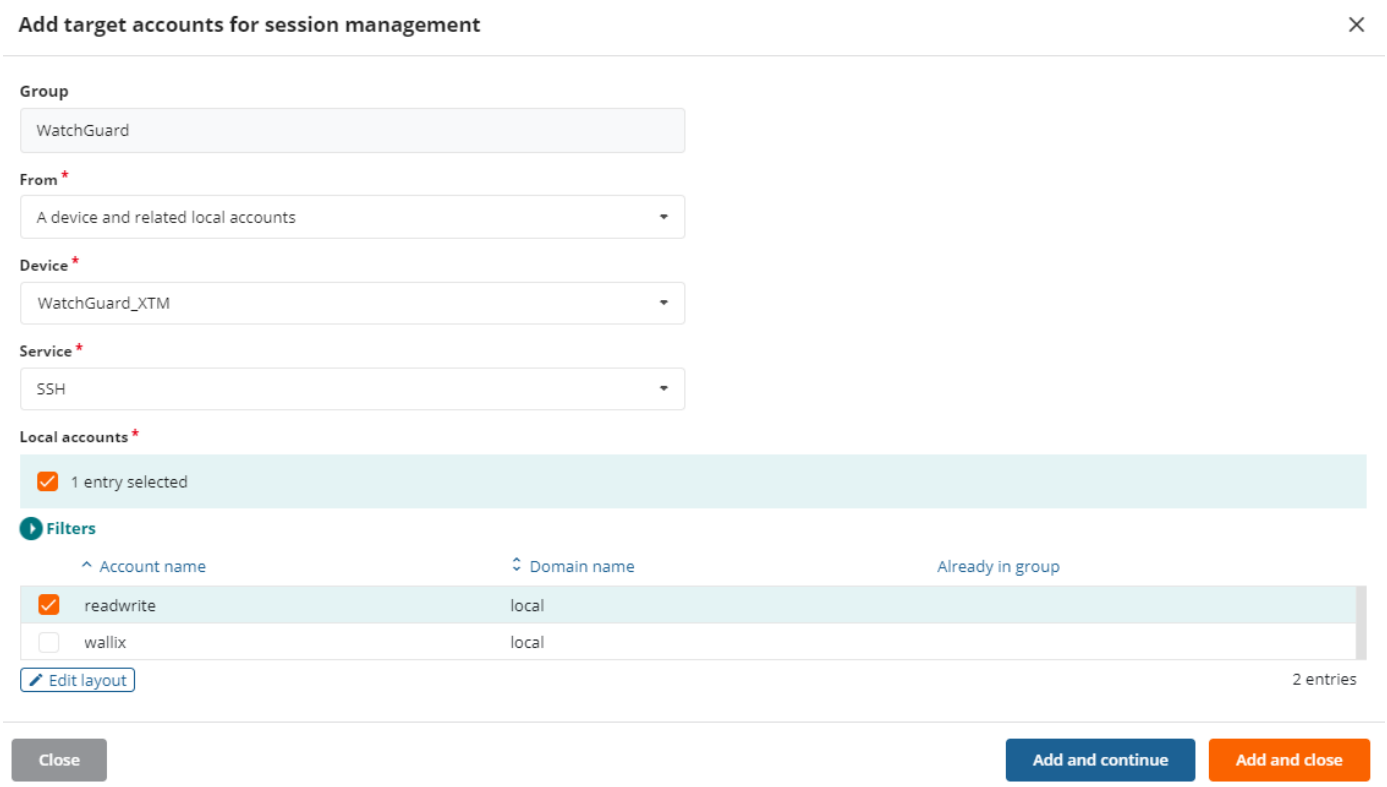
Add the RDP service to the already created device



Create a new account if different from the previously created CLI account

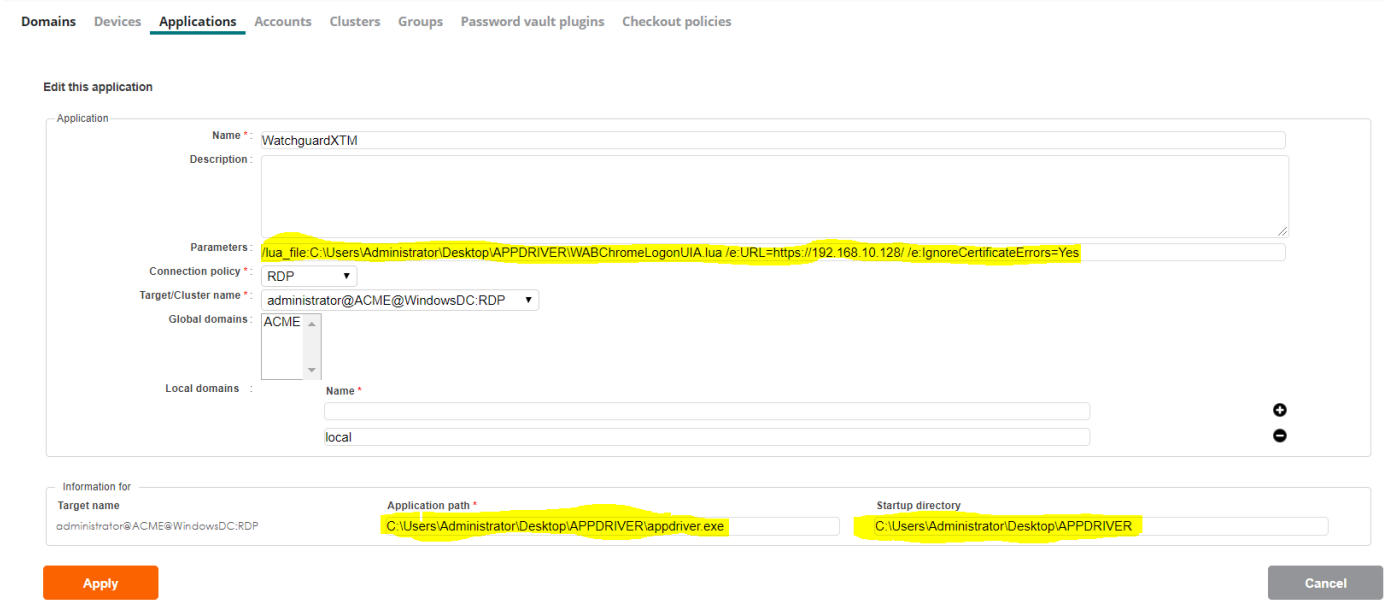


Add the new account to the WatchGuard group



In order to connect to the firewall WALLIX uses an application.
This application is launched using AppDriver (an exe that is installed on a windows system).
RDP is used to connect to the windows system and launch the application.
This creates a secure connection and ensure the integrity of the session, recording and logs.

Create the application

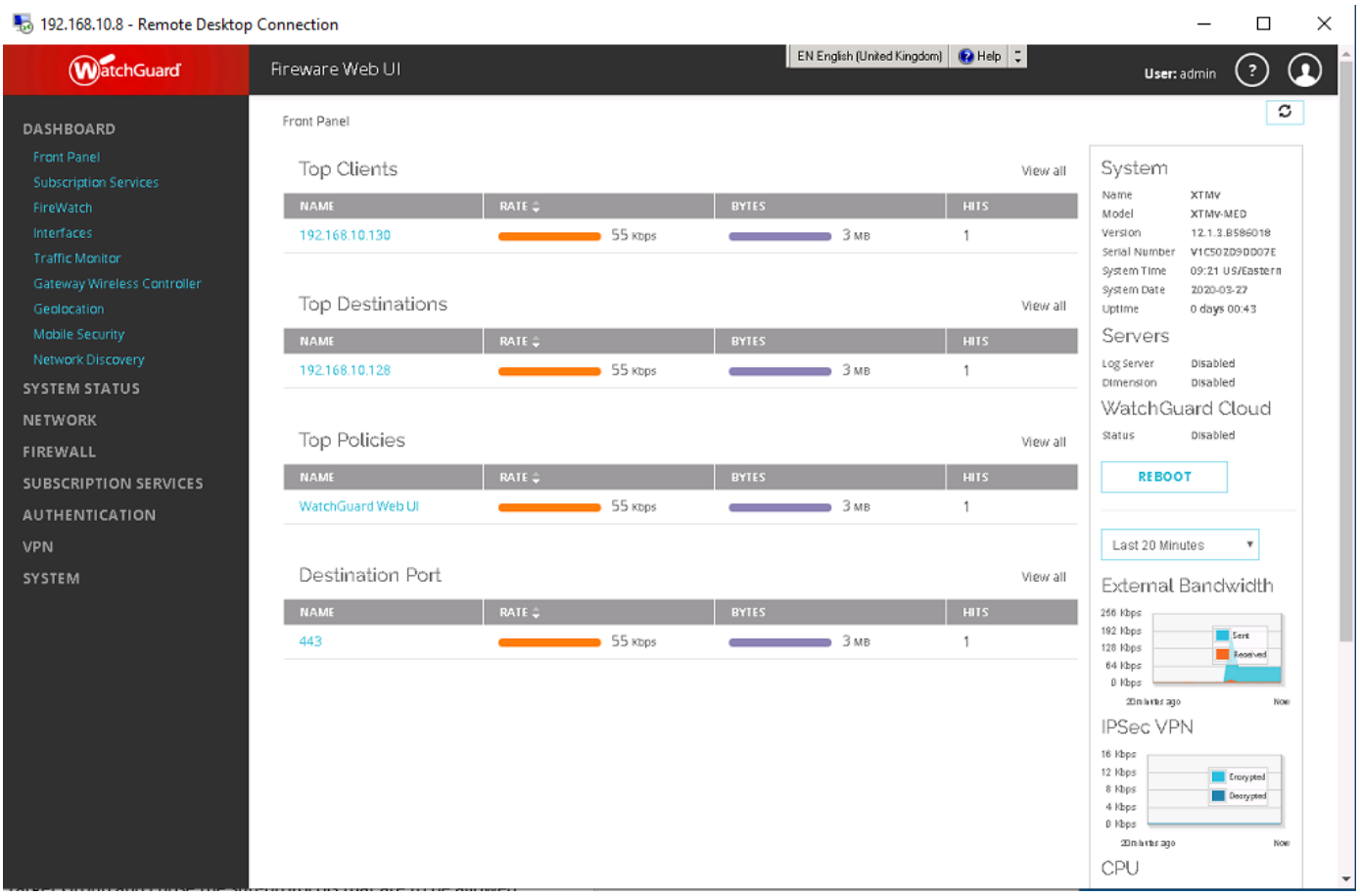


Parameters (sample parameter)
/lua_file:C:\Users\Administrator\Desktop\APPDRIVER\WABChromeLogonUIA.lua /e:URL=https://192.168.10.128/ /e:IgnoreCertificateErrors=Yes

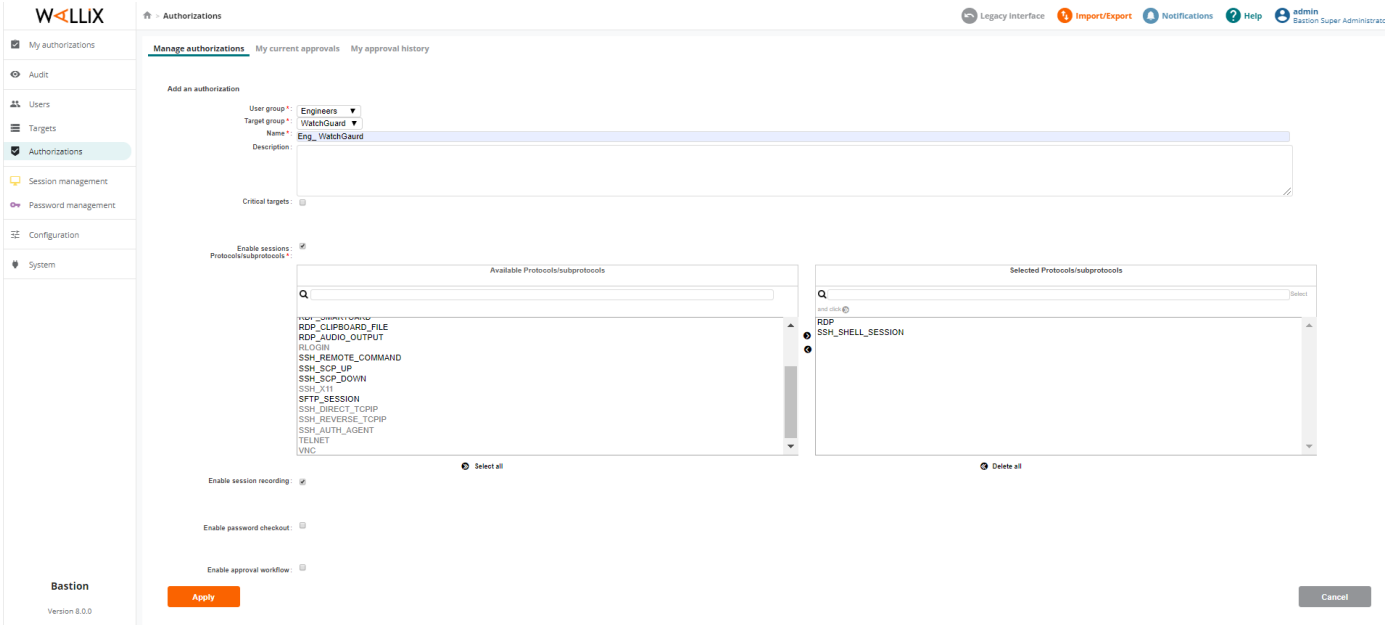
Application path
C:\Users\Administrator\Desktop\APPDRIVER\appdriver.exe

Startup directory
C:\Users\Administrator\Desktop\APPDRIVER

The bastion will launch Chrome and direct it to the URL of the firewall in this case https://192.168.10.128
for ease of configuration I have changed the default WatchGuard https port 8080 to 443

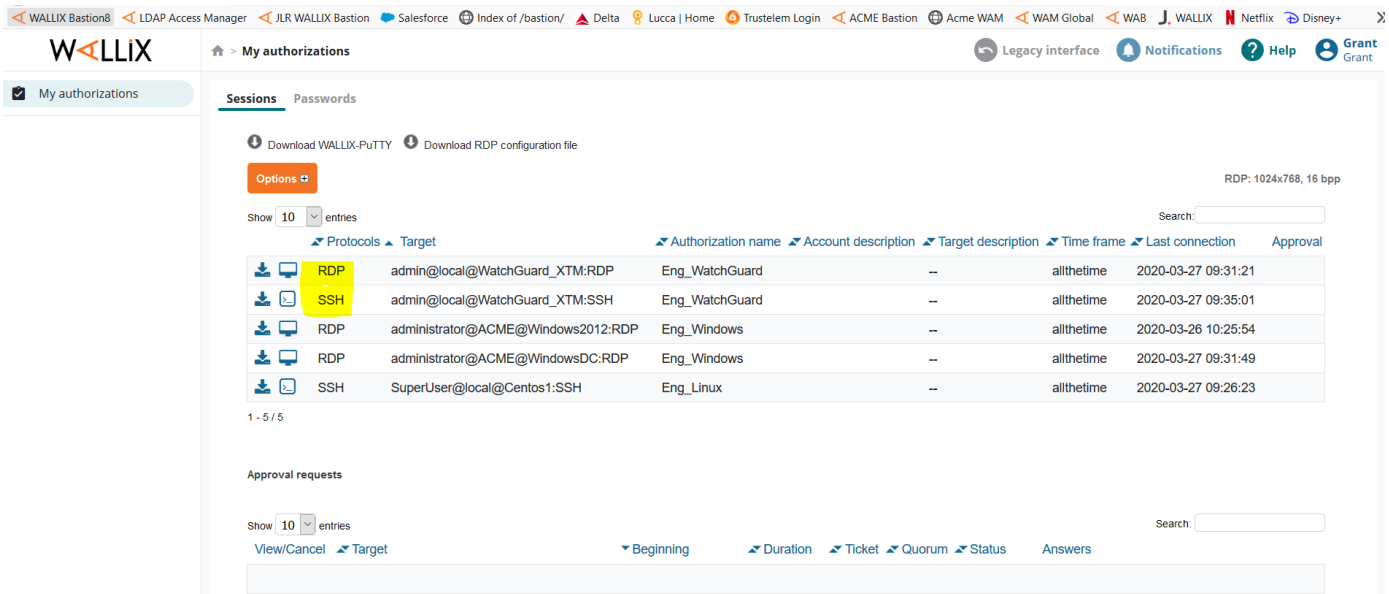


Create an authorisation for the User Group and Target Group and chose the sub-protocols that are to be allowed
Below I have created an authorisation for the Engineers User Group to connect to the WatchGuard Target Group using RDP and SSH Shell

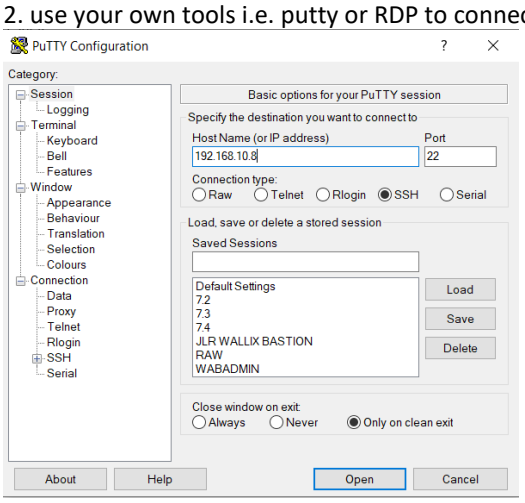


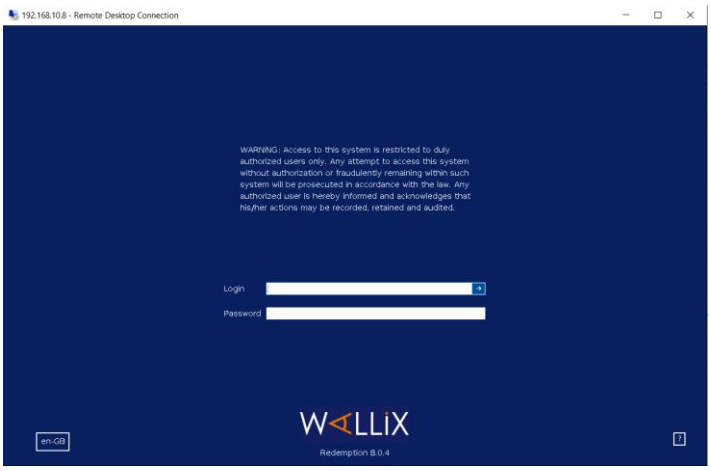
Connecting to the Firebox via the WALLIX Bastion via SSH

1. connect either via the WAB GUI

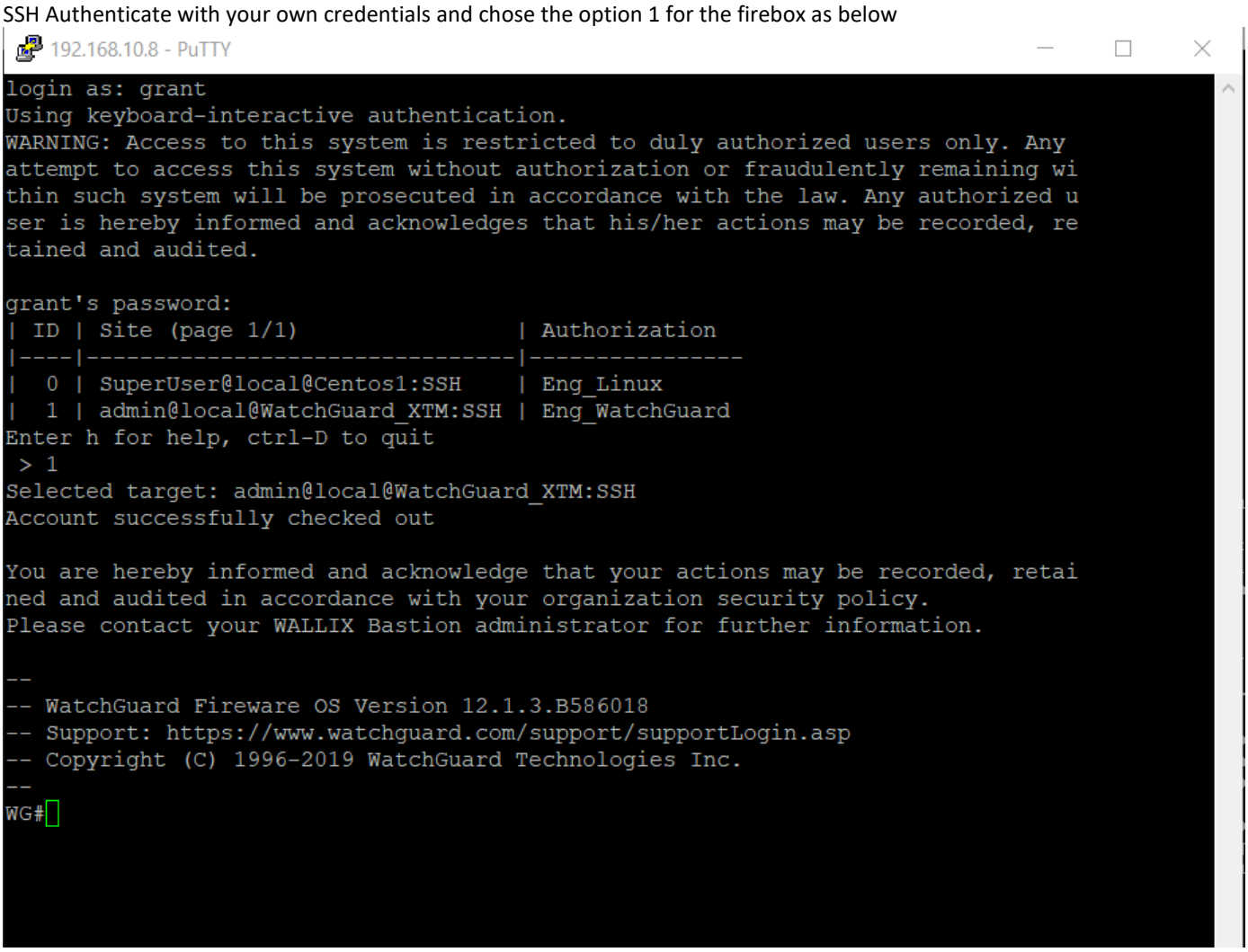


2. use your own tools i.e. putty or RDP to connect to the WAB

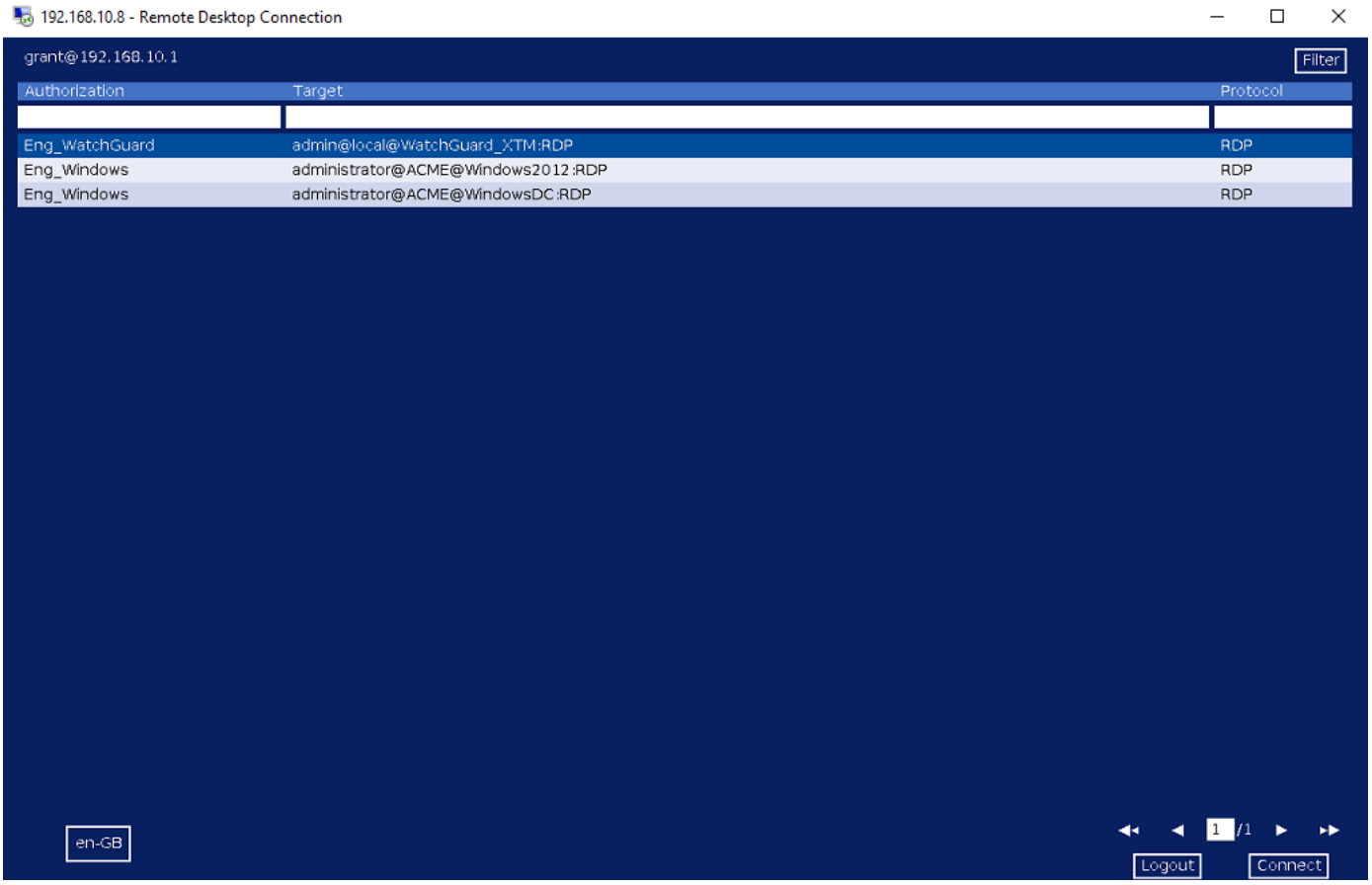




SSH Authenticate with your own credentials and chose the option 1 for the firebox as below



RDP Authenticate with your own credentials and chose the option 1 for the firebox as below



After selecting to connect to the firebox you are presented with a warning / message saying that the session will be recorded etc. The Bastion will then insert the username and password into the session and the user / admin never needs to know it