

# 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

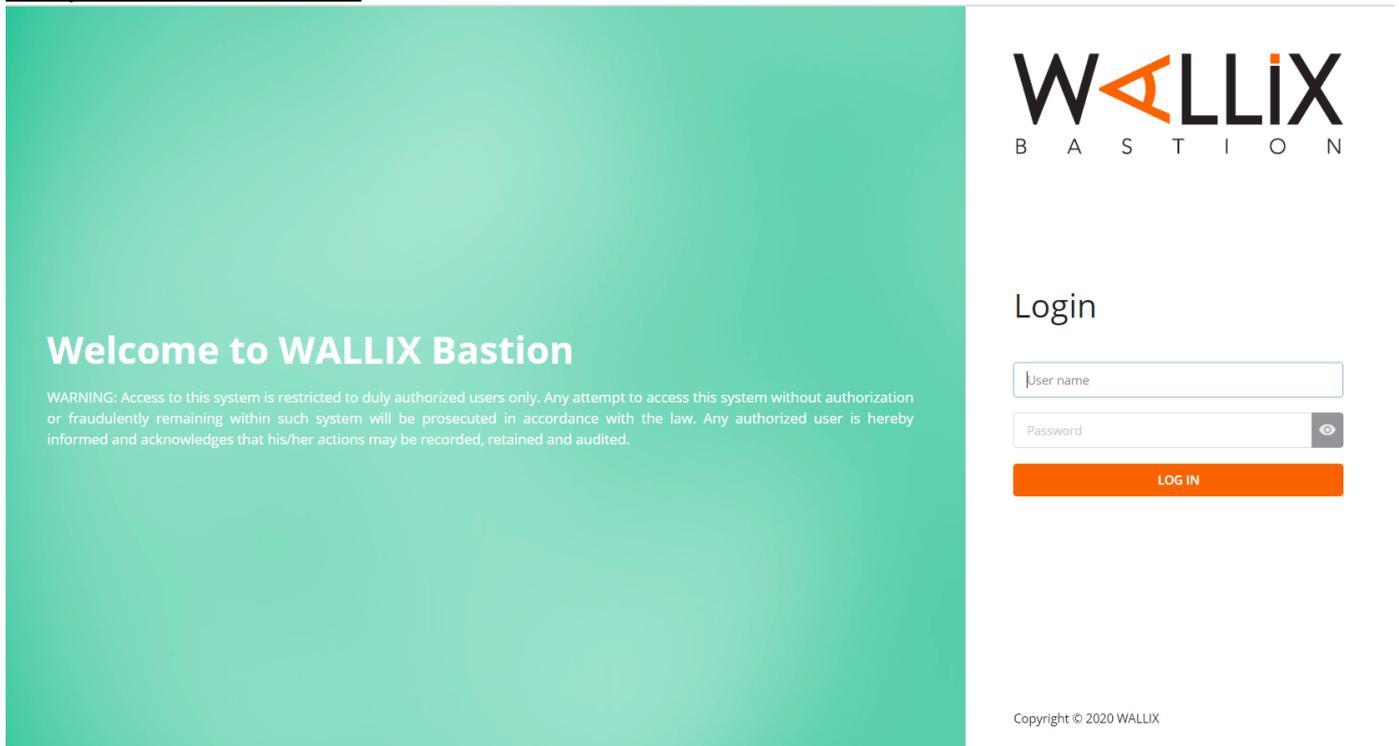
# Integration of WALLIX and WatchGuard

**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 Firewall® 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

## Set up of the WALLIX Bastion



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

The screenshot shows the WLLIX web interface for configuring a target device. The breadcrumb navigation is 'Targets > Devices > WatchGuard\_XTM'. The user is logged in as 'admin' (Bastion Super Administrator). The 'General' tab is active, showing the following configuration:

- Name: WatchGuard\_XTM
- Alias: WGXTM
- IP address or FQDN: 192.168.10.4

A summary table on the right side of the page shows the following counts:

Category	Count
Name	1
IP address or FQDN	1
Services	0
Local domains	0
Local accounts	0
Global accounts	1
Groups	0
Certificates	0

I then create the service

In this case it is SSH using port 4118 (WatchGuard Cli Admin port)

### New service SSH



#### Device

WatchGuard\_XTM

#### Service name \*

SSH

#### Port \*

4118

#### Connection policy \*

SSH

#### Proxy options \*

- SSH SHELL SESSION
- SSH REMOTE COMMAND
- SSH SCP UP
- SSH SCP DOWN
- SSH X11
- SFTP SESSION
- SSH DIRECT TCPIP
- SSH REVERSE TCPIP
- SSH AUTH AGENT

Close

Apply and close

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

**WALLIX** Home > Targets > Accounts > New Legacy

- My authorizations
- Audit
- Users
- Targets**
- Authorizations
- Session management
- Password management
- Configuration
- System

**General** Password SSH private key

**Device \***  
WatchGuard\_XTM

**Local domain \***  
local

**Account name \***  
wallixadmin

**Account login \***  
wallixadmin

**Description**

**Apply**

### A target group is then required

Create a WatchGuard group

**WALLIX** Home > Targets > Groups > WatchGuard

- My authorizations
- Audit
- Users
- Targets**
- Authorizations
- Session management
- Password management
- Configuration
- System

**General** Session management targets Password management targets

**Name \***  
WatchGuard

**Description**

**Apply**

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

The screenshot shows the WALLIX web interface. On the left is a navigation menu with items: My authorizations, Audit, Users, Targets (highlighted), Authorizations, Session management, Password management, Configuration, and System. The main content area shows a breadcrumb path: Targets > Groups > WatchGuard. There are tabs for General, Session management targets (active), Password management targets, and Restrictions. Under Session management targets, there are sub-tabs: Account, Scenario account, Account mapping, and Interactive login. A '+ Target(s)' button is visible. Below it is a 'Filters' section with a table header: Account name, Domain type, Domain name, and Resource type. The table is currently empty, with a message: 'Click on the + button to add an item'. An 'Edit layout' button is at the bottom of the filters section.

**Add target accounts for session management**



**Group**

WatchGuard

**From \***

A device and related local accounts

**Device \***

WatchGuard\_XTM

**Service \***

SSH

**Local accounts \***

1 entry selected

**Filters**

Account name

Domain name

Already in group

wallix

local

1 entry

Close

Add and continue

Add and close

## RDP HTTPS Connections

Add the RDP service to the already created device

**WALLIX** Targets > Devices > WatchGuard\_XTM Legacy interface

My authorizations  
Audit  
Users  
Targets  
Authorizations  
Session management  
Password management  
Configuration  
System

General **Services** Local domains Local accounts Global accounts Groups Certificates

+ Service

Filters

Service name	Protocol	Port
SSH	SSH	4118

Edit layout

### New service RDP

Device: WatchGuard\_XTM

Service name\*: RDP

Port\*: 3389

Connection policy\*: RDP

Proxy options\*  
 RDP CLIPBOARD UP  
 RDP CLIPBOARD DOWN  
 RDP CLIPBOARD FILE  
 RDP PRINTER  
 RDP COM PORT  
 RDP DRIVE  
 RDP SMARTCARD  
 RDP AUDIO OUTPUT

Close Apply and close

Bastion

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

New account

General Password SSH private key

Device: WatchGuard\_XTM

Local domain\*: local

Account name\*: readwrite

Account login\*: readwrite

Checkout policy\*: default

Automatic password change  Deselect option to disable automatic password change for this account

Automatic SSH key change  Deselect option to disable automatic SSH key change for this account

Description

Close Apply and continue Apply and close

Enter the general data and apply. You will then access the next tabs.

## Add the new account to the WatchGuard group

### Add target accounts for session management ✕

**Group**  
WatchGuard

**From \***  
A device and related local accounts

**Device \***  
WatchGuard\_XTM

**Service \***  
SSH

**Local accounts \***  
 1 entry selected

**Filters**

Account name	Domain name	Already in group
<input checked="" type="checkbox"/> readwrite	local	
<input type="checkbox"/> wallix	local	

[Edit layout](#) 2 entries

Close Add and continue Add and close

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

[Domains](#) [Devices](#) [Applications](#) [Accounts](#) [Clusters](#) [Groups](#) [Password vault plugins](#) [Checkout policies](#)

Edit this application

**Application**

Name \*: WatchguardXTM

Description :

Parameters : /lua\_file:C:\Users\Administrator\Desktop\APPDRIVER\WABChromeLogonUIA.lua /e-URL=https://192.168.10.128/ /e-IgnoreCertificateErrors=Yes

Connection policy \*: RDP

Target/Cluster name \*: administrator@ACME@WindowsDC:RDP

Global domains : ACME

Local domains :

Name *
local

**Information for**

Target name : administrator@ACME@WindowsDC:RDP

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

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

Apply Cancel

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

The screenshot displays the WatchGuard Fireware Web UI interface. The left sidebar contains a navigation menu with categories like DASHBOARD, SYSTEM STATUS, NETWORK, FIREWALL, and SUBSCRIPTION SERVICES. The main content area is titled 'Front Panel' and features several traffic analysis sections:

- Top Clients:** A table showing traffic from 192.168.10.130 at a rate of 55 kbps, with 3 MB of bytes and 1 hit.
- Top Destinations:** A table showing traffic to 192.168.10.128 at a rate of 55 kbps, with 3 MB of bytes and 1 hit.
- Top Policies:** A table showing traffic for the 'WatchGuard Web UI' policy at a rate of 55 kbps, with 3 MB of bytes and 1 hit.
- Destination Port:** A table showing traffic on port 443 at a rate of 55 kbps, with 3 MB of bytes and 1 hit.

On the right side, there is a 'System' information panel with details such as Name (XTMV), Model (XTMV-MED), Version (12.1.3.B586018), and System Time (09:21 US/Eastern). Below this is a 'WatchGuard Cloud' status section and a 'REBOOT' button. At the bottom right, there are graphs for 'External Bandwidth' and 'IPSec VPN' showing traffic trends over time.

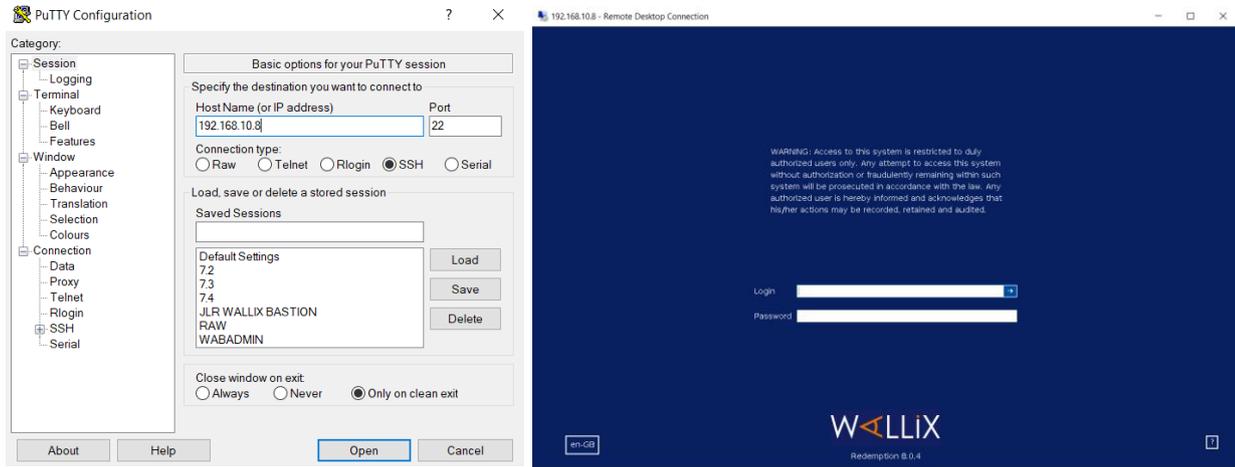
Create an authorisation for the User Group and Target Group and chose the sub-protocols that are to be allowed  
 Below I have created an authorisation for the Engineers User Group to connect to the WatchGuard Target Group using RDP and SSH Shell

## Connecting to the Firebox via the WALLIX Bastion via SSH

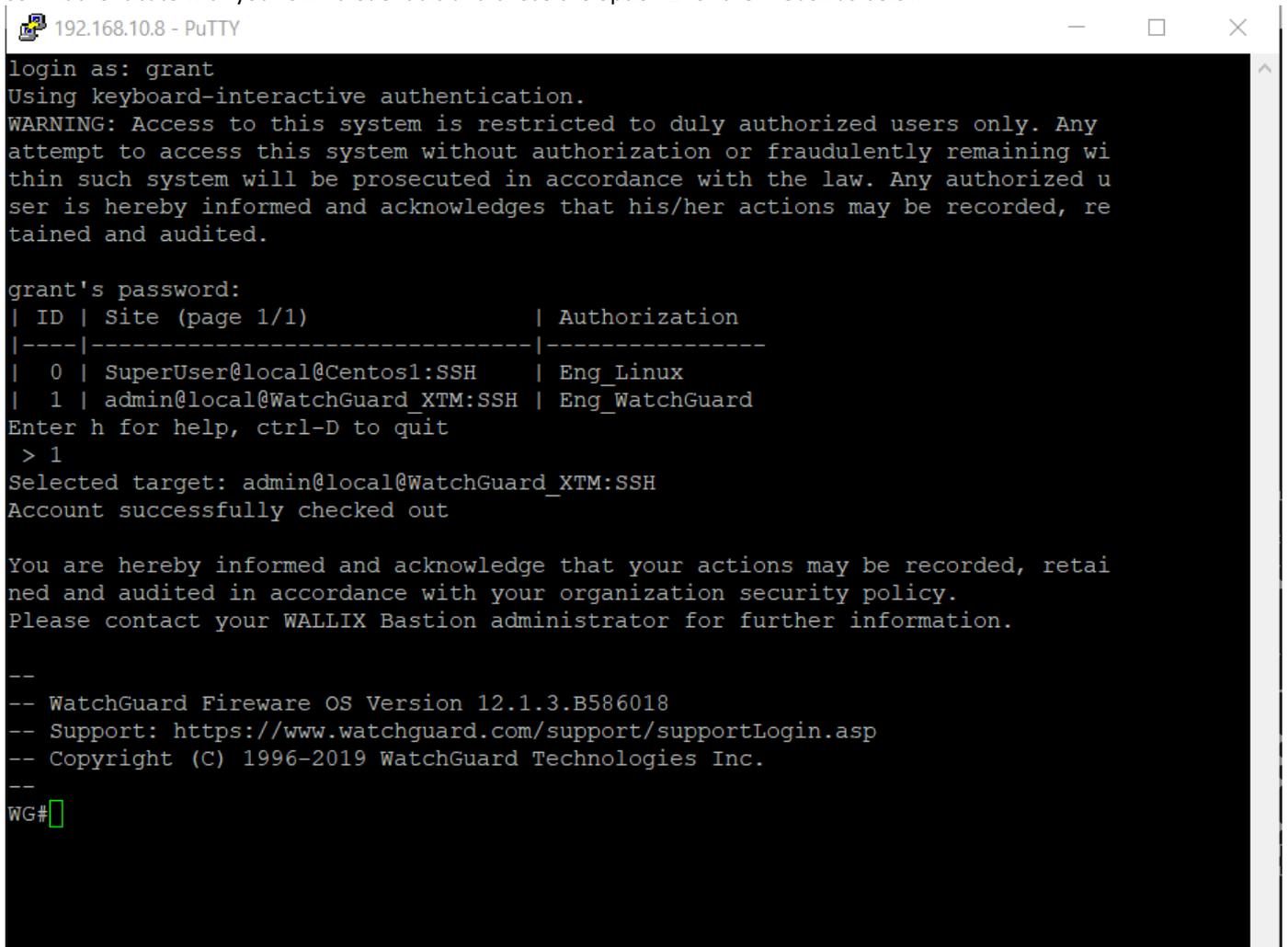
1. connect either via the WAB GUI

Protocols	Target	Authorization name	Account description	Target description	Time frame	Last connection	Approval
RDP	admin@local@WatchGuard_XTM:RDP	Eng_WatchGuard	--	--	allthetime	2020-03-27 09:31:21	
SSH	admin@local@WatchGuard_XTM:SSH	Eng_WatchGuard	--	--	allthetime	2020-03-27 09:35:01	
RDP	administrator@ACME@Windows2012:RDP	Eng_Windows	--	--	allthetime	2020-03-26 10:25:54	
RDP	administrator@ACME@WindowsDC:RDP	Eng_Windows	--	--	allthetime	2020-03-27 09:31:49	
SSH	SuperUser@local@Centos1:SSH	Eng_Linux	--	--	allthetime	2020-03-27 09:26:23	

## 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

192.168.10.8 - Remote Desktop Connection

grant@192.168.10.1

Authorization	Target	Protocol
Eng_WatchGuard	admin@local@WatchGuard_XTM:RDP	RDP
Eng_Windows	administrator@ACME@Windows2012:RDP	RDP
Eng_Windows	administrator@ACME@WindowsDC:RDP	RDP

en-GB

1 / 1

Logout Connect

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

