

# 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

## Set up of the WALLIX Bastion

### Welcome to WALLIX Bastion

WARNING: Access to this system is restricted to duly authorized users only. Any attempt to access this system without authorization or fraudulently remaining within such system will be prosecuted in accordance with the law. Any authorized user is hereby informed and acknowledges that his/her actions may be recorded, retained and audited.

WALLIX

BASTION

Login

User name

Password

LOG IN

Copyright © 2020 WALLIX

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

WALLIX

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Bastion

Version 8.0.0

Targets > Devices > WatchGuard\_XTM

Legacy interfaceImport/ExportNotificationsHelpadminBastion Super Administrator

GeneralServicesLocal domainsLocal accountsGlobal accountsGroupsCertificates

Name\*

WatchGuard\_XTM

Alias

WGXTM

IP address or FQDN\*

192.168.10.4

Description

Apply

Hide summary >

General

Name: WatchGuard\_XTM

IP address or FQDN: 192.168.10.4

Services0

Local domains0

Local accounts0

Global accounts1

Groups0

Certificates0

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

New service SSH

X

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

3

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

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Targets > Accounts > New

Legacy

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

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Targets > Groups > WatchGuard

General

Session management targets

Password management targets

R

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

WALLIX

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Targets > Groups > WatchGuard

Legacy interface

General

Session management targets

Password management targets

Restrictions

Account

Scenario account

Account mapping

Interactive login

Target(s)

Filters

Account name

Domain type

Domain name

Resource type

Click on the + button to add an item

Edit layout

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

Edit layout

1 entry

Close

Add and continue

Add and close

RDP HTTPS Connections

Add the RDP service to the already created device

WALLIX

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Bastion

Targets > Devices > WatchGuard\_XTM

Legacy interface

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

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

New account

General Password SSH private key

Device

WatchGuard\_XTM

Checkout policy

default

Local domain

local

Account name

readwrite

Account login

readwrite

Automatic password change

Automatic SSH key change

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

☒ readwrite

local

☐ 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

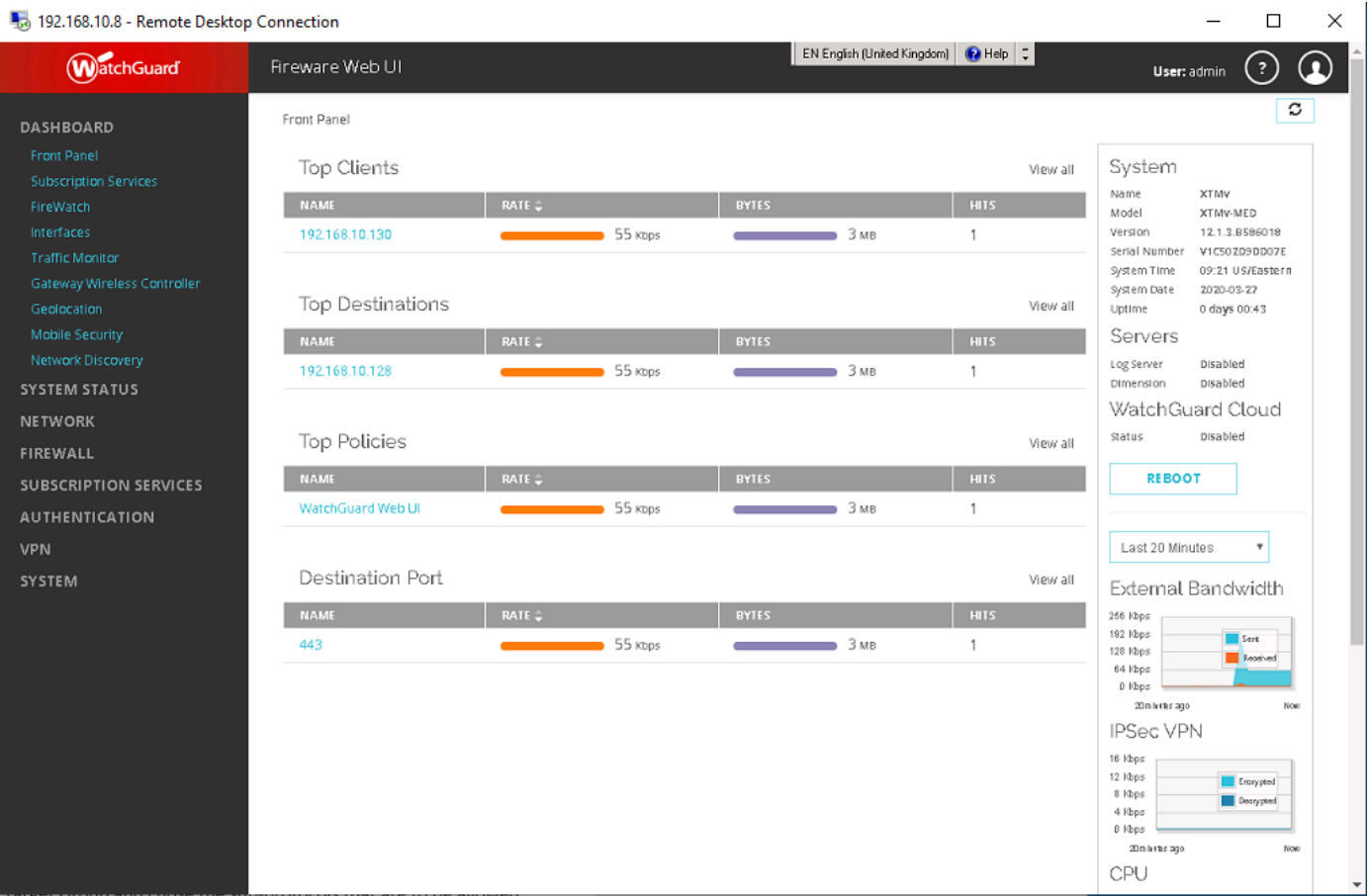
Cancel

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





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

WALLIX

My authorizations

My current approvals

My approval history

My authorizations

Audit

Users

Targets

Authorizations

Session management

Password management

Configuration

System

Legacy interface

Import/Export

Notifications

Help

admin

Bastion Super Administrator

Add an authorization

User group: Engineers

Target group: WatchGuard

Name: Eng\_WatchGuard

Description:

Critical targets:

Enable sessions: ☒

Protocols/subprotocols:

Available Protocols/subprotocols

Selected Protocols/subprotocols

Enable session recording: ☒

Enable password checkout: ☐

Enable approval workflow: ☐

Apply

Cancel

Connecting to the Firebox via the WALLIX Bastion via SSH

1. connect either via the WAB GUI

WALLIX Bastion8

LDAP Access Manager

ILR WALLIX Bastion

Salesforce

Index of /bastion/

Delta

Lucca | Home

Trustelem Login

ACME Bastion

Acme WAM

WAM Global

WAB

WALLIX

Netfix

Disney+

Legacy interface

Notifications

Help

Grant

Grant

My authorizations

Sessions

Passwords

Download WALLIX-PuTTY

Download RDP configuration file

Options

RDP: 1024x768, 16 bpp

Show 10 entries

Search:

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

1 - 5 / 5

Approval requests

Show 10 entries

Search:

View/Cancel

Target

Beginning

Duration

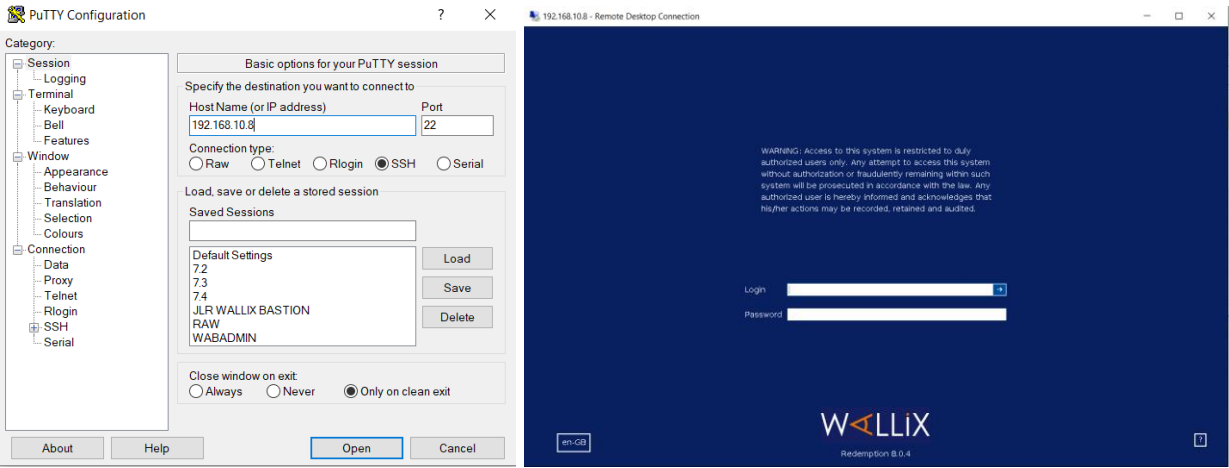
Ticket

Quorum

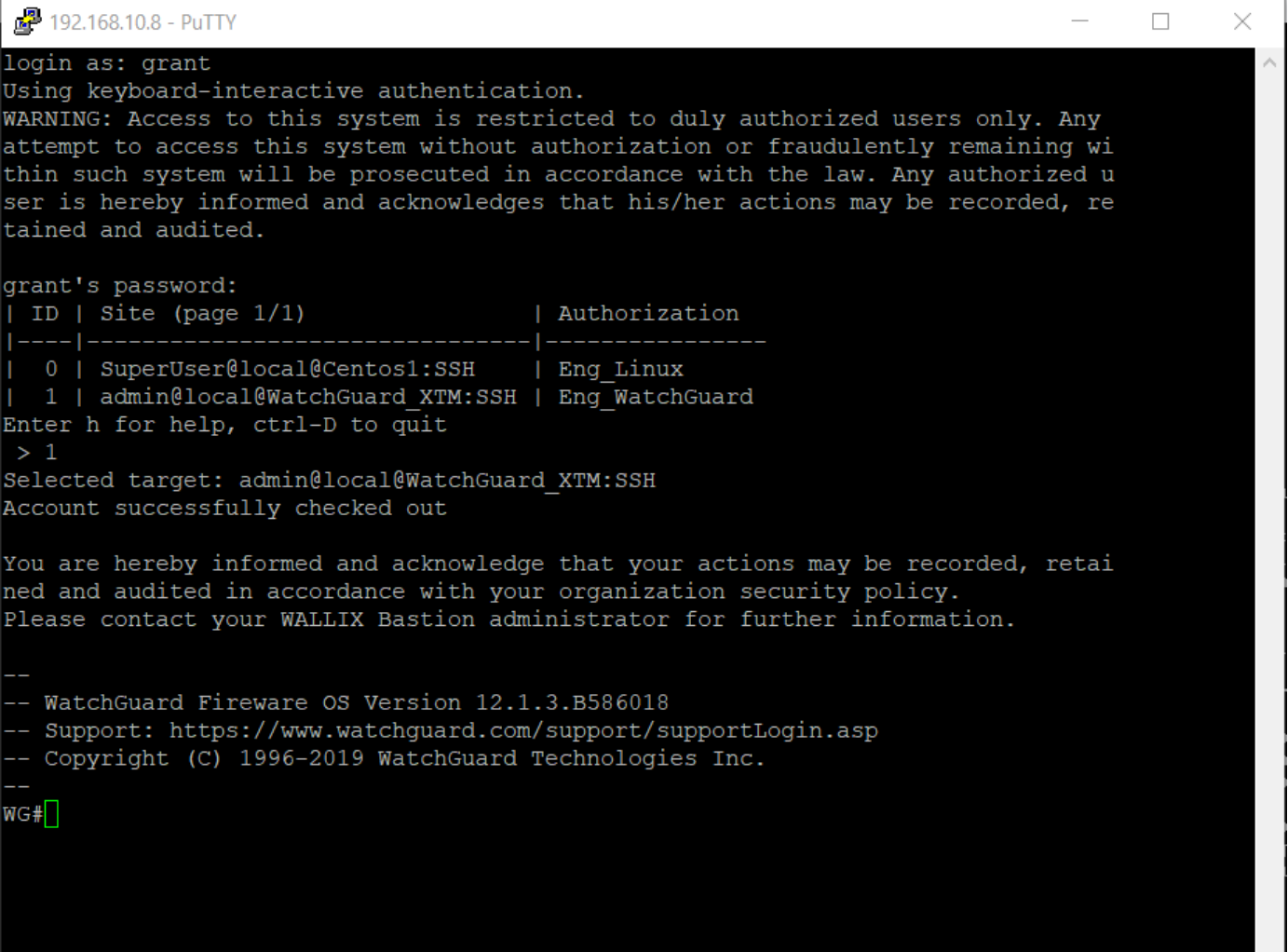
Status

Answers

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

192.168.10.8 - Remote Desktop Connection

Information

You are hereby informed and acknowledge that your actions may be recorded, retained and audited in accordance with your organization security policy.  
Please contact your WALLIX Bastion administrator for further information.

OK

Refused

WALLIX

192.168.10.8 - Remote Desktop Connection

EN English (United Kingdom)

Help

User: admin

DASHBOARD

Front Panel

Subscription Services

FireWatch

Interfaces

Traffic Monitor

Gateway Wireless Controller

Geolocation

Mobile Security

Network Discovery

SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

Front Panel

Top Clients

NAME	RATE	BYTES	HITS
192.168.10.130	55 kbps	3 MB	1

Top Destinations

NAME	RATE	BYTES	HITS
192.168.10.128	55 kbps	3 MB	1

Top Policies

NAME	RATE	BYTES	HITS
WatchGuard Web UI	55 kbps	3 MB	1

Destination Port

NAME	RATE	BYTES	HITS
443	55 kbps	3 MB	1

System

NameXTMV

ModelXTMV-MED

Version12.1.3.B586018

Serial NumberV1C502D9DD07E

System Time09:21 US/Eastern

System Date2020-03-27

Uptime0 days 00:43

Servers

Log ServerDisabled

DimensionDisabled

WatchGuard Cloud

StatusDisabled

REBOOT

Last 20 Minutes

External Bandwidth

IPSec VPN

CPU

12