



# Best Practices – WatchGuard Accessportal - Grundlagen und Konfiguration

Thomas Fleischmann

Senior Sales Engineer, Central Europe  
[Thomas.Fleischmann@watchguard.com](mailto:Thomas.Fleischmann@watchguard.com)

# Agenda

- Voraussetzung
  
- Was ist das WatchGuard Access Portal ?
  
- Einrichtung
  - Applikationsgruppen & Applikationen / Web Seiten
  - Zugriffsrechte
  
- Anpassung des Access Portals
  
- Weitere Informationen



# Voraussetzung

## Voraussetzung

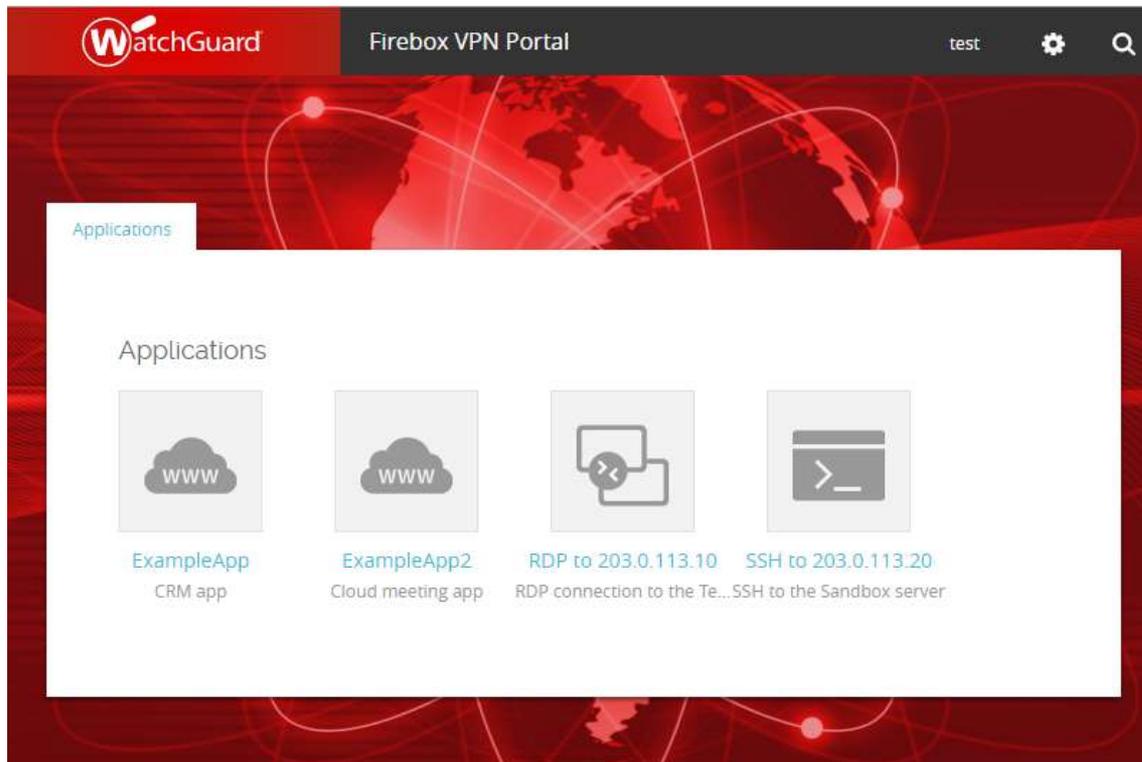
- Das Access Portal ist seit der Version 12.1 in der WatchGuard FireOS enthalten.
- Die Lizenz für das Access Portal ist Bestandteil der Total Security Suite (TSS) von WatchGuard.
- Das Access Portal funktioniert **nicht** auf folgende Produkten: XTM, XTMv, T Series, M200 oder M300.
- Das Access Portal unterstützt FireboxV, FireboxCloud, und alle anderen Firebox Modelle (M370 oder höher).



# Was ist das WatchGuard Access Portal ?

# Access Portal

- Die neue Access Portal-Funktion ermöglicht es Benutzern eine externen Webanwendungen von Drittanbietern zu verwenden, und zum anderen, RDP- und SSH-Sitzungen im Browser zu lokalen Ressourcen ohne einen SSL-Client zu starten.



# Access Portal

- Der sichere Remote-Zugriff auf (virtuelle) Maschinen über RDP bietet privilegierten Benutzern die Möglichkeit, Netzwerke remote zu verwalten
- Eine SSH-Sitzungen in HTML5- und SSL-kompatiblen Webbrowsern ermöglichen es privilegierten Benutzern, mit Hilfe einer sicheren Shell, kritische Netzwerkressourcen zu verwalten.
- Die Sicherheit von TLS 1.2 erhöht somit auf die Sicherheit für RDP- und SSH-Sitzungen !!



# Access Portal

- Die HTTPS Verbindung zu den Applikationen wird von der Firebox hergestellt.
- Benutzer melden sich am Access Portal an und sehen im Portal links zu Web Applikationen, RDP Host und SSH Host.
  - Sie können die Applikation & -Gruppen angeben, mit denen Benutzer und Benutzergruppen eine Verbindung herstellen können.
- Single Sign-On über einen Identitätsanbieter eines Drittanbieters (z. B. **Okta, OneLogin, etc.**) wird über das SAML-Authentifizierungsprotokoll unterstützt.

(In der Zukunft auch durch ein eigenes WatchGuard Produkt – WatchGuard AuthPoint)



# Access Portal — Geteilte Einstellungen

- Access Portal und Mobile VPN mit SSL teilen diese VPN-Portaleinstellungen:
  - Interfaces, auf denen das VPN-Portal verfügbar ist
  - Authentifizierungsserver
  - Portal Design Anpassung

When you activate Mobile VPN with SSL, the "SSLVPN-Users" group

Activate Mobile VPN with SSL

General Authentication Advanced

## Authentication Server Settings

Auto reconnect after a connection is lost

Force users to authenticate after a connection is lost

Allow the Mobile VPN with SSL client to remember password

Define users and groups to authenticate with Mobile VPN with SSL.

<input type="checkbox"/>	NAME
<input type="checkbox"/>	SSLVPN-Users
<input type="checkbox"/>	windows
<input type="checkbox"/>	fmann
<input type="checkbox"/>	Michael
<input type="checkbox"/>	fmann21
<input type="checkbox"/>	groupName

ADD

REMOVE

## VPN Portal

### Interface for connections:

Any-External

### Authentication Servers:

RADIUS

Firebox-DB

 CONFIGURE

# Access Portal — Geteilte Einstellungen

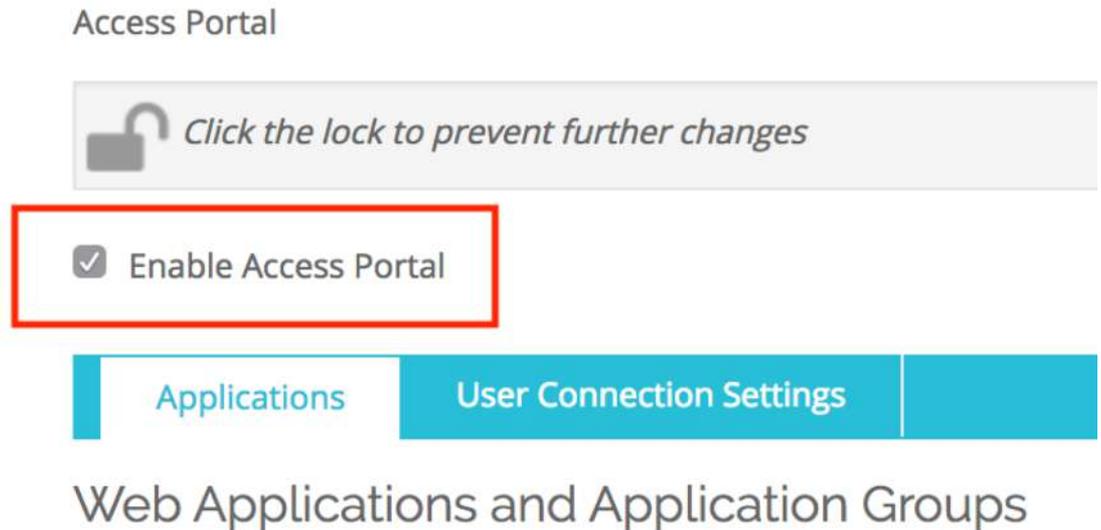
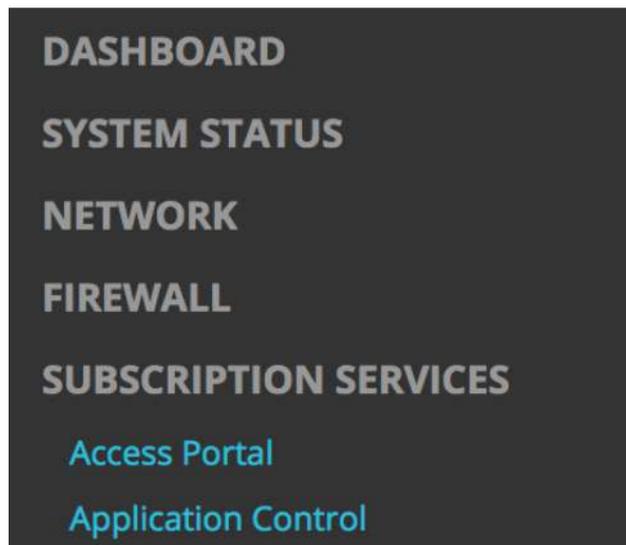
- Access Portal und Mobile VPN mit SSL teilen sich die Firewall-Policy WatchGuard SSLVPN.
- Any-External ist das einzige verfügbare Interface für das Access Portal, wenn Mobile VPN mit SSL **nicht** auf der Firebox konfiguriert wurde.
- Any-External, Any-Trusted und Any-Optional sind verfügbar, wenn das Access Portal aktiviert ist und Mobile VPN mit SSL aktiviert ist (**oder** in der Vergangenheit war).



A horizontal banner with a red background. In the center is a white silhouette of a globe. Overlaid on the globe are several white lines representing a network or data flow, with some lines ending in small white circles. The overall aesthetic is technical and global.

# Einrichtung

- Aktivieren des Access Portals
  - Die Konfiguration des Access Portals erfolgt in den Bereich der *Subscription Services*.



# VPN Portal

## Interface for Connections:

Any-External

## Authentication Servers:

RADIUS

Firebox-DB



# Authentication Servers

Specify the authentication servers to use for connections

**AUTHENTICATION SERVER**

RADIUS ↓

---

Firebox-DB

---

Firebox-DB

# Interfaces

Specify the interfaces for connections to the VPN Portal

**INTERFACE**

Any-External

---

Any-External

egt

# Web Applications and Application Groups

Specify the applications that appear in the VPN Portal. Application

## NAME

▼ Applications



Windows 10

▼ Webseite



WatchGuard

ADD ▼

EDIT

REMOVE

Web Application

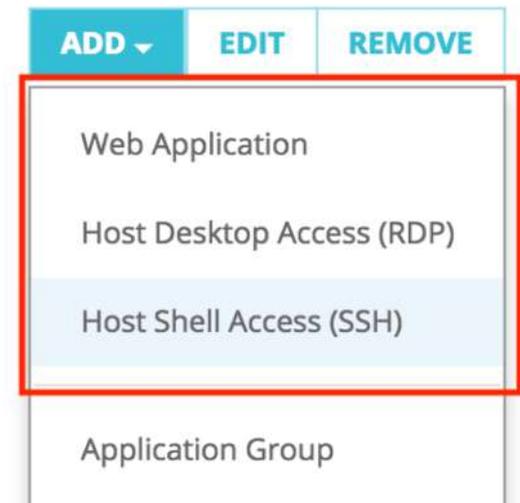
Host Desktop Access (RDP)

Host Shell Access (SSH)

Application Group

- Applikation Gruppen anlegen
  - Im ersten Step wird eine oder mehrere Applikation Gruppen angelegt.

- Erst danach kann man Applikationen für die einzelnen Applikationsgruppen definieren.
- Es macht Sinn, die Applikationen nach Typen oder nach Aufgaben zu sortieren.
  - D.h. Alle RDP Session in einer Applikation Gruppe zu legen **oder**
  - Dem Benutzer eine eindeutige Applikation Gruppe zu ordnen, worin er alle seine Applikationen findet.



## ■ Einige Anmerkungen zu RDP Session

- Das Access Portal unterstützt die Sicherheitstypen Any, NLA, TLS und RDP für Verbindungen mit RDP-Hosts. Wir empfehlen die Standardeinstellung Any, die für die meisten Verbindungen funktioniert. Wenn Any ausgewählt ist, verhandelt die Firebox das Sicherheitsprotokoll mit dem Remote-Host.
- Wir empfehlen, in den RDP-Einstellungen für Access Portal **Trust Certificate** auszuwählen.
- Wenn Sie kein **Trust Certificate** auswählen, müssen Sie die Zertifizierungsstellenkette für den RDP-Host in die Firebox importieren.
- Bei Domänen Rechnern prüfen sie in den Domain Settings, ob **Allows connections only from computers running Remote Desktop with Network Level Authentication** aktiviert ist.

Unter [https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/services/access%20portal/access\\_portal\\_config.html](https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/services/access%20portal/access_portal_config.html) finden sie dazu weitere Hinweise.

- Spezielle Applikation Gruppen für Benutzer und Gruppen werden im Bereich *User Connection Settings* eingerichtet.

Access Portal / Add User or Group

 Click the lock to prevent further changes

Select a user or group.

Authentication Server:

Type:

Name:

Select the resources that are available to this user or group.

NAME	TYPE
<input type="checkbox"/> Applications	Application Group
<input type="checkbox"/>  Windows 10	Host Desktop Access (RDP)
<input type="checkbox"/> Webseite	Application Group
<input type="checkbox"/>  WatchGuard	Web Application

OK

CANCEL



# Anpassung des Access Portals

- Sie können diese Elemente der Login- und Portalseiten anpassen:
  - Seitentitel
  - Login Logo
  - Kopfzeilenlogo
  - Hintergrundbild
- Sie können auch eine benutzerdefinierte CSS-Datei hochladen, um Seitenelemente wie Schaltflächen anzupassen

The screenshot displays the 'SAML' configuration tab within a management interface. It features a navigation bar with 'General', 'Customization', and 'SAML' tabs. The 'Page Title' is set to 'Example Company Access Portal'. Under the 'Customization' section, there are four main options:

- Custom login logo:** This option is checked. It shows a preview of a blue logo with the text 'Example Company'. Below the preview, there is a 'Choose File' button with 'logo.jpg' selected, and 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom header logo:** This option is unchecked. It shows a circular placeholder with 'NO IMAGE AVAILABLE'. Below it, there is a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom background image:** This option is unchecked. It shows a circular placeholder with 'NO IMAGE AVAILABLE'. Below it, there is a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom CSS file:** This option is unchecked. It shows a 'Choose File' button with 'No file chosen' selected, and 'UPLOAD' and 'RESET CSS' buttons.

At the bottom of the configuration area, there are two buttons: 'PREVIEW LOGIN PAGE' and 'PREVIEW APPLICATION PAGE'.



# Weitere Informationen

# Access Portal — Authenticated Users

- Sie können die Benutzer sehen, die mit dem Access Portal verbunden sind:
  - Auf der Firewall-Webbenutzeroberfläche auf der Seite Systemstatus> Authentifizierungsliste

Authentication List 30 SECONDS ▾ ⏸

Authentication List

Summary

Mobile VPN with L2TP: 0	Mobile VPN with SSL: 0	Mobile VPN with IPSec: 0
Mobile VPN with IKEv2: 0	<b>Access Portal: 0</b>	Firewall: 0

Total Users: 0

Users Locked Out: 0 UNLOCK USERS

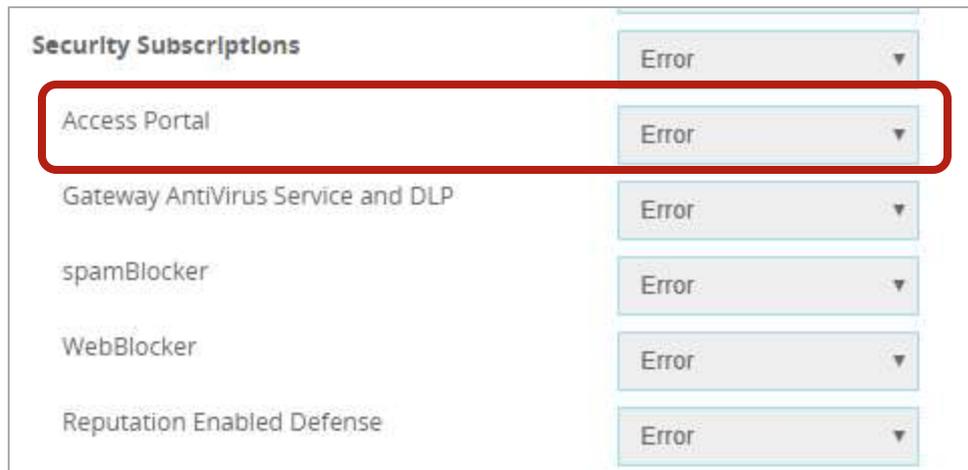
Authenticated Users

LOG OFF USERS

USER	TYPE	DOMAIN	CLIENT	ELAPSED TIME	IP ADDRESS	LOGIN LIMIT
------	------	--------	--------	--------------	------------	-------------

# Access Portal — Diagnostic Log Level

- Sie können auch die Diagnoseprotokollierungsstufe für Access Portal-Verbindungen festlegen
  - Gehen sie unter System > Diagnostic Log
  - Legen Sie im Abschnitt **Security Subscriptions** die Protokollstufe für die Option Zugriffsportal fest



A stylized globe is centered in the image, rendered in a dark red color. Overlaid on the globe is a complex network of white lines and nodes, resembling a global communication or data network. The nodes are small white circles, and the lines are thin white arcs that crisscross the globe. The background is a solid, vibrant red color. A horizontal, semi-transparent red band runs across the middle of the image, serving as a backdrop for the text.

**Live Demo**



**Danke !**