



WatchGuard Accessportal - Grundlagen und Konfiguration

Thomas Fleischmann

Senior Sales Engineer, Central Europe
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

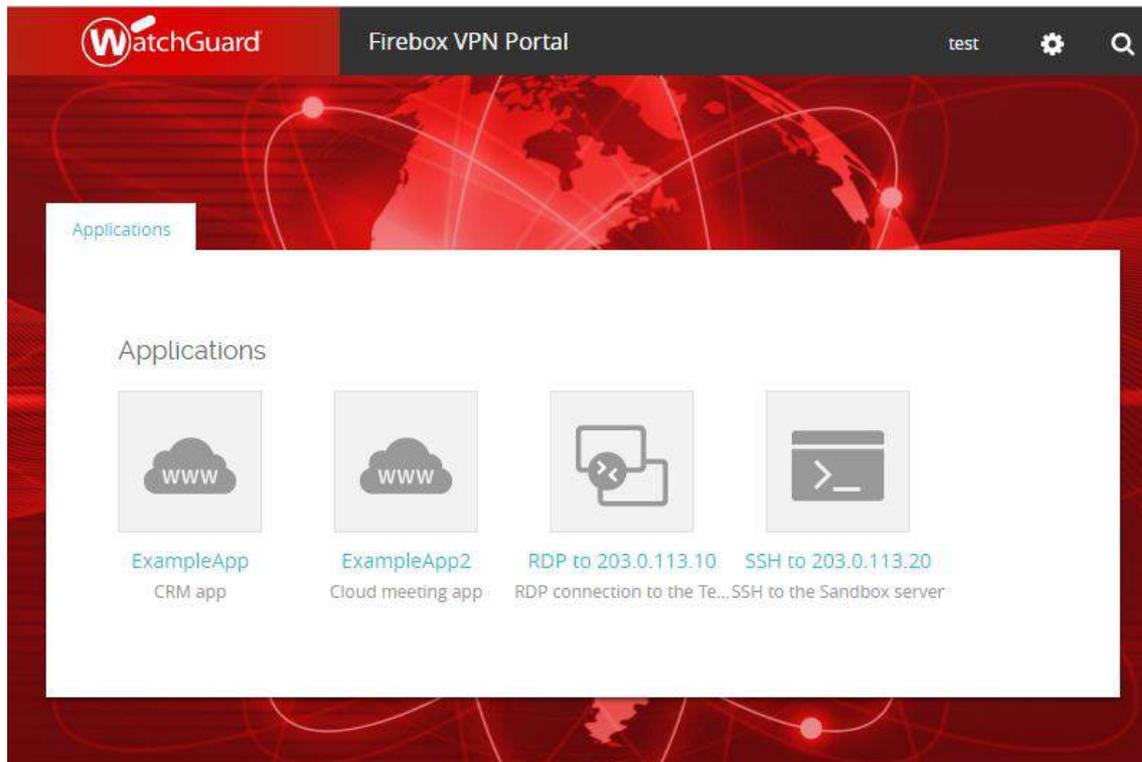
- Das Access Portal ist seit der Version 12.1 in der WatchGuard FireOS enthalten.
- Die Lizenz für das Access Portal ist Bestandteil der Total Security Suite (TSS) von WatchGuard.
- Das Access Portal funktioniert **nicht** auf folgenden Produkten: XTM, XTMv, T Series, M200 oder M300.
- Das Access Portal unterstützt FireboxV, FireboxCloud, und alle anderen Firebox Modelle (M270 oder höher).



Was ist das WatchGuard Access Portal ?

Access Portal

- Die neue Access Portal-Funktion ermöglicht es Benutzern eine externen und interne 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 wird mit Hilfe des SAML-Authentifizierungsprotokoll unterstützt.



Access Portal

Mobile VPN / Mobile VPN with SSL / Configure



Click the lock to prevent further changes

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

Activate Mobile VPN with SSL

General

Authentication

Advanced

Firebox IP Addresses or Domain Names

Type a firebox IP or domain name for SSL VPN users to connect to.

Primary

hetznerfirebox03.cybersec.w

Backup

hetznerfirebox01.cybersec.w

Networking and IP address pool

Konfigurieren Sie die VPN-Portal-Einstellungen

- Die VPN-Portal-Einstellungen geben Authentifizierungsserver, Schnittstellen, Port-Einstellungen und Zeitgeber für das Access-Portal und Mobile VPN mit SSL an.

Access Portal

Wenn Sie einen anderen VPN-Portal-Port als 443 angeben, müssen Benutzer die Portnummer für die Verbindung zum Access-Portal oder mobilen VPN mit SSL angeben.

Wenn Sie z. B. den VPN-Portal-Port 444 angeben und die Firebox-IP-Adresse 203.0.113.2 ist:

- Um sich mit dem Access-Portal zu verbinden, müssen Benutzer eine Verbindung mit `https://203.0.113.2:444` herstellen.
- Um ein Mobile VPN mit SSL-Verbindung zu starten, müssen die Benutzer Port 444 manuell in das Dialogfenster Mobile VPN mit SSL-Verbindung eingeben. Benutzer müssen z. B. `203.0.113.2:444` eingeben.
- Um Mobile VPN mit SSL-Client-Software herunterzuladen, müssen die Benutzer eine Verbindung mit `https://203.0.113.2:444/sslvpn` herstellen.

Access Portal

Port Precedence

- Mehrere Firebox-Funktionen verwenden SSL/TLS für sichere Kommunikation und teilen sich denselben OpenVPN-Server.
- Die Funktionen, die sich den OpenVPN-Server teilen, sind in der Reihenfolge ihrer Priorität von der höchsten bis zur niedrigsten:
 - Managed Tunnel über SSL auf Hub-Geräten
 - BOVPN über TLS im Server-Modus
 - Mobiles VPN mit SSL
 - Access Portal
- Funktionen mit niedrigerer Priorität erben einige SSL/TLS-Einstellungen von aktivierten Funktionen mit höherer Priorität.
- Die gemeinsamen Einstellungen sind für die Funktionen mit niedrigerer Priorität nicht konfigurierbar.

Info: https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/services/access%20portal/ssl_tls_settings_precedence.html

Reverse Proxy for the Access Portal

- In Fireware v12.5 oder höher können Sie Reverse-Proxy-Actions in der Access-Portal-Konfiguration konfigurieren.
- Mit Reverse-Proxies können Remote-Benutzer ohne VPN-Client eine sichere Verbindung zu internen Webanwendungen und Microsoft Exchange-Diensten herstellen.
- Der Reverse-Proxy leitet HTTP-Verkehr von externen Netzwerken an Exchange-Server oder andere Webanwendungen in internen Netzwerken, die sich hinter einer Firebox befinden, weiter.

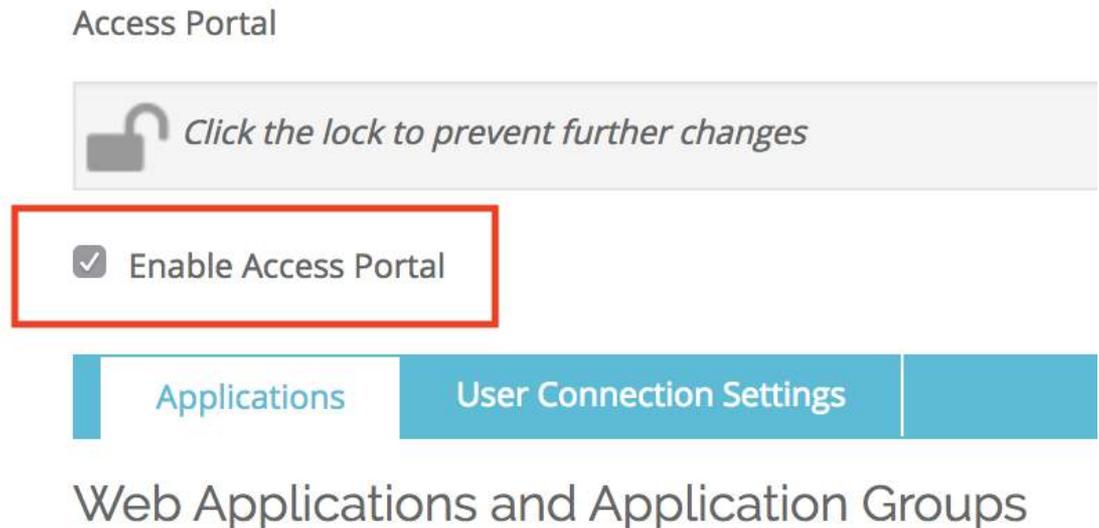
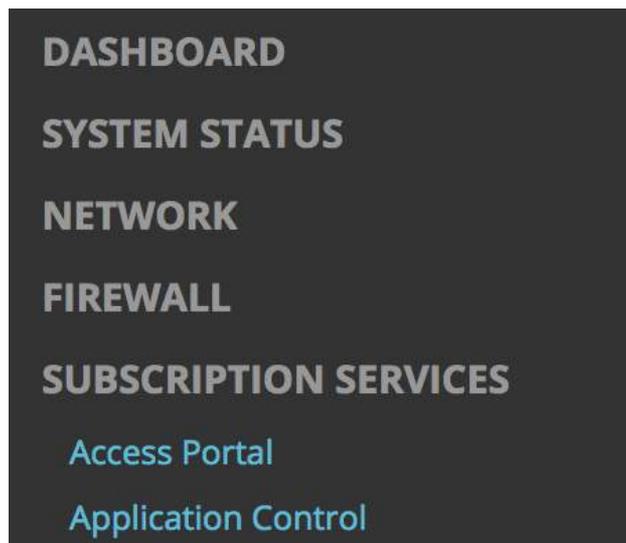
Zu diesem Thema wird ein eigenes Best Practice Webinar erfolgen am 24.04.2020 um 9:00 Uhr. Anmelden können sie sich unter

https://secure.watchguard.com/WB-04.24.2020-CE-Germany-BPFBReverseProxy_LP.html

A horizontal banner with a red background. In the center is a stylized globe showing the continents. Overlaid on the globe is a network of white lines, including latitude and longitude lines, and several curved lines that suggest global connectivity or data flow. Two small white circles are placed at the ends of some of these curved lines, resembling nodes or data points.

Einrichtung

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



- Verbindung Einstellung
 - Unter *User Connection Settings* verweist auf den Bereich *Mobile VPN with SSL*. Hier kann man folgendes einrichten:
 - Auf welchem Interface das Portal auf Anfragen horcht.
 - Auch der Port für die Verbindung (Standard 443) kann umgelegt werden.
 - Im Bereich *User Connection Settings*
 - Welche Authentifizierung Server für die Benutzer Anmeldung verwendet werden

Authentication Servers

Specify the authentication servers to use for connect

AUTHENTICATION SERVER

RADIUS (default)

Firebox-DB

Firebox-DB ▼

ADD
REMOVE

Firebox-DB
servers are also used by

RADIUS

fmann.local

cybersec.watch

AuthPoint

ort. This is the configurat

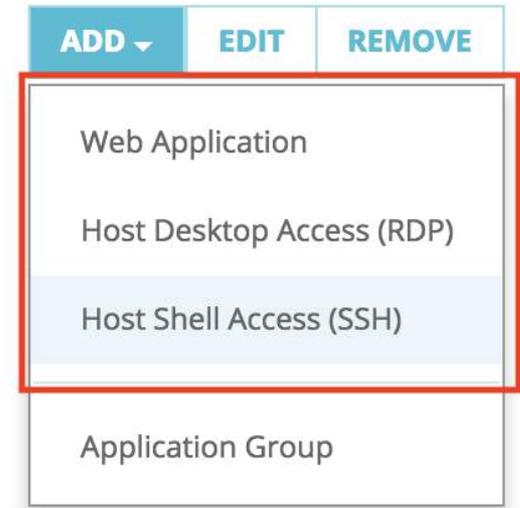
ort for Mobile VPN with S!

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

NAME	
▼ Applications	
	Windows 10
▼ Webseite	
	WatchGuard

ADD ▼	EDIT	REMOVE
Web Application		
Host Desktop Access (RDP)		
Host Shell Access (SSH)		
Application Group		

- 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 Zertifikats Kette 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 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



Sizing

Sizing Informationen zum Access Portal

- Je nach Art der Verbindung wird entsprechend Ressourcen auf der Firebox verbraucht.
- Eine RDP Session kann ca. bis zu 100MB oder mehr RAM belegen, abhängig von Einstellungen der Session.
- Man kann ungefähr so rechnen:
(Freier Speicher (RAM) / 100 MB) – 300 MB RAM = Anzahl der möglichen RDP Verbindungen.
- WatchGuard kann durch seine technischen Ansprechpartner hier helfen, um ein Sizing umzusetzen.



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 'Customization' section. The interface is organized into several sections for customization:

- Page Title:** A text input field containing 'Example Company Access Portal'.
- Custom login logo:** A checked checkbox. Below it is a preview of a blue rectangular logo with 'Example Company' text. A 'Choose File' button is followed by 'logo.jpg'. To the right are 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom header logo:** An unchecked checkbox. Below it is a circular placeholder with 'NO IMAGE AVAILABLE'. A 'Choose File' button is followed by 'No file chosen'. To the right are 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom background image:** An unchecked checkbox. Below it is a circular placeholder with 'NO IMAGE AVAILABLE'. A 'Choose File' button is followed by 'No file chosen'. To the right are 'UPLOAD' and 'RESET IMAGE' buttons.
- Custom CSS file:** An unchecked checkbox. Below it is a 'Choose File' button followed by 'No file chosen'. To the right are '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 Fireware-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	Access Portal: 0	Firewall: 0

Total Users: 0

Users Locked Out: 0 UNLOCK USERS

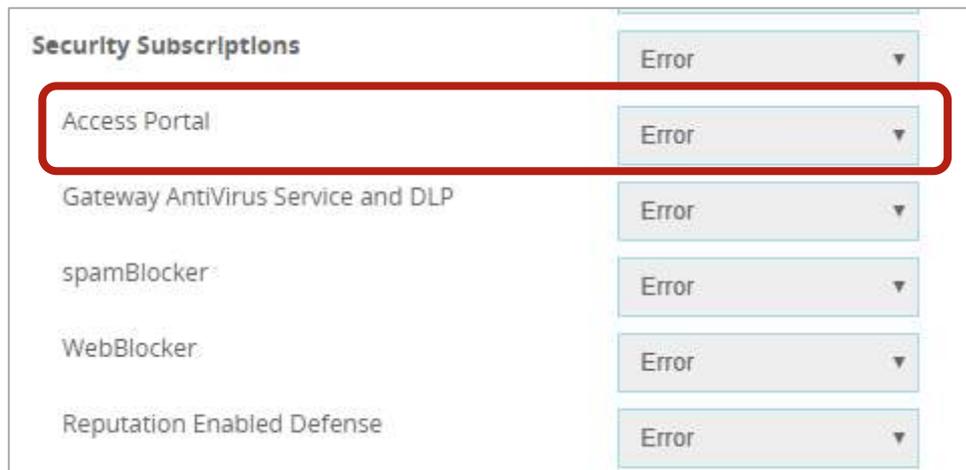
Authenticated Users

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





Live Demo



Danke !