Best Practices – 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

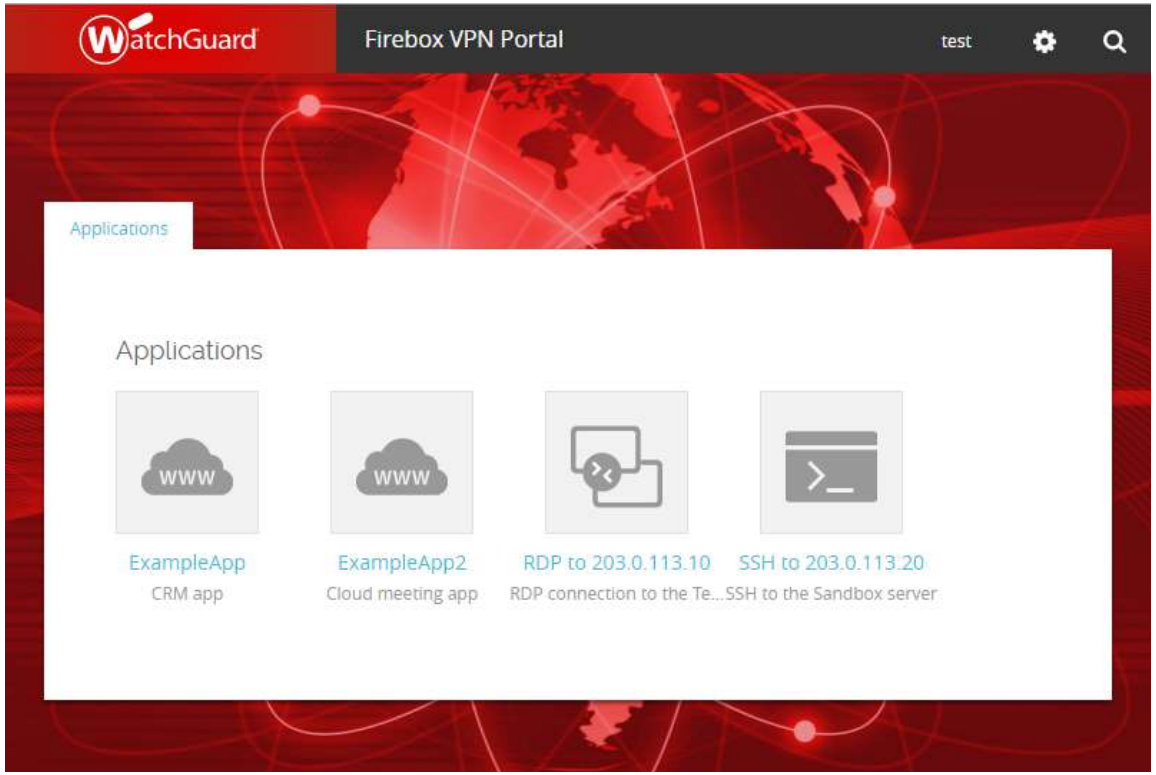
Voraussetzung

- 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 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 !!

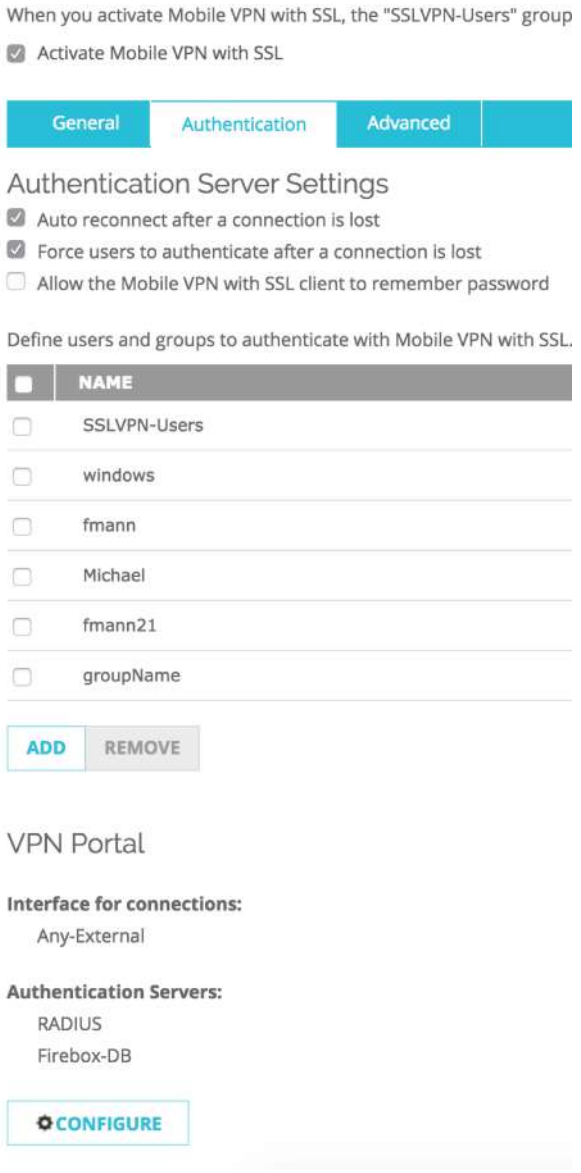
Access Portal

- 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



Access Portal — Geteilte Einstellungen

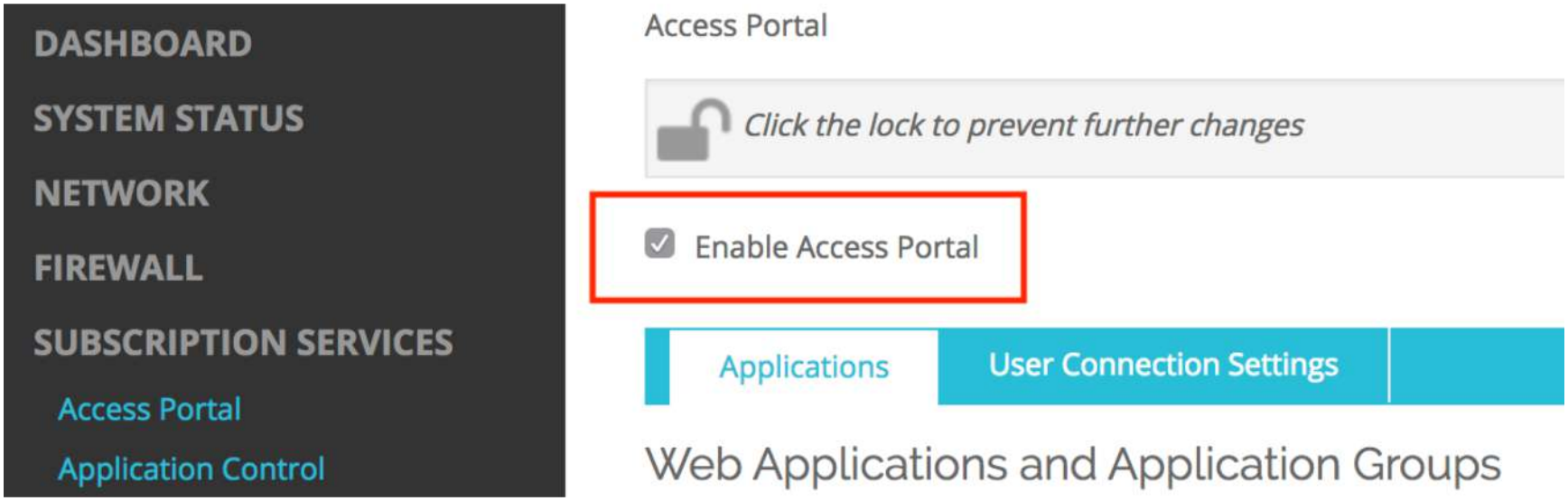
- Access Portal und Mobile VPN mit SSL teilen sich die Firewall-Policy WatchGuard SSLVPN.

- 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).

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

CONFIGURE

Authentication Servers

Specify the authentication servers to use for connec

AUTHENTICATION SERVER
RADIUS
Firebox-DB

Firebox-DB ADD REMOVE

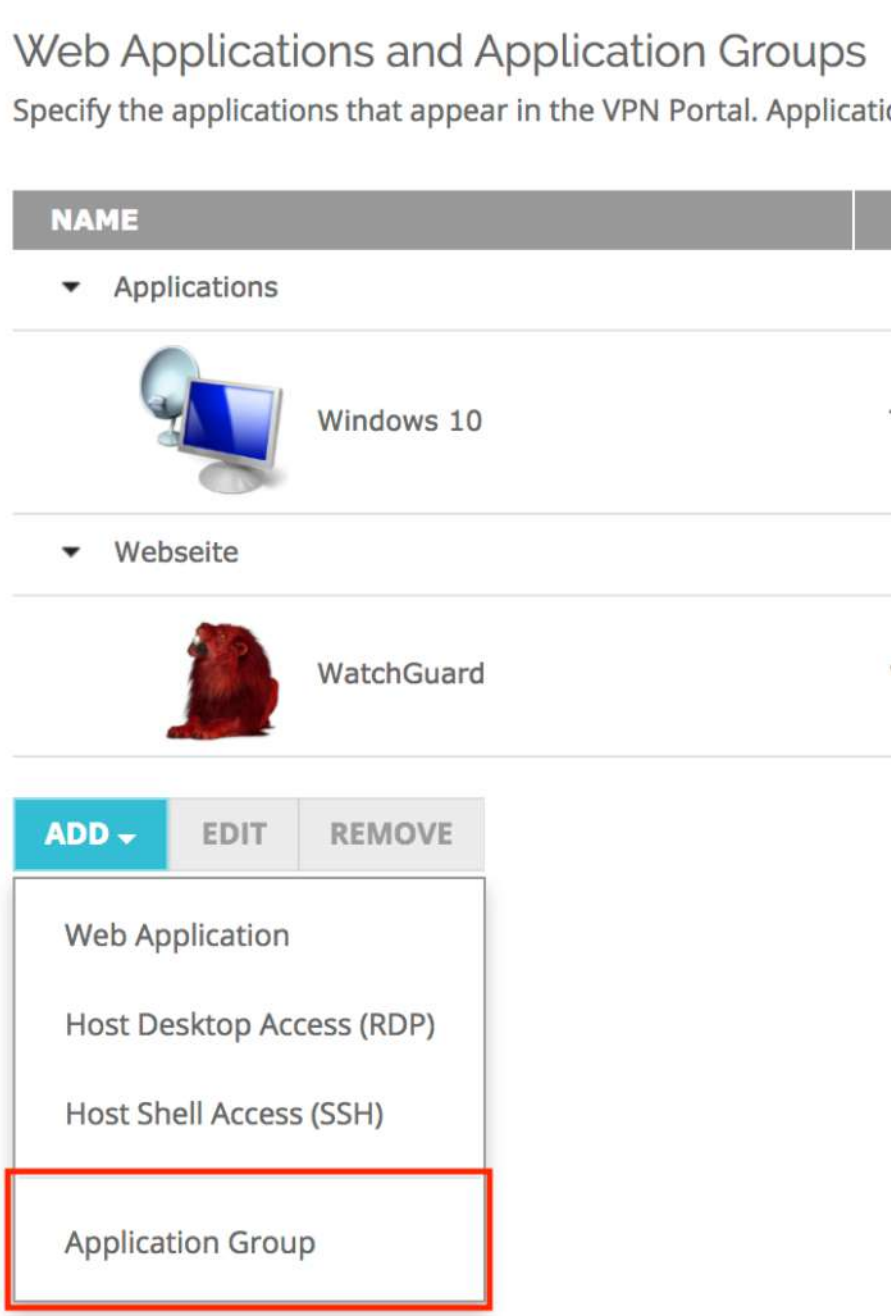
Interfaces

Specify the interfaces for connections to the VPN Pc

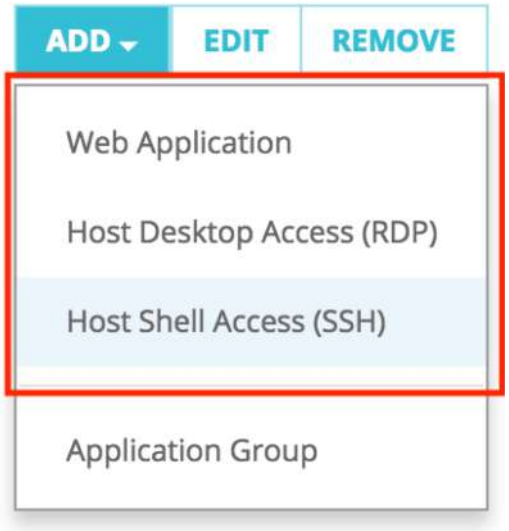
INTERFACE
Any-External

Any-External ADD REMOVE

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



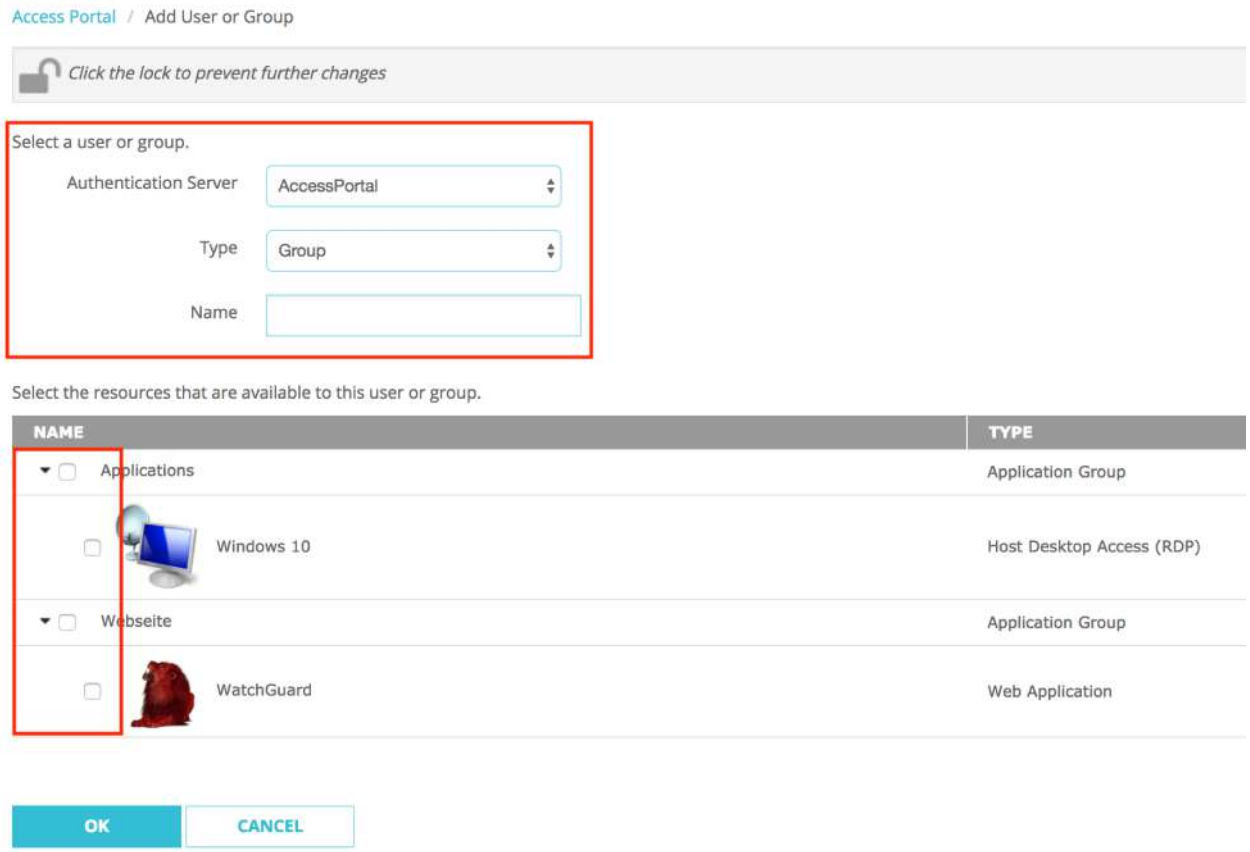
- Erst danach kann man Applikationen für die einzelnen Applikationsgruppen definieren.
- Es macht Sinn, die Applikationen nach Typen oder nach Aufgaben zu sortieren.
  - D.h. Alle RDP Session in einer Applikation Gruppe zu legen oder
  - Dem Benutzer eine eindeutige Applikation Gruppe zu ordnen, worin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

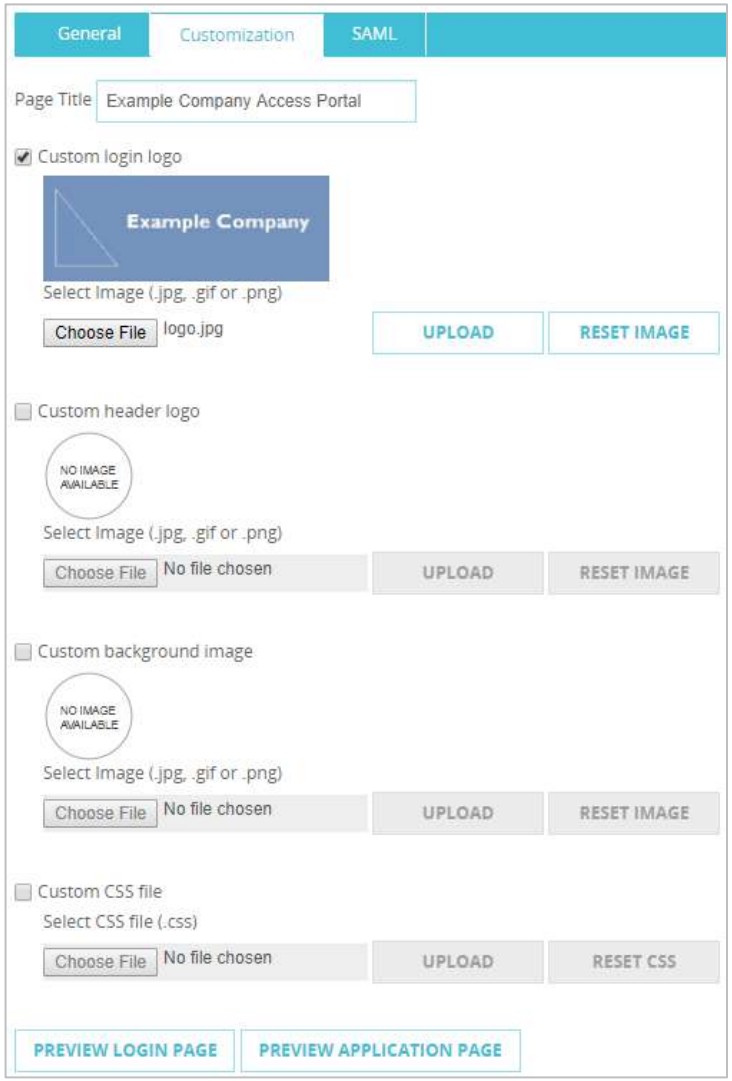
Unter https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/services/access%20portal/access_portal_config.html finden sie dazu weitere Hinweise.

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



Anpassung des Access Portals

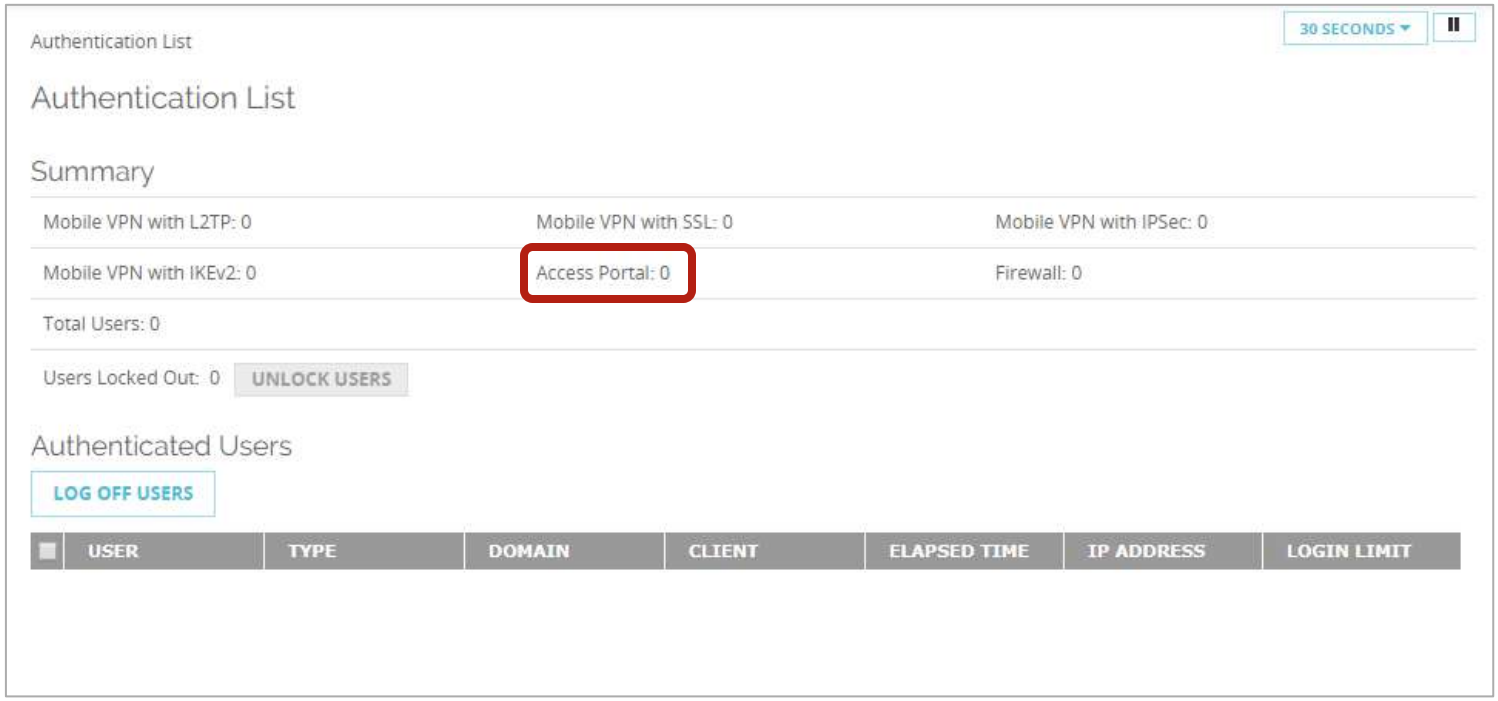
- Sie können diese Elemente der Login- und Portalseiten anpassen:
  - Seitentitel
  - Login Logo
  - Kopfzeilenlogo
  - Hintergrundbild
- Sie können auch eine benutzerdefinierte CSS-Datei hochladen, um Seitenelemente wie Schaltflächen anzupassen



Weitere Informationen

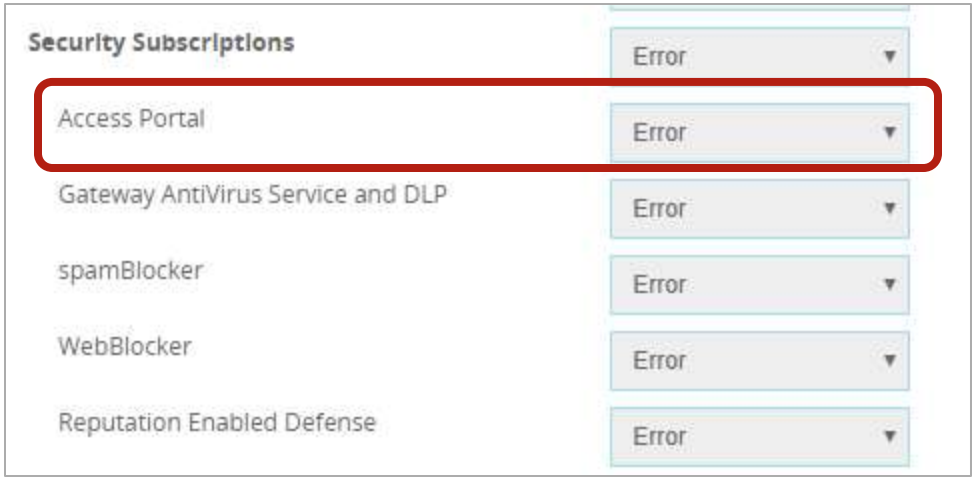
Access Portal — Authenticated Users

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



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