




# Best Practices – WatchGuard Access Portal – SAML

**Thorsten Steding**  
Sales Engineer, Central Europe

# Service in Total Security!

Features & Services	TOTAL SECURITY SUITE	Basic Security Suite
Intrusion Prevention Service (IPS)	✓	✓
App Control	✓	✓
WebBlocker	✓	✓
spamBlocker	✓	✓
Gateway AntiVirus	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Protection (DLP)	✓	
Threat Detection & Response	✓	
Access Portal* 	✓	
Dimension Command	✓	
Support	<b>Gold (24x7)</b>	Standard (24x7)

*\*Available on Firebox M370 appliances or higher.*

# Access Portal



- HTML5 application portal
  - HTML5, clientless
  - Web-application
  
- SSO to Access Portal
  - SAML 2.0
  - RADIUS, AD, Firebox-DB, ...



Platforms	
M370	M670
M400	M4600
M470	M5600
M500	Firebox Cloud
M570	FireboxV

A red-themed graphic featuring a world map in the background, overlaid with a network of white lines and nodes. The text "Access Portal: SAML Configuration Example" is centered in white.

# Access Portal: SAML Configuration Example

# Security Assertion Markup Language (SAML)

**SAML** ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.

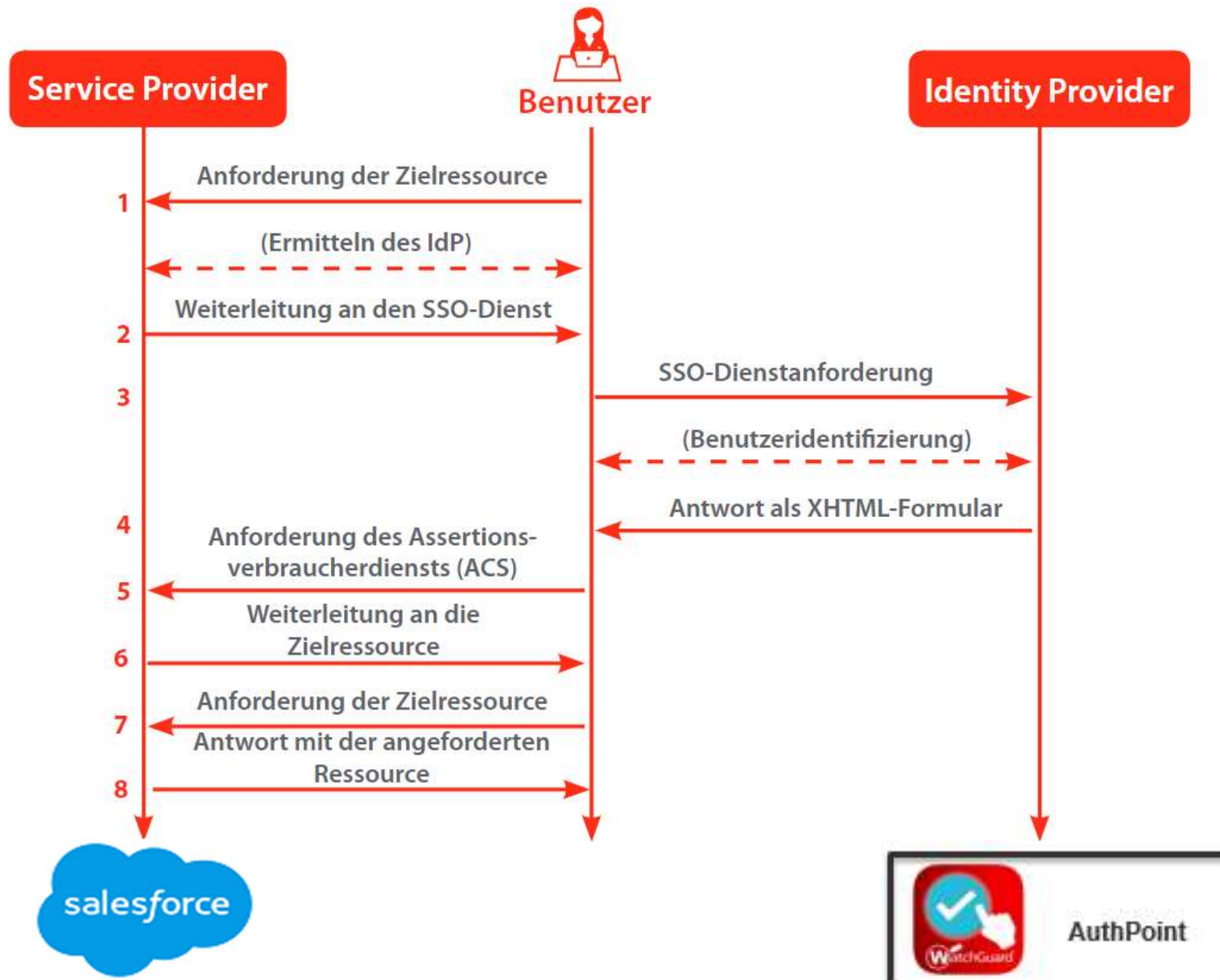
## Browser Single Sign-on:

Ein Benutzer ist nach der Anmeldung an einer Webanwendung automatisch auch zur Benutzung weiterer Anwendungen authentisiert.

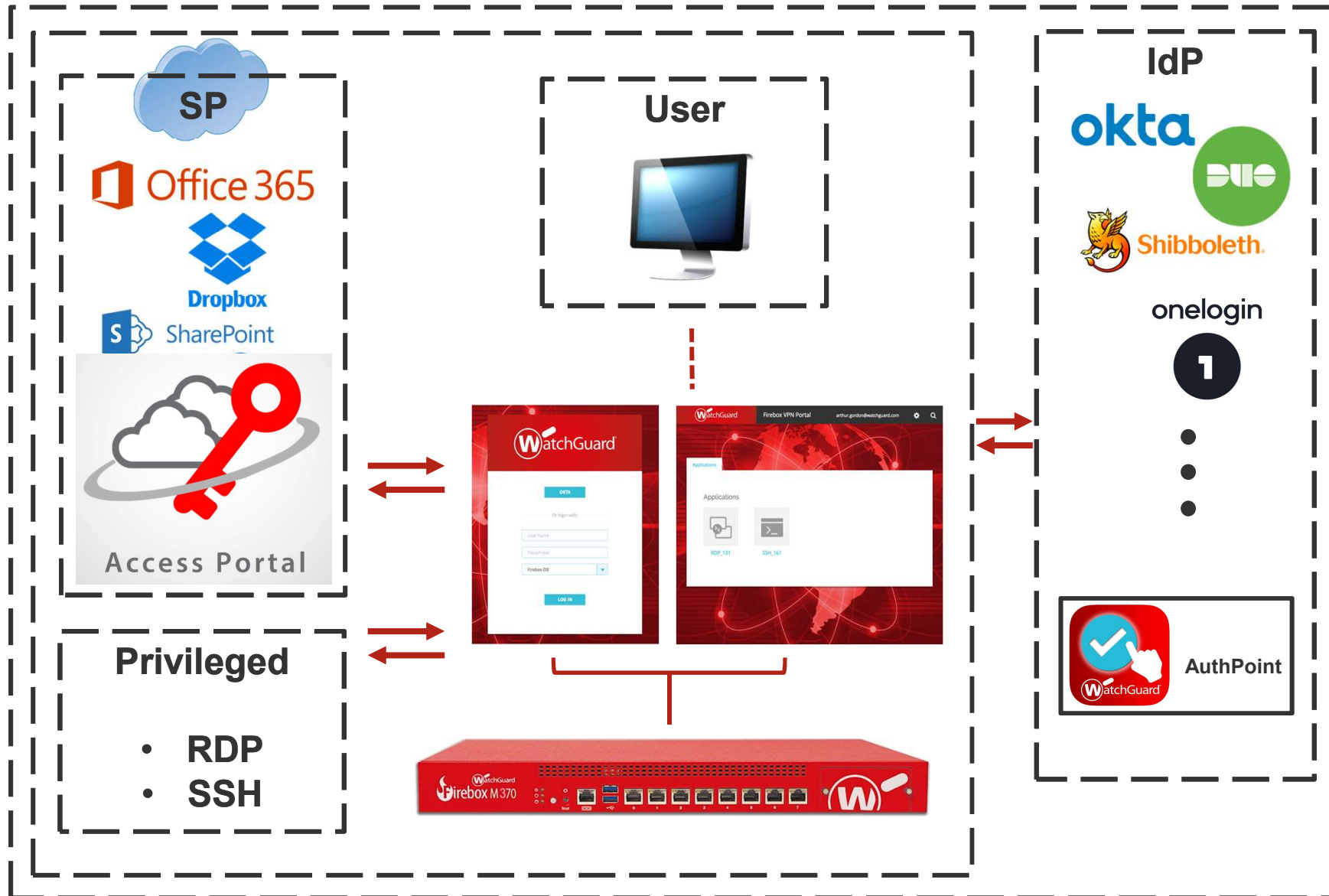
Autorisierungsdienste die Kommunikation mit einem Dienst läuft über eine Zwischenstation, den Identity Provider, der die Berechtigung überprüft.

Quelle:Wikipedia

# SAML 2.0 Workflow



# Access Portal with SAML integration



# Access Portal (SP) + AuthPoint

- Access SP metadata from Firebox SAML settings page:

The screenshot displays the WatchGuard Fireware Web UI configuration page for SAML settings. The left sidebar shows navigation options like Dashboard, System Status, Network, Firewall, and Subscription Services. The main content area is titled 'Access Portal / VPN Portal' and has tabs for 'General', 'Customization', and 'SAML'. Under 'SAML', there is a checkbox for 'Enable SAML' which is checked. The 'Service Provider (SP) Settings' section includes a 'Name of SSO' field for the IdP Name and a 'Host Name' field with a placeholder '[URL of your choice here]'. A red callout box with a white border and arrow points to the Host Name field, containing the text: 'The hostname is customizable and determines URL of SP metadata for IdP'. Below the Host Name field, a sample URL is shown: 'https:// [URL of your choice here] /auth/saml'. The 'Identity Provider (IdP) Settings' section includes an 'IdP Metadata URL' field and a 'Group Attribute Name' dropdown menu currently set to 'MemberOf' with an 'EDIT' button next to it. At the bottom of the settings are 'SAVE' and 'CANCEL' buttons.

- Expect form `https:// [customizable URL name] /auth/saml` for SP metadata



# Access Portal + AuthPoint

- Proceeding to the custom URL for SAML from the Firebox, should provide the following page data:

SAML 2.0 Configuration for WatchGuard Access Portal

After you enable SAML in the WatchGuard Access Portal configuration, you must follow one of the procedures on this page to provide SAML configuration information to your Identity Provider (IdP) administrator. The IdP administrator requires this information to configure the Access Portal as a Service Provider (SP). To make sure your IdP meets the requirements, see [SAML Single Sign-On Requirements in Fireware Help](#).

**Option 1**  
If your IdP accepts SP metadata, provide this URL to your IdP administrator.

`https:// [custom URL] .com/auth/saml/metac` **COPY**

**Option 2**  
Provide these details to your IdP administrator.

SAML Entity ID  
`https:// [custom URL] .com/auth/saml` **COPY**

Assertion Consumer Service (ACS) URL  
`https:// [custom URL] .com/auth/saml/acs` **COPY**

Single Logout Service (SLS) URL  
`https:// [custom URL] .com/auth/saml/sls` **COPY**

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIDnzCCAoegAwIBAgIEWFDduzANBgkqhkiG9w0BAQsFADBHMIRmweQYDVQQKEwpX
YXRjaEd1YXJkaWwvZmVudDQwLWVudDQwLWVudDQwLWVudDQwLWVudDQwLWVudDQw
c2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2Ft
Mw
EQYDVQQKEwpXZXRjaEd1YXJkaWwvZmVudDQwLWVudDQwLWVudDQwLWVudDQwLWVudDQw
U
RmlyZXdhcmUgc2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2FtY2Ft
AoiBAQDMvM0JmXl6eFfdwkaI40AZGH9fczV3BT3g3d+42zUnbFvJK8DgYiaUB
CpL8ioW3idglbS2FSMJYwfvUf4eJCr3NglcFm4Uj+yUK3/WODdaiGFZEdXm5E
-----
```

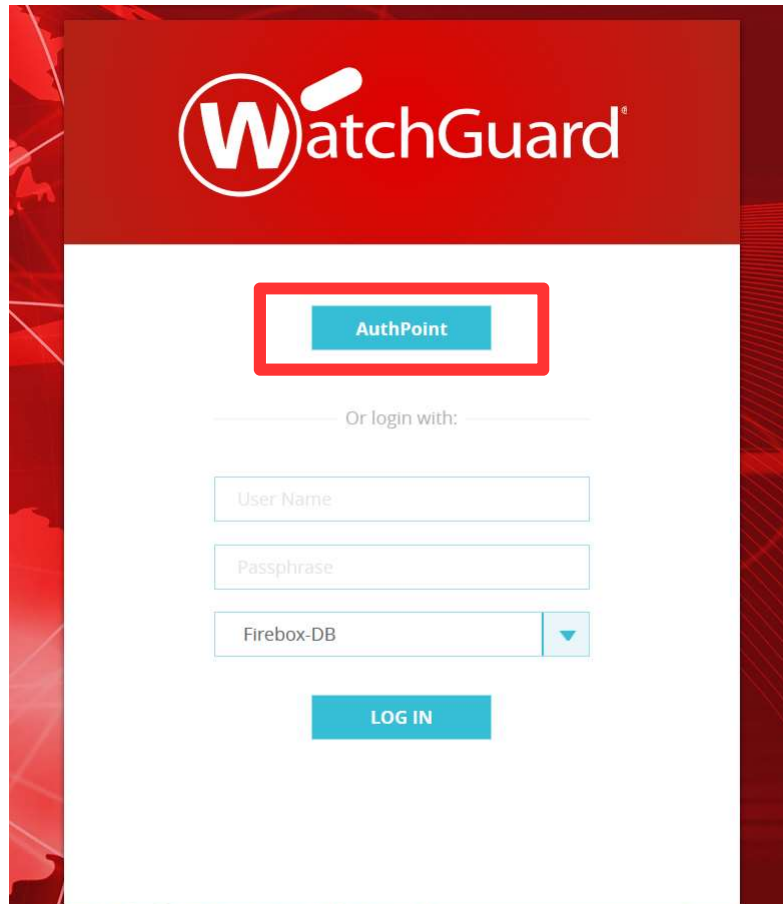
**DOWNLOAD CERTIFICATE** **COPY**

Identifies the SP to the IdP

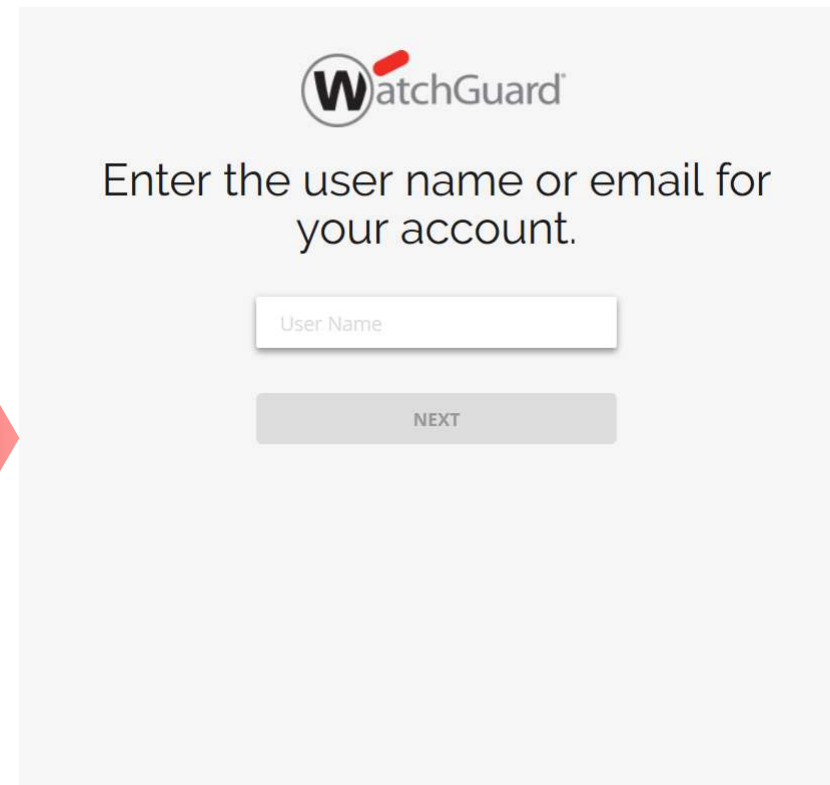
ACS URL for posting of IdP response from an SP

- Click on 'Download Certificate' and save to familiar file directory

# SAML Single Sign-On over AuthPoint

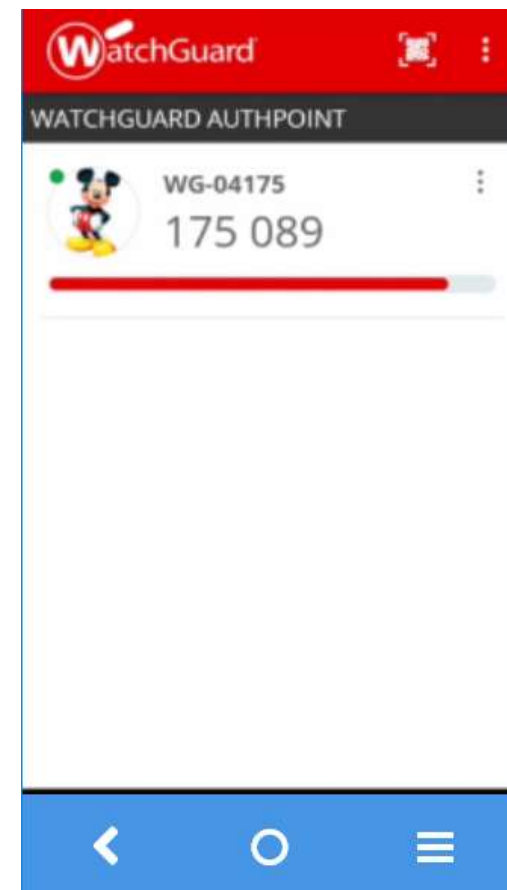
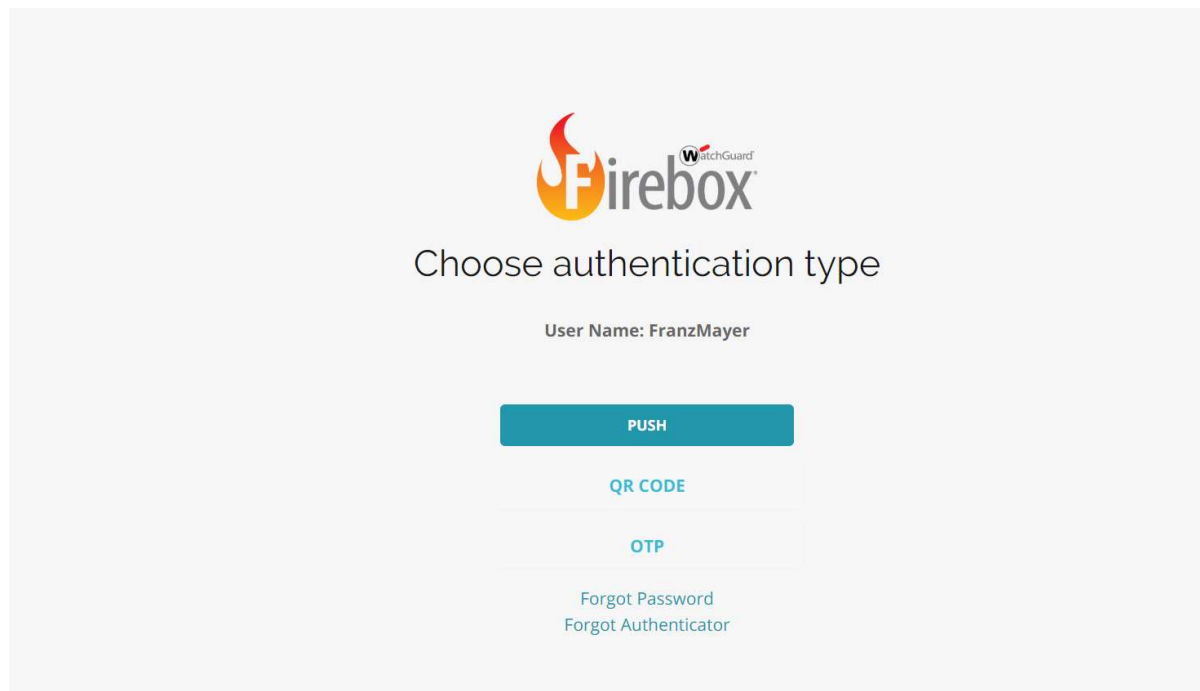


The image shows the WatchGuard login page. At the top, the WatchGuard logo is displayed. Below the logo, there is a red-bordered button labeled "AuthPoint". Underneath this button, the text "Or login with:" is followed by three input fields: "User Name", "Passphrase", and "Firebox-DB" (with a dropdown arrow). At the bottom of the form is a blue "LOG IN" button.



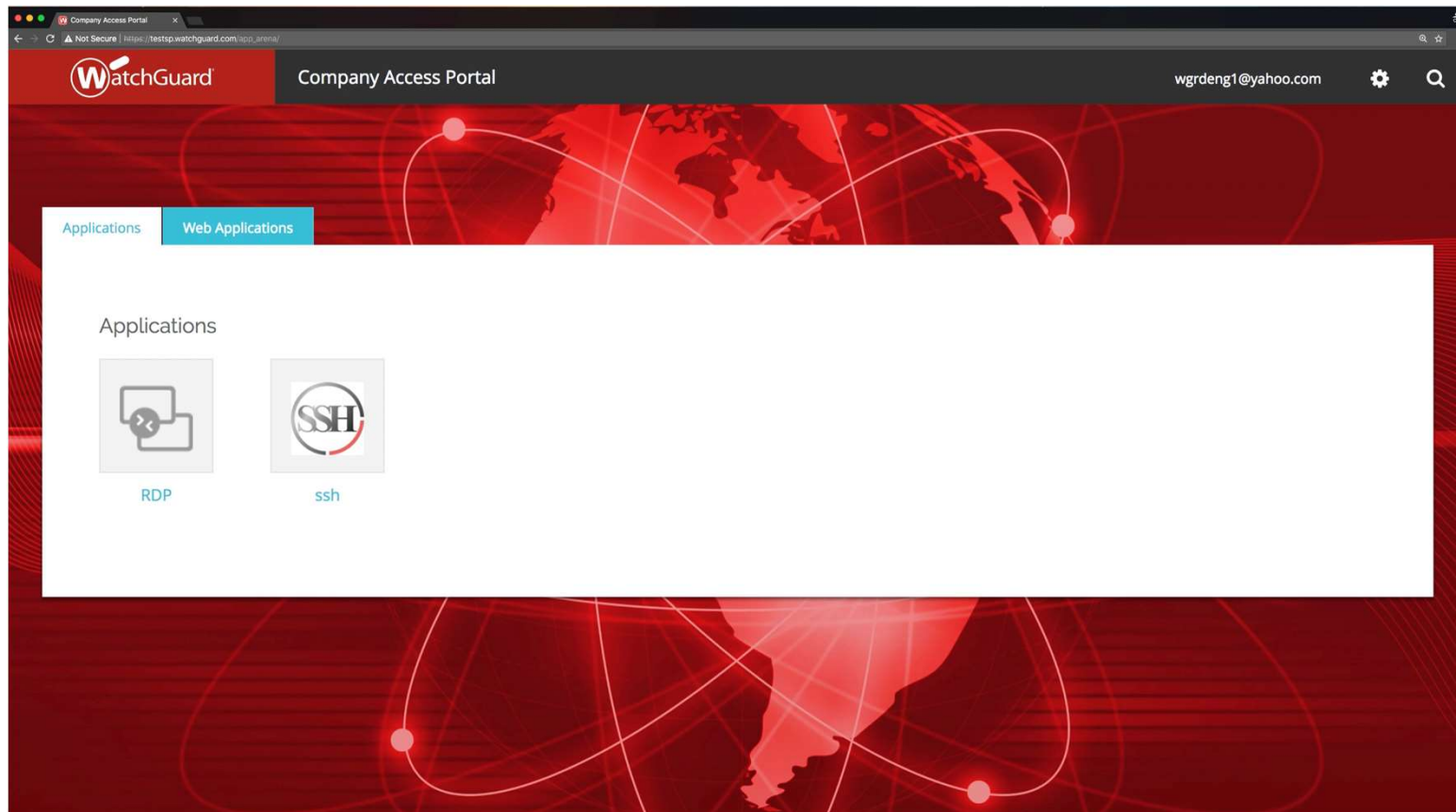
The image shows a simplified version of the WatchGuard login page. It features the WatchGuard logo at the top. Below the logo, the text "Enter the user name or email for your account." is displayed. Underneath this text is a single input field labeled "User Name". At the bottom of the form is a grey "NEXT" button.

# Zwei Faktor Authentifizierung



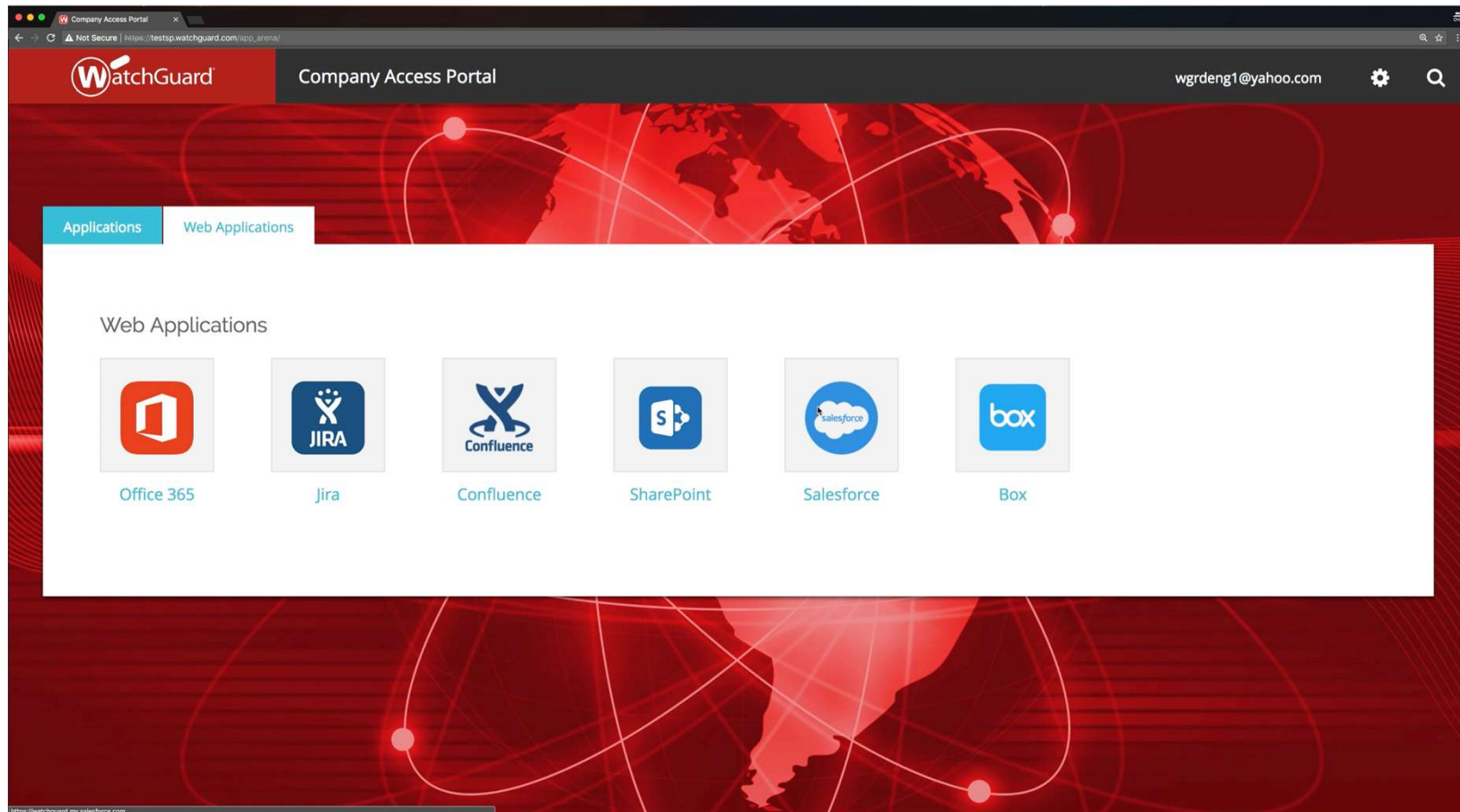
# Access Portal

- Applications tabs



# Access Portal

- Web applications tab







### Secure Cloud Wi-Fi

WatchGuard's Wi-Fi solutions provide the strongest protection from malicious attacks and rogue APs using patented WIPS technology.



### Network Security

Award-winning, enterprise-grade protection for SMBs and distributed enterprises in one cost-effective, centrally managed solution.



### Actionable Visibility

WatchGuard Dimension brings big-data visibility to network security for quick preventive or corrective action against threats.