

The background of the title slide is a vibrant red color. It features a stylized globe in the center, with white lines representing a network or data flow. The globe is semi-transparent, allowing the network lines to be seen through it. The overall aesthetic is modern and technical.

Best Practices WatchGuard AuthPoint - Integration in die WatchGuard Firebox

Thomas Fleischmann
Senior Sales Engineer CE
Thomas.Fleischmann@watchguard.com

Agenda

- Konzept von AuthPoint
- Schnittstellen in der Firebox zu AuthPoint
 - VPN mit RADIUS
 - Access Portal mit SAML / RADIUS
 - User Login Firebox mit RADIUS
- *Live Demo*



Konzept von AuthPoint

WatchGuard AuthPoint - MFA Das ist **wirklich** einfach



Multi-Factor Authentication

Password | Push Message | Phone Biometrics | Mobile Phone DNA



AuthPoint Mobile App

iOS & Android | 11 Sprachen | OTP | QR Code | Multiple Authenticators



WatchGuard Cloud

Visibility | Configuration | Management | Token-Zuweisung in Sekunden



Umfangreiche MFA-Abdeckung

Dutzende von 3rd Party Integrationen | Web SSO | Windows/Mac Computer Logon

Voraussetzungen

- Benutzer sind im AD und bei WatchGuard AuthPoint angelegt.
- Benutzer können ihren Token verwenden.
- WatchGuard AuthPoint Gateway ist installiert.
- RADIUS funktioniert mit der Firebox für VPN oder andere Funktionen.



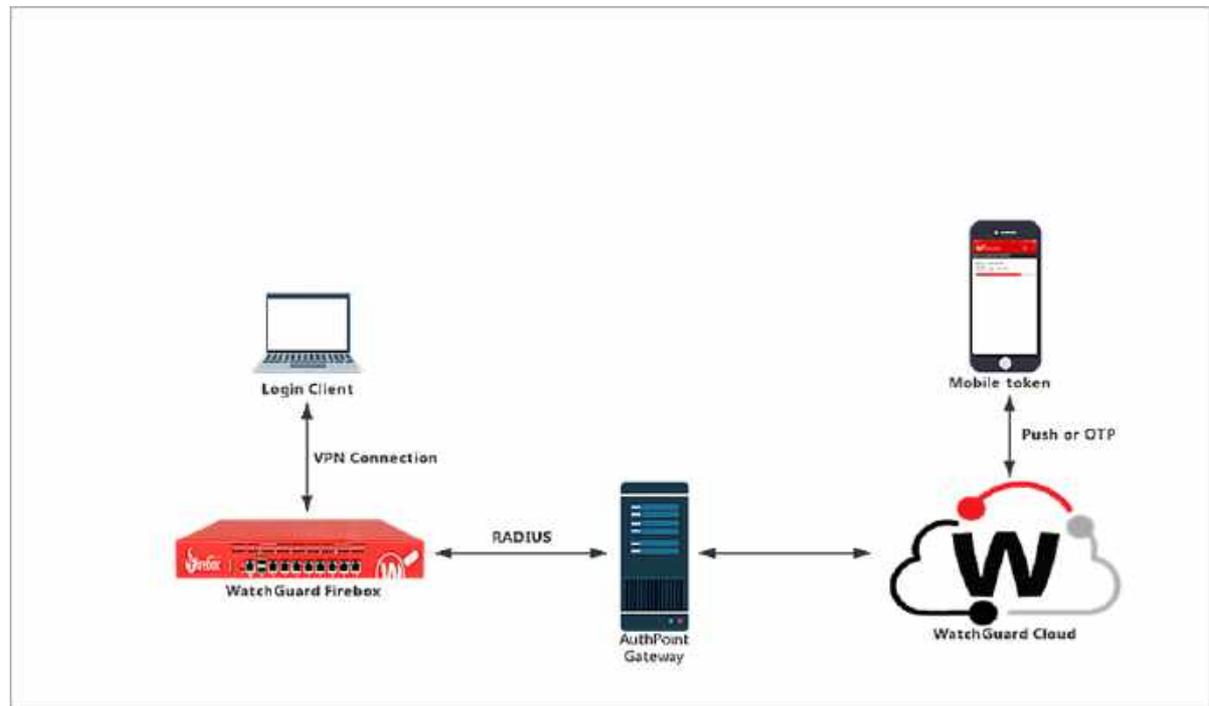
VPN mit RADIUS

VPN mit RADIUS

- Integration Guides zu den einzelnen VPN Arten mit AuthPoint können unter folgende Links gefunden werden:
 - IPsec: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ipsec-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C 4
 - SSL VPN: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ssl-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C 2
 - L2TP: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-l2tp-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C 3
 - IKEv2: https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/firebox-ikev2-vpn-radius_authpoint.html?tocpath=Self-Help%20Tools%7CIntegration%20Guides%7CAuthPoint%7C 1

VPN mit RADIUS

- Als Beispiel wird hier kurz die folgende Integration dargestellt
 - „Firebox Mobile VPN with SSL Integration with AuthPoint”



VPN mit RADIUS

Servers / Radius / Edit

 Click the lock to prevent further changes

Before you configure your Firebox device to use a RADIUS authentication server, ma

Domain Name

Primary Server Settings

Enable RADIUS Server

IP Address:

Port:

Shared Secret:

Confirm Secret:

Timeout:

seconds

Retries:

Dead Time:

Minutes

Group Attribute:

- Zu einem überprüft man die Einstellung des RADIUS Server auf der Firebox.

– Timeout sollte man auf 60 Sekunden ändern.

– Group Attribute muß den Wert 11 enthalten. Dieser Wert ist auch als Filter-Id bekannt.

VPN mit RADIUS

General Authentication Advanced

Authentication Server Settings

Specify the authentication servers to use for connections to Mobile SSL with VPN.

AUTHENTICATION SERVER

RADIUS (default) ←

Firebox-DB

Firebox-DB ▾ ADD REMOVE

Note: These authentication servers are also used by the Access Portal. Changes to

Users and Groups

Specify the users and groups for Mobile VPN with SSL. The users and groups you specify must be defined in the Active Directory. If you select Host Sensor Enforcement, hosts must meet the Host Sensor Enforcement requirements for mobile VPN.

SELECT	NAME	TYPE	SERVER
<input checked="" type="checkbox"/>	SSLVPN-Users	Group	Any
<input checked="" type="checkbox"/>	AuthPoint	Group	RADIUS

- Im der Mobile User VPN Einstellung für SSL muß der RADIUS Server als Authentifizierung Server aktiviert werden.

- Des Weiteren muß eine Gruppe mit den Gruppennamen des RADIUS Server dort hinterlegt sein.

VPN mit RADIUS

- Unter den Einstellungen in WatchGuard AuthPoint ist es wichtig, dass der RADIUS Name mit den Einstellungen auf dem RADIUS Client in der Firebox übereinstimmt.
- Die **Timeout** Einstellungen sollten entsprechend angepasst werden.

RADIUS Client

Name *
AuthPoint

RADIUS client trusted IP or FQDN *
10.0.1.254

Value sent for RADIUS attribute 11 (Filter-Id) *
User's Active Directory groups

To change your Shared Secret please fill out the field below, or leave blank for no change.

Shared Secret
Shared Secret

Enable MS-CHAPv2

NPS RADIUS Server trusted IP or FQDN *
10.0.1.225

Port *
1812

Timeout In Seconds *
30

VPN mit RADIUS

- Im AuthPoint Gateway Einstellungen muß die Radius Ressource hinzugefügt werden.

RADIUS

Port *

1822

Select a RADIUS resource

AUTHPOINT × DIMENSION ×

Select a RADIUS

- Wichtig ist hierbei, dass man den RADIUS Port auf den notwendigen Wert einstellt.

VPN mit RADIUS

- Zum Schluss sollte man überprüfen, ob der Benutzer auch die Ressource über seine Gruppe erhält !
- Hier ist es wichtig bei den VPN Ressourcen zu definieren, ob der User sich per Push oder Eingabe des OTP am System authentifiziert.

Resources	Resource Type	Password	OTP	Push	QR Code
Access Portal	SAML	✓	✓	✓	✓
 AuthPoint	RADIUS Client	✓		✓	
WGDC	IDP Portal	✓	✓	✓	✓
LogonApp	Logon App	✓	✓	✓	✓
Salesforce	SAML	✓	✓	✓	✓
Dimension	RADIUS Client	✓		✓	
Home AP	SAML	✓	✓	✓	✓



Access Portal mit SAML / RADIUS

Anleitung

- Die Anleitung finden sie unter

https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/AuthPoint/access-portal-saml_authpoint.html?tocpath=Integration-Guides%7CAuthPoint%7CAmazon%20Web%20Services%20Integration%20with%20AuthPoint%7C 18

- Weitere Anleitungen unter

https://www.watchguard.com/help/docs/help-center/en-US/Content/Integration-Guides/_intro/authpoint-integrations.html

Konfiguration des WatchGuard Access Portals

- Unter <https://cloud.watchguard.com> – einloggen.
- Im AuthPoint Bereich unter „Resources“ den Link „Copy SAML Metadata URL“ kopieren.

Resources

Choose a resource type



ADD

NAME



TYPE

Access Portal

SAML

groupName

RADIUS Client

LogonApp

Logon App

Salesforce

SAML

WGDCE

IdP Portal

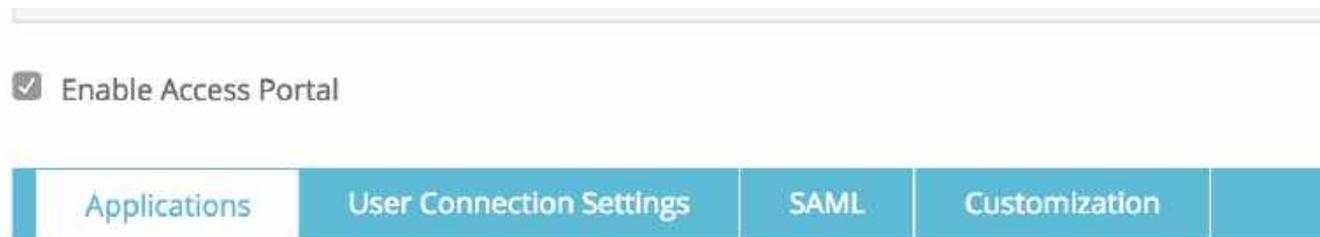
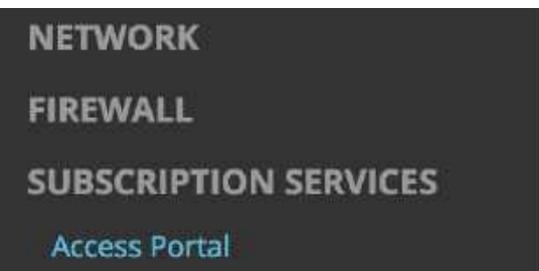
DOWNLOAD METADATA

DOWNLOAD CERTIFICATE

COPY SAML METADATA URL

Konfiguration des WatchGuard Access Portals

- In der Konfiguration der WatchGuard Firewall im Bereich „Subscription Services“ den Menü-Punkt „Access Portal“ auswählen.
- Den Punkt „[Enable Access Portal](#)“ anklicken und speichern.



Konfiguration des WatchGuard Access Portals

- Version 12.1.x:
 - Öffnen des Bereichs „User Connection Settings“ und dort den Button „Configure“ anklicken.
 - Den Karteireiter „SAML“ auswählen.
- Version 12.2:
 - Direkte Wahl des Karteireiters „SAML“.
- Auswahl „Enable SAML“, um ein SAML basierte MFA zu konfigurieren.

Enable Access Portal

Applications

User Connection Settings

SAML

Customization

To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IdP) you specify.

Enable SAML

Service Provider (SP) Settings

Konfiguration des WatchGuard Access Portals

Enable Access Portal

Applications

User Connection Settings

SAML

Customization

To authenticate Access Portal users with SAML single sign-on, the Firebox exchanges authentication information with an Identity Provider (IdP) you specify.

Enable SAML

Service Provider (SP) Settings

To configure your Firebox as the SAML Service Provider, specify the name of your IdP to appear as the authentication server name.

IdP Name

For the Host Name, specify a fully qualified domain name that resolves to the Firebox external interface.

Host Name

DNS Name des Dienstanbieters

After you save the configuration to your Firebox, follow the IdP configuration instructions at <https://accessportal.cybersec.watch/auth/saml>

SAML Konfiguration Seite

Identity Provider (IdP) Settings

Specify the SAML connection settings for your third-party Identity Provider.

IdP Metadata URL

META Daten Link von AuthPoint

Group Attribute Name

EDIT

Konfiguration des WatchGuard Access Portals

Option 2

Provide these details to your IdP administrator.

SAML Entity ID

[COPY](#)

Authpoint: Service Provider Entity ID

Assertion Consumer Service (ACS) URL

[COPY](#)

AuthPoint: Assertion Consumer Service

Single Logout Service (SLS) URL

[COPY](#)

AuthPoint: Logout URL

X.509 Certificate

```
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgI EWsYE8TANBgkqhkiG9w0BAQsFADBHMRMwEQYDVQQKEwpX
YXRjaEd1YXJkMREwDwYDVQQLEwhGaXJld2FyZTEdMBsGA1UEAxMURmlyZXdhcmUg
c2FtbCBDbGllbnQwHhcNMTEwMzA2MTEwMzUzWhcNMTEwMzA2MTEwMzUzWjBHMRMw
EQYDVQQKEwpYXRjaEd1YXJkMREwDwYDVQQLEwhGaXJld2FyZTEdMBsGA1UEAxMU
RmlyZXdhcmUgc2FtbCBDbGllbnQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AolBAQD1fKfW7Me8AHOw/rdDtoFmQ81nhQI3Ys997wQf7I0PcYqGfxTq2D70KPrI
Pazbb3ZTfoExo9qKNI1b9sow/QPK9cEX8ncp7viEP1gExM3q5tZmM8OrV+35OrPG
PWzqo6OEJYuYGI1PQ3wKrX4VDeHmMHwzvekobG44y4ytLzjbzocIR3mhvJdAX/B
YNQdKdQ349/1I90C7x8a3UFUpDp/9Yb3ldS0DLcRjlbzU5JNeQTsgKIOXVEjWhTX
clQGSso826A8W34DOXaNC7//BBMOXiDBOBh9iRXRPxJlgJwc421QaOe8/pMP1MhO
tnF3X1qQbTpS1YqFwh+2bXCptI2/AgMBAAGjZGwgZUwJgYDVR0RB8wHYIbYWNj
-----END CERTIFICATE-----
```

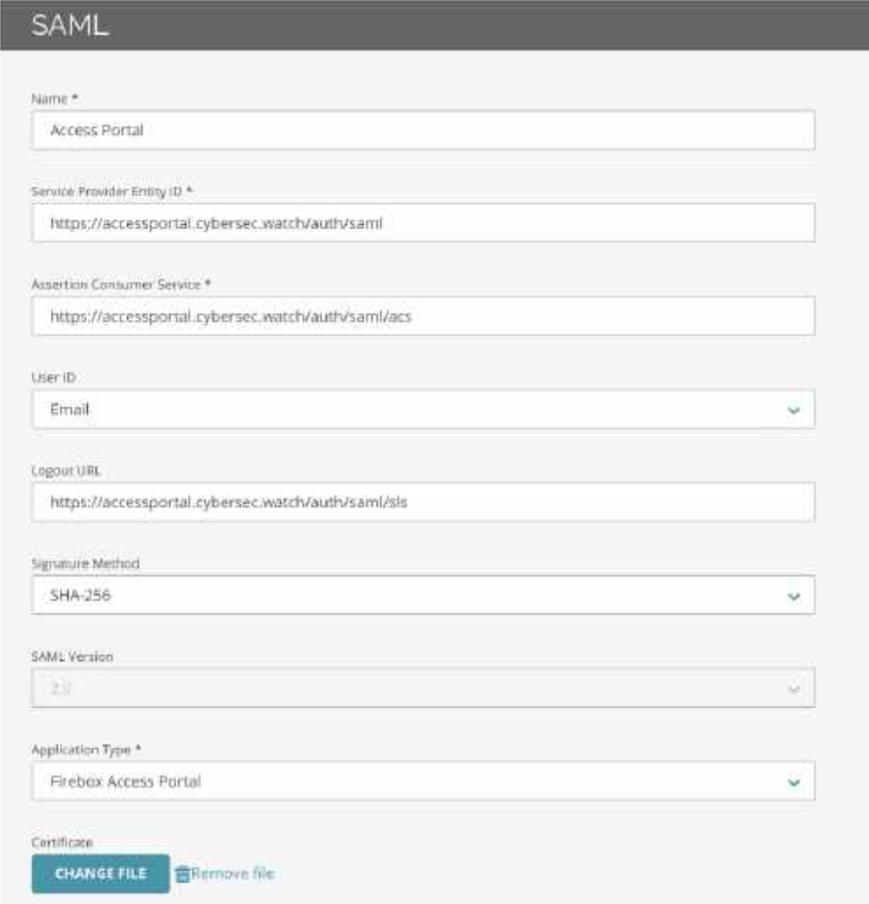
[DOWNLOAD CERTIFICATE](#)

[COPY](#)

Zertifikat, was in AuthPoint mit der
Ressource gespeichert werden muss.

Konfiguration von WatchGuard AuthPoint

- Die Daten aus dem Access Portal übernehmen (Copy & Paste).

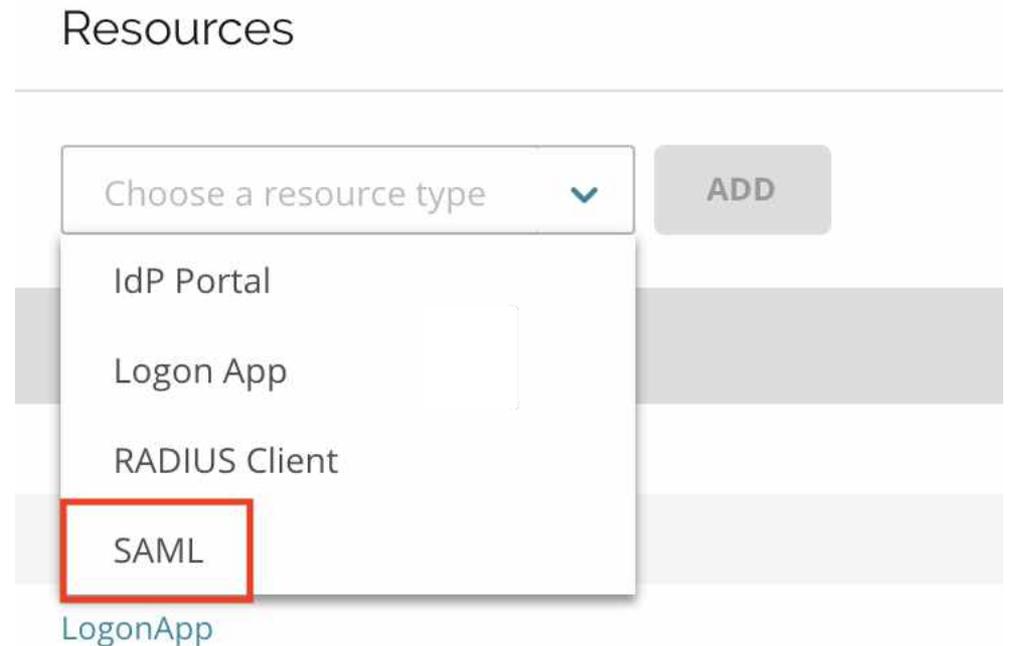


The screenshot shows the SAML configuration page in WatchGuard AuthPoint. The page has a dark header with the word "SAML" in white. Below the header, there are several form fields and dropdown menus for configuring SAML settings. The fields are as follows:

- Name ***: Text input field containing "Access Portal".
- Service Provider Entity ID ***: Text input field containing "https://accessportal.cybersec.watch/auth/saml".
- Assertion Consumer Service ***: Text input field containing "https://accessportal.cybersec.watch/auth/saml/acs".
- User ID**: Dropdown menu with "Email" selected.
- Logout URL**: Text input field containing "https://accessportal.cybersec.watch/auth/saml/sls".
- Signature Method**: Dropdown menu with "SHA-256" selected.
- SAML Version**: Dropdown menu with "2.0" selected.
- Application Type ***: Dropdown menu with "Firebox Access Portal" selected.
- Certificate**: A section with a "CHANGE FILE" button and a "Remove file" link with a trash icon.

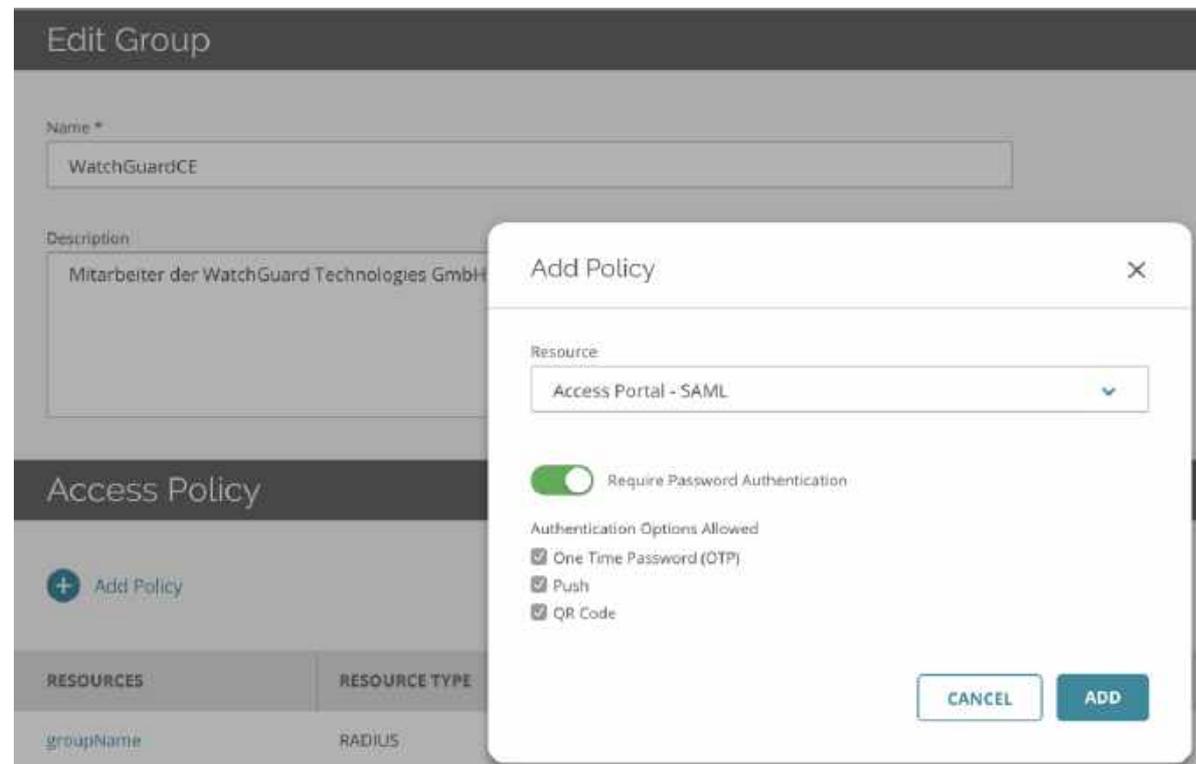
Konfiguration von WatchGuard AuthPoint

- Unter der Konfiguration von WatchGuard AuthPoint eine neue Ressource des Typ „SAML“ erstellen.



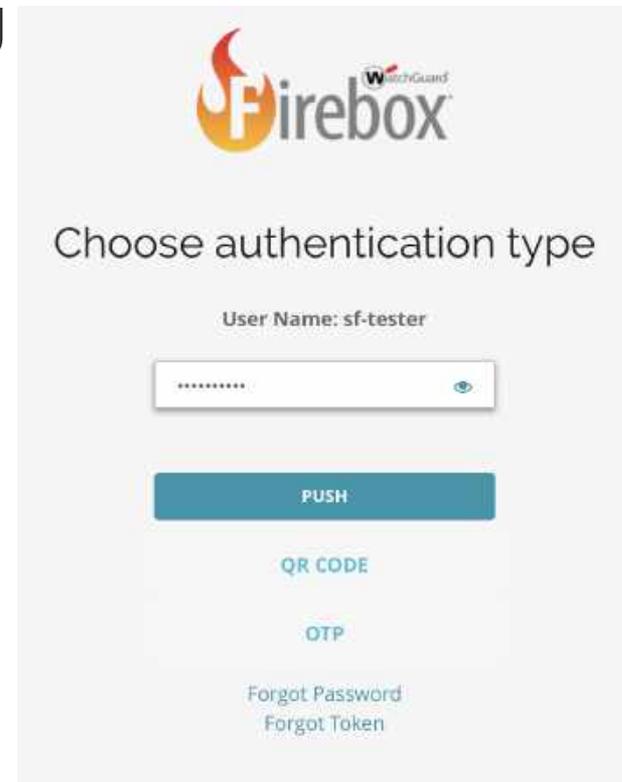
Konfiguration von WatchGuard AuthPoint

- Die gespeicherte Ressource für das Access Portal einer Gruppe in AuthPoint hinzufügen.
- Festlegen, welche Access Policy die Gruppe hat.



Test

- Anmelden an dem Access Portal der Firewall
 - `https://<FQDN der Firebox>`
- Auswahl der MFA Authentifizierung
 - Gewählter IdP Name im Portal
- Auf dem IdP-Portal anmelden
 - Je nach zugelassener Methode





User Login Firebox mit RADIUS

User Login Firebox mit RADIUS

- Im Bereich **User and Roles** kann man weitere Systeme Benutzer anlegen.
- In der Konfiguration des Benutzer wird dann die Art der Authentifizierung festgelegt.

Add User

User Name: fmann21

Authentication Server: AuthPoint

Role: Firebox-DB, RADIUS

Passphrase: fmann.local

Confirm Passphrase: cybersec.watch

AuthPoint

OK CANCEL

User Login Firebox mit RADIUS

- Beim Login an der Firebox muß man nun folgende Informationen angeben.
 - Username
 - Passwort
 - RADIUS
(Authentifizierungsmethode)
 - RADIUS Gruppe
(Hier als Wert DOMAIN abgefragt)

User Name

fmann21

Passphrase

●●●●●●●●

Authentication Server

RADIUS

Domain

AuthPoint

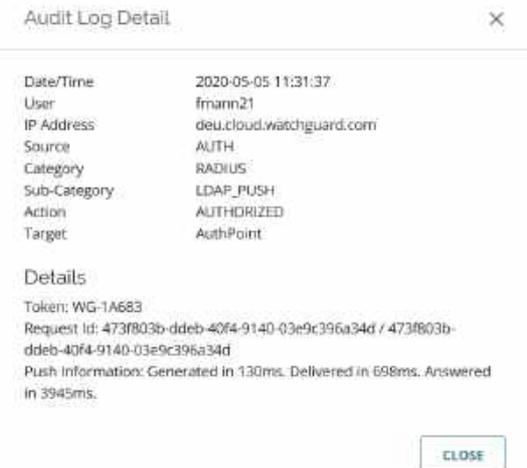
LOG IN



Troubleshooting

Troubleshooting

- Es existiert mehrere Informationen zu Anmeldungen im System.
- In der WatchGuard Cloud werden im Bereich **Monitor** Anmeldungen und Fehlschläge der selbigen als Report generiert.
- Im Bereich **Administration -> Audit Log** werden auch alle Anmeldungen (Erfolgreich und Fehlgeschlagene) erfasst und mit Informationen dargestellt.



Audit Log Detail

Date/Time	2020-05-05 11:31:37
User	fmam21
IP Address	deu.cloud.watchguard.com
Source	AUTH
Category	RADIUS
Sub-Category	LDAP_PUSH
Action	AUTHORIZED
Target	AuthPoint

Details

Token: WG-1A683
Request Id: 473f803b-ddeb-40f4-9140-03e9c396a34d / 473f803b-ddeb-40f4-9140-03e9c396a34d
Push Information: Generated in 130ms. Delivered in 698ms. Answered in 3945ms.

CLOSE

Troubleshooting

Fehlerbehebung bei RADIUS-Authentifizierung

- Sehen Sie sich diese Logmeldungen und Fehlermeldungen an:
 - Audit-Protokolle in der WatchGuard-Cloud
 - RADIUS-Protokolle auf dem AuthPoint Gateway
 - RADIUS-Client-Fehlermeldungen
 - Firebox-Protokollmeldungen - Wenn die Firebox als RADIUS-Client konfiguriert ist, durchsuchen Sie die Firebox-Protokollmeldungen nach Benutzerauthentifizierungsereignissen und Verbindungsfehlern zwischen der Firebox und dem AuthPoint Gateway.

Troubleshooting

Fehlerbehebung bei der LDAP-Authentifizierung

- Sehen Sie sich diese Logmeldungen an:
 - Suchen Sie in den LDAP-Protokollen auf dem Gateway:
 - Ergebnisse der Konnektivitätstests
 - Synchronisierungsereignisse
 - Anfragen zur Benutzerauthentifizierung
 - Fehler bei Verbindungen mit dem Domänencontroller
 - Suchen Sie in den Audit-Protokollen der WatchGuard-Cloud nach:
 - LDAP-Änderungen der external identity
 - LDAP-Benutzer-Synchronisationsfehler

- In diesem Verzeichnis finden Sie die Gateway-Protokolldateien:
C:\ProgramData\WatchGuard\AuthPoint\Protokolle



Live Demo



Danke