WatchGuard Access Portal

Ausweitung der WatchGuard Sicherheit auf geschäftskritische Ressourcen in der Cloud

Was ist das WatchGuard Access Portal?

Das Access Portal, Teil der Total Security Suite (TSS) von WatchGuard, ist ein Dienst, mit dem Sie schnell und problemlos einen zentralen Zugang zu Ihren Cloud-gehosteten Anwendungen bereitstellen können. Es wurde für Unternehmen konzipiert, die auf Cloud-Ressourcen angewiesen sind. Mit diesem Portal können kleine und mittelständische Unternehmen kostenintensive Authentifizierungsbereitstellungen vermeiden. Das Access Portal umfasst ein HTML5-Anwendungsportal, Single-Sign-On-Unterstützung (SSO) für RDP-/SSH-Intranetdienste und SAML 2.0 zur Reduzierung des Verwaltungsaufwands. Die durchschnittliche Wachstumsrate von Cloud-Plattformen, -Unternehmensdiensten und -Anwendungen wird zwischen 2015 und 2020 voraussichtlich 22 % pro Jahr betragen. Das bedeutet einen Anstieg auf 236 Milliarden USD und macht eine Zugangskontrolle für sensible Cloud-Ressourcen unerlässlich.

Was ist SAML 2.0?

Security Assertion Markup Language (SAML) ist ein Standard für die Anmeldung von Benutzern bei weiteren Anwendungen auf Basis einer vorhandenen Sitzung. Dieser Standard für einmaliges Anmelden (Single Sign-On, SSO) bietet gegenüber der Anmeldung mit einem Benutzernamen/Kennwort erhebliche Vorteile:

- Die Eingabe der Anmeldedaten entfällt.
- Die Mitarbeiter müssen sich keine Kennwörter merken oder diese erneuern.
- Die Verwendung unsicherer Kennwörter ist ausgeschlossen.

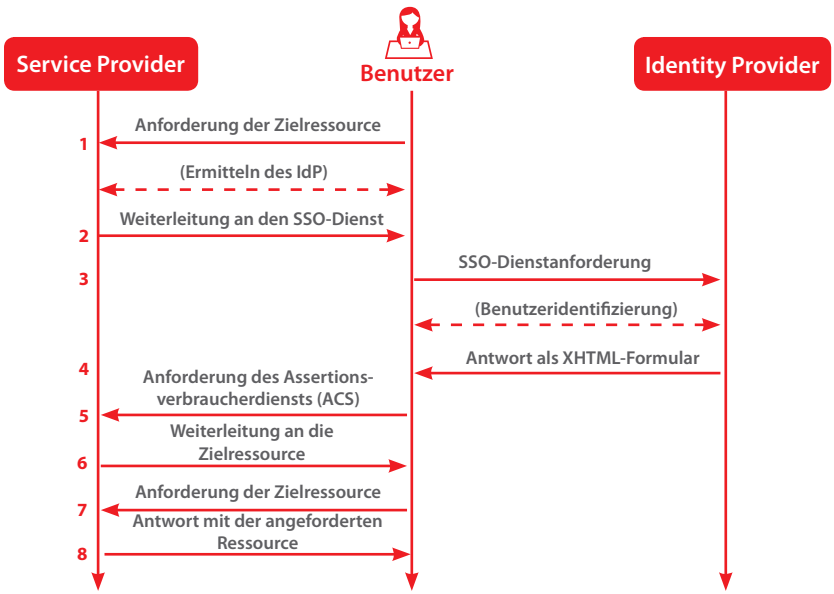
Ein Großteil aller Unternehmen kennt die Identitäten ihrer Benutzer bereits, da diese in der Active Directory-Domäne oder im firmeneigenen Intranet angemeldet sind. Diese Informationen können effizient verwendet werden, um die Benutzer auch bei anderen Programmen, wie webbasierten Anwendungen, anzumelden. SAML zählt zu den ausgereiften Standards hierfür.

Wie funktioniert die einmalige Anmeldung mit SAML 2.0?

Beim Single Sign-On mit SAML wird die Benutzeridentität vom Identity Provider zum Service Provider übertragen. Dazu werden digital signierte XML-Dokumente ausgetauscht.

Das folgende Beispielszenario veranschaulicht den Vorgang: Ein Benutzer hat sich in einem System angemeldet, das als Identity Provider (IdP) fungiert. Er möchte sich bei einer Remote-Anwendung anmelden, zum Beispiel einem Support- oder Buchhaltungsprogramm (den Service Provider, SP). Dies geschieht folgendermaßen:

1. Der Benutzer greift über einen Link im Intranet, ein Lesezeichen oder eine sonstige Verknüpfung auf die Remote-Anwendung zu. Die Anwendung wird geladen.
2. Die Anwendung bestimmt die Herkunft des Benutzers, beispielsweise anhand der Unterdomäne der Anwendung oder der IP-Adresse des Benutzers, und leitet ihn zwecks Authentifizierung wieder an den IdP weiter. Das ist die Authentifizierungsanforderung.
3. Der Benutzer unterhält entweder eine aktive Browser-Sitzung mit dem IdP oder erstellt durch die Anmeldung beim Identity-Provider-System eine neue.
4. Die Authentifizierungsantwort des Identity Providers ist ein XML-Dokument, das den Benutzeramen oder die E-Mail-Adresse des Benutzers enthält. Der IdP signiert dieses Dokument mit einem X.509-Zertifikat und übergibt es an den SP.
5. Der SP, der den IdP bereits kennt und über den Fingerabdruck des Zertifikats verfügt, ruft die Authentifizierungsantwort ab und validiert sie anhand des Fingerabdrucks.
6. Die Identität des Benutzers wurde verifiziert, und ihm wird Zugang zum Application Store des Access Portals gewährt.



Was ändert sich durch das Access Portal bei der Authentifizierung?

Das Access Portal kann als Service Provider eingerichtet werden und – über die digitale Zertifikatsignatur des Identity Providers – als Zugangspunkt für Benutzer fungieren und Anmeldevorgänge initiieren, damit IT-Administratoren einen zentralen Zugang zu RDP- und SSH-Ressourcen im Intranet des Unternehmens bereitstellen können.

Für autorisierte Benutzer kann das Access Portal angepasst und als zentraler Anmeldedienst für Webanwendungen eingesetzt werden, die nicht im Intranet gehostet werden. Das Access Portal von WatchGuard bietet umfassende Unterstützung für verbreitete Identity Provider, um Unternehmen mehrstufige Authentifizierungslösungen an die Hand zu geben. Das Access Portal ist mit folgenden IdP kompatibel:

- Shibboleth
- OneLogin
- Okta

Gängige Software-Token, die in Verbindung mit dem Access Portal verwendet werden können, umfassen:

- SecureID
- Duo-Security-Token
- OneLogin-XX-Token
- Google Authenticator
- Okta-Mobilgeräte-Token

Die wichtigsten Firebox®-Anwendungsfälle

Web Single Sign-On (WSSO) für zugangsberechtigte Intranet-Benutzer

Um den Schutz auf Secure-Shell- oder Remote-Desktop-Server auszudehnen, kann das WatchGuard Access Portal für eine starke Authentifizierung konfiguriert werden. Dies gestattet eine mehrstufige Authentifizierung und Single-Sign-On-Workflows, die einen sicheren und bequemen Zugang zu einem Intranet-Verwaltungsserver gewährleisten.

Clientloser Zugang für Remote-Netzwerkadministratoren

Privilegierte Netzwerkadministratoren benötigen einen zentralen Referenzpunkt für den Zugriff auf Cloud-gehostete HTML5-Produktivitätssoftware wie O365, OneDrive, Box, usw. Das WatchGuard Access Portal bietet einen zentralen zugriffsberechtigten Kontozugang und IdP-initiiertes SSO für derartige Anwendungen. Mit SAML 2.0 lässt sich das Access Portal für einen zentralen Remote-Zugang über den IdP konfigurieren.

Über WatchGuard

WatchGuard® Technologies gehört zu den führenden Anbietern im Bereich Netzwerksicherheit. Mehr als 80.000 Unternehmen weltweit vertrauen auf die ausgeklügelten Schutzmechanismen auf Enterprise-Niveau, wobei dank der einfachen Handhabung insbesondere kleine bis mittlere sowie dezentral aufgestellte Unternehmen von WatchGuard profitieren. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält WatchGuard Niederlassungen in ganz Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter **WatchGuard.de**.

Deutschland, Österreich, Schweiz: +49 700 92229333 INTERNATIONALER VERTRIEB +1.206.613.0895 www.watchguard.de

Mit diesem Dokument werden keine ausdrücklichen oder implizierten Gewährleistungen gegeben. Alle hier aufgeführten technischen Daten können sich ändern. Informationen zu zukünftigen Produkten, Ausstattungsmerkmalen und Funktionen werden zu gegebener Zeit zur Verfügung gestellt. ©2017 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo und WatchGuard Dimension sind Marken bzw. eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle weiteren Markennamen sind das Eigentum ihrer jeweiligen Inhaber. Teilenr. WGCE67057_121917