WatchGuard Access Portal

Расширение защиты WatchGuard для критически важных активов в облаке

Что такое Access Portal?

Портал доступа, входящий в состав Total Security Suite (TSS) WatchGuard, представляет собой сервис, который позволяет реализовать централизованный доступ к облачным сервисам приложений и позволяет избегать дорогостоящих решений для аутентификации. Портал доступа включает в себя портал приложений HTML5, поддержку единого входа для интранет-служб RDP/SSH и поддержку SAML 2.0 для снижения административной нагрузки. Распространение облачных платформ и связанных с ними сервисов продолжает расти, как и контроль доступа к чувствительным активам в облаке.

Что такое SAML 2.0?

Язык разметки безопасности (SAML) является стандартом для регистрации пользователей в приложениях на основе их сеансов в другом контексте. Этот стандарт единого входа в систему (SSO) имеет значительные преимущества перед входом в систему с использованием имени пользователя/пароля:

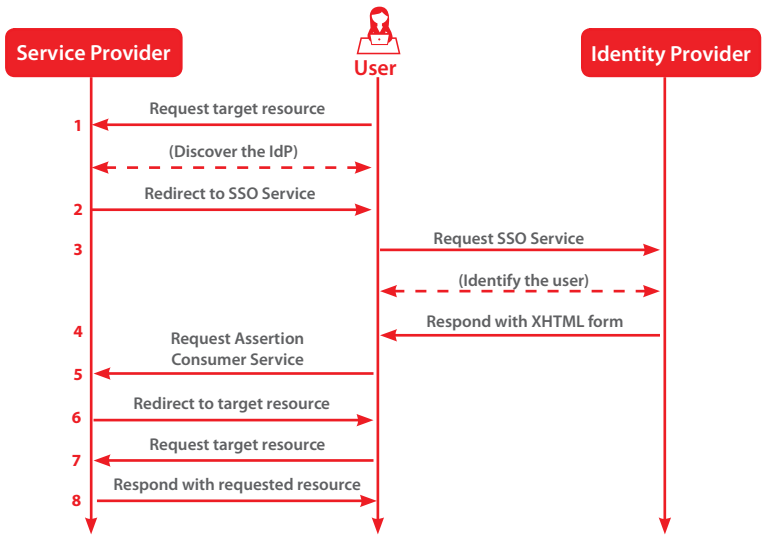
- Нет необходимости вводить учетные данные
- Не нужно запоминать и обновлять пароли
- Отсутствие слабых паролей

Большинство организаций знакомы с идентификацией пользователей, поскольку используют в своем домене Active Directory. Имеет смысл использовать эту информацию для регистрации пользователей в других приложениях, таких как веб-приложения, и одним из наиболее элегантных способов сделать это является использование SAML.

Как SSO работает с SAML 2.0?

SAML SSO работает, передавая данные пользователя из одного места (сервер аутентификации) к другому (поставщику услуг). Это делается путем обмена документами с цифровой подписью XML. В качестве примера — следующий сценарий: пользователь регистрируется в системе, которая действует как поставщик удостоверений (IdP). Пользователь хочет войти в удаленное приложение. Происходит следующее:

1. Пользователь обращается к удаленному приложению, используя ссылку в интрасети, закладку или что-то подобное, и приложение загружается.
2. Приложение идентифицирует пользователя (субдомен приложения, IP-адрес пользователя или аналогичный) и перенаправляет его обратно в IdP с запросом на аутентификацию.
3. Пользователь либо уже имеет существующий активный сеанс с IdP (например, в браузере), либо устанавливает его, войдя в IdP.
4. IdP создает ответ аутентификации через форму XML, содержащую имя пользователя или его адрес электронной почты, подписывает его с помощью сертификата X.509 и помещает эту информацию в SP.
5. SP, который уже знает IdP и имеет отпечаток сертификата, извлекает ответ аутентификации и проверяет его с помощью отпечатка сертификата.
6. Пользователь идентифицирован и ему предоставляется вход в хранилище приложений портала доступа.



Как Access Portal может изменить аутентификацию?

Портал доступа можно активировать как сервис SP, и, посредством цифровой подписи сертификатов с выбранным IdP, он может быть еще одной точкой доступа, чтобы инициировать логины для администраторов – для централизованного доступа к ресурсам RDP и SSH.

Для привилегированного пользователя портал доступа WatchGuard можно сместить и расширить в центральную службу для доступа к веб-приложениям, размещенным как снаружи, так и внутри интрасети компании. Служба портала WatchGuard полностью поддерживает популярные системы мультифакторной аутентификации – MFA.

Лучшие случаи использования Firebox®

WSSO в привилегированную интрасеть

Для обеспечения защиты серверов RDP, портал WatchGuard Access Portal может быть настроен для надежной проверки подлинности и включить многофакторную аутентификацию, а также включать SSO для удобного и безопасного доступа к ресурсам интрасети через RDP/SSH.

Бесконтактный доступ для удаленных сетевых администраторов

Для привилегированного сетевого администратора требуется единый централизованный доступ к облачным офисным продуктам, таким как O365, One-Drive, Box и т.д. Портал доступа WatchGuard предлагает доступ к привилегированным учетным записям, а также SSO с поддержкой IdP в одном сайте. С SAML 2.0 портал доступа можно настроить через провайдера IdP для централизованного удаленного доступа.

Про WatchGuard

WatchGuard – это почти миллион интегрированных многофункциональных систем управления угрозами по всему миру. Характерные «красные коробки» WatchGuard – это самые умные, быстрые и продвинутые устройства защиты в отрасли, в которых все механизмы сканирования работают с недоступной прочим вендорам производительностью. Штаб-квартира WatchGuard расположена в Сиэтле (США). Компания имеет офисы в Северной Америке, Европе, Азиатско-Тихоокеанском регионе и Латинской Америке.

Больше информации:

www.watchguard.com

www.watchguard.com/secplicity (блог об информационной безопасности)

Про БАКОТЕК

БАКОТЕК® – международная группа компаний, которая занимает лидирующие позиции в сфере фокусной Value Added IT-дистрибуции и поставляет решения ведущих мировых IT-производителей. Позиционируя себя как True Value Added IT-дистрибьютор, БАКОТЕК предоставляет профессиональную до- и пост-продажную, маркетинговую, техническую поддержку для партнеров и конечных заказчиков. Территориально группа компаний работает в 26 странах на рынках Центральной и Восточной Европы, Балкан, Балтии, Кавказа, Центральной Азии с офисами в Праге, Кракове, Риге, Минске, Киеве, Баку и Нур-Султане.

Группа компаний БАКОТЕК является официальным дистрибьютором решений WatchGuard в Украине, странах Балтии, Центральной Азии и СНГ.

www.bakotech.com
watchguard@bakotech.com