MobileIron

DATA SHEET

Sécuriser les données dynamiques des applications et simplifier l'authentification

AppConnect, Tunnel et proxy Kerberos

L'informatique mobile a modifié les habitudes de travail des entreprises : les employés peuvent travailler partout et à tout moment grâce à leurs appareils mobiles. Dans un environnement où les méthodes de travail sont de plus en plus nomades, les entreprises doivent sécuriser les échanges entre leurs serveurs et les applications mobiles.

Pour obtenir ce genre de connexion, on utilise couramment les réseaux privés virtuels (VPN). Dans le cas d'un VPN classique, le trafic du réseau passe en intégralité par une connexion sécurisée créée entre l'utilisateur de l'appareil et le serveur VPN. Cette solution convenait parfaitement à l'ère du PC, mais nous sommes depuis passés à l'ère du mobile : un VPN classique lié à un appareil est insuffisant pour garantir la sécurité des données mobiles.

Contrairement aux PC, les appareils mobiles ne sont pas limités à quelques applications professionnelles, mais peuvent utiliser des centaines d'applications personnelles et professionnelles. Certaines applications sont dédiées à des communications professionnelles, d'autres à des communications personnelles. Malheureusement, les applications ne font pas toutes l'objet d'un contrôle : certaines peuvent être mal intentionnées afin, par exemple, d'accéder à des informations protégées par le pare-feu d'une entreprise.

Pour les appareils mobiles

Chez MobileIron, nous savons que ces anciennes méthodes ne sont plus adaptées. C'est pourquoi, nous souhaitions créer une nouvelle solution qui serait conforme à notre philosophie en matière de sécurité informatique. Notre solution repose sur deux concepts majeurs :

- Séparation des données : autoriser uniquement les applications professionnelles approuvées par l'IT.
- Protection de l'accès : l'accès au réseau est protégé en fonction de deux paramètres, l'identité de l'utilisateur et la conformité de l'appareil.

En autorisant uniquement les applications de confiance à accéder aux réseaux de l'entreprise, la séparation des données offre plusieurs avantages : elle protège les données professionnelles, garantit la confidentialité des données personnelles des utilisateurs sur le réseau d'entreprise et permet aux applications d'accéder rapidement et facilement aux données en leur accordant des certificats et des paramètres de configuration VPN en arrière-plan.

Défi
Sécuriser les data-in-motion sans nuire à l'expérience utilisateur ni fragiliser la sécurité du réseau.

Solution
AppConnect, Tunnel et proxy Kerberos

Atouts

- Accès dynamique, fiable et intelligent
- Protège le réseau d'entreprise
- Facile à installer
- Simple à utiliser
- Respecte la vie privée des utilisateurs

Séparation des données
Autorise uniquement les applications professionnelles approuvées

Protection de l'accès
L'accès aux applications professionnelles n'est accordé qu'après vérification de l'identité de l'utilisateur et du statut de l'appareil

La protection de l'accès consiste à vérifier à la fois l'identité de l'utilisateur et le statut de l'appareil, afin de fournir un accès sécurisé et intelligent à l'application, mais aussi aux données dynamiques (data-in-motion). Le statut de l'appareil est très important, car il donne une indication sur sa fiabilité. En se basant sur cette caractéristique, les entreprises peuvent s'assurer que les appareils qui ont été jailbreakés ou sur lesquels les données ne sont pas protégées ne pourront pas se connecter à leur réseau. Il arrive régulièrement, surtout dans le cadre des programmes BYOD, que les appareils ne soient pas toujours conformes, ce qui rend le contrôle d'accès dynamique indispensable.

MobileIron a créé deux produits qui se complètent pour mieux refléter notre philosophie et fournir un accès sécurisé, transparent et intelligent aux data-in-motion : AppConnect et Tunnel. En les associant au proxy Kerberos, qui vise à simplifier l'identification des utilisateurs via l'authentification unique (Single Sign-On ou SSO), les entreprises disposent désormais d'une gamme complète d'outils pour sécuriser l'informatique mobile, sans nuire à l'expérience utilisateur.

AppConnect

Sorti en décembre 2012, AppConnect était le premier VPN dédié aux applications sur un appareil mobile. Son rôle principal est de compartimenter chaque application. Il permet de sécuriser à la fois les données présentes sur l'appareil et le circuit de communication, afin de protéger les ressources de l'entreprise derrière le pare-feu. Pour cela, AppConnect contrôle les accès en vérifiant l'identité de l'utilisateur et le statut de l'appareil.

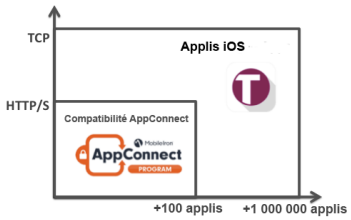
La surveillance continue de ces deux paramètres permet de prendre des mesures au niveau de l'application et du circuit de communication. Si l'appareil vient à être jailbreaké, l'application et le circuit de communication peuvent être désactivés. Le conteneur AppConnect dispose également de fonctionnalités performantes de prévention de perte de données, telles que le blocage de la fonction « copier-coller » et la limitation du partage de données entre les applications.

Tunnel

AppConnect a été un précurseur de la sécurisation des data-in-motion pour les applications compatibles. Tunnel reste dans cette continuité en offrant cette protection à des millions d'applications supplémentaires disponibles dans l'App Store. Désormais, la majorité des applications fonctionnant sous iOS peuvent instaurer un VPN par application avec Tunnel pour protéger les ressources de l'entreprise.

Tunnel est un VPN par application conçu sur les interfaces de programmation (API) d'iOS qui se connecte directement à MobileIron Sentry et repose sur les trafics HTTP et TCP. Il permet aux entreprises d'autoriser certaines applications, notamment des applications développées en interne ou provenant de l'App Store, à accéder aux ressources de l'entreprise protégées par un pare-feu. Tunnel bloque les applications non autorisées et les applications personnelles, améliorant ainsi la sécurité et la protection de la vie privée de l'utilisateur. À l'instar d'AppConnect, Tunnel autorise les communications uniquement si l'utilisateur et l'appareil sont conformes. Si l'un des deux ne l'est pas, alors la connexion peut être interrompue.

AppConnect et Tunnel
Solutions complémentaires pour protéger les data-in-motion. Désormais, des millions d'applications supplémentaires peuvent être protégées grâce à Tunnel.



Safari devient un navigateur d'entreprise
Grâce à Tunnel et au proxy Kerberos, les utilisateurs peuvent ouvrir les liens de leur messagerie directement dans Safari. La sécurité et l'authentification sont gérées en arrière-plan.

Proxy Kerberos : authentification unique

Le nouveau proxy Kerberos de MobileIron Sentry vise à faciliter l'authentification des utilisateurs tout en garantissant le même niveau de sécurité.

Auparavant, accéder aux données protégées d'une entreprise impliquait de passer par de nombreuses étapes, telles que le démarrage d'un VPN, et de saisir un code d'accès complexe. MobileIron souhaitait alléger ce processus et le rendre plus simple, plus sécurisé et transparent. Idéalement, les processus de communication et d'authentification s'exécuteraient instantanément en arrière-plan.

Grâce à Sentry et à son proxy Kerberos, cela est désormais possible. Ce proxy autorise les appareils iOS 7 non enregistrés dans un réseau de confiance à se connecter via l'authentification unique. Grâce à l'association de Tunnel et du proxy Kerberos, les liens de la messagerie native s'ouvrent dans Safari, un tunnel est automatiquement créé et l'utilisateur est authentifié, le tout de manière transparente. Désormais, vous pouvez utiliser Safari pour accéder aux contenus de votre entreprise protégés par l'authentification unique.

Grâce à AppConnect, Tunnel et au proxy Kerberos développés par MobileIron, les entreprises disposent de toute une gamme de produits pour sécuriser et simplifier le travail de leurs utilisateurs.

MAKING MOBILE FIRST

MobileIron

415 East Middlefield Road
Mountain View, CA 94043 USA
Tél. +1.650.919.8100

Fax +1.650.919.8006
info@mobileiron.com

