MOBILITYGUARD

DESCRIPCIÓN DE LA SOLUCION Y CARACTERITICAS GENERALES

El presente documento describe de manera general los beneficios de la solución desarrollada por MobilityGuard, sus características tanto técnicas como comerciales. También se adjunta información de comparativos frente a soluciones del mercado.

Esta descripción se hace bajo tres aspectos:

1. Que es OneGate? Beneficios
2. Descripción Técnica y su Justificación
3. Comparativo frente a soluciones similares en el mercado Colombiano.
4. Características Comerciales

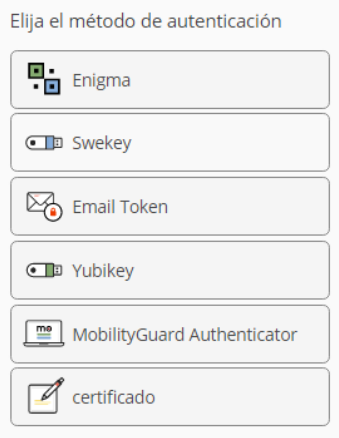
1. ¿QUÉ ES ONEGATE? BENEFICIOS

MG-OneGate es una solución que permite exponer a través de un portal unificado las aplicaciones y recursos de su organización, elevando los niveles de seguridad, e implementando de forma ágil controles de acceso basados en políticas y marcos regulatorios, además facilita el despliegue de mecanismos solidos de autenticación y cifrado fuerte en las comunicaciones, tanto para usuarios internos o externos de la organización, todo esto enfocado en una adecuada gestión del ciclo de vida del usuario.

A continuación, se detalla cada uno de sus principales beneficios:

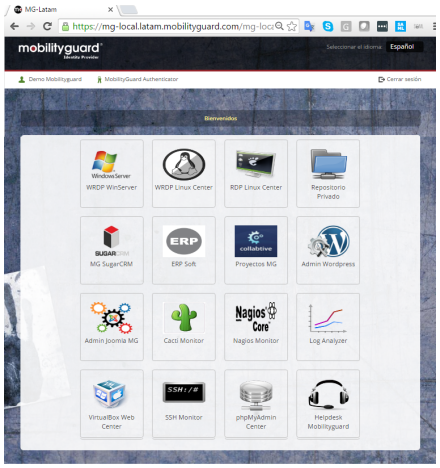
Autenticación sólida para la exposición de recursos o aplicaciones a usuarios internos o externos de la organización.

OneGate presenta diversos mecanismos de autenticación (Más de 18 métodos), entre los que se destacan varios mecanismos (2-factor), de fácil implementación, despliegue y puesta en marcha.



Presentación de aplicativos o recursos mediante portal unificado.

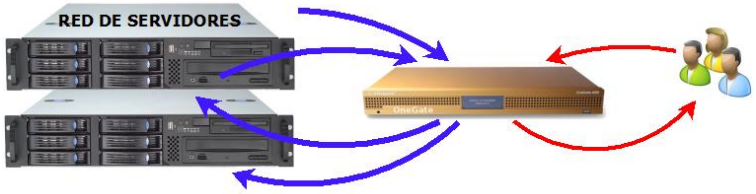
A través de un portal unificado es posible presentar todas las aplicaciones que son requeridas por los usuarios para sus actividades diarias facilitando el acceso a las mismas de forma ágil, teniendo un único punto de acceso para ser controlado y vigilado.



Enmascaramiento de aplicaciones o recursos a nivel de red, puertos y dominio

OneGate es un proxy reverso con funcionalidades extendidas, de esta forma los usuarios hacen uso de las aplicaciones interactuando únicamente con OneGate ya que es éste quien presenta las aplicaciones como si fuese el servidor de aplicaciones final.

De esta manera el usuario nunca accede directamente al servidor final, desconociendo características de red o dominio reales del recurso, lo que a nivel de seguridad reduce riesgos de recolección de información, escaneo de puertos y escaneo de vulnerabilidades.



Presentación en HTTPS de las aplicaciones.

Todas las aplicaciones que son accedidas por los usuarios a través de OneGate son protegidas mediante cifrado SSL/TLS proporcionado por OneGate.

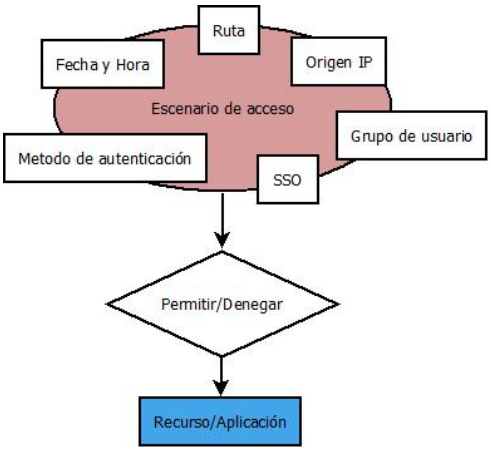
De esta manera se mejora la administración de certificados SSL/TLS ya que solo se requiere del certificado instalado en OneGate, siendo este el único punto de gestión del certificado y única inversión por compra de certificado.

Comunicación cifrada ajustable.

El flujo de información sensible que se origina en el usuario y llega a OneGate se cifra mediante TLS 1.2 y a su la vez dicho cifrado puede ser ajustado a diferentes niveles. (256, 512, 1024, 2048).

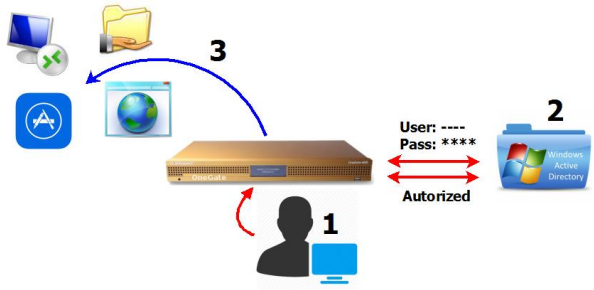
Control de acceso de acuerdo a perfiles y escenarios.

OneGate permite definir políticas flexibles de acceso a aplicaciones de acuerdo a perfiles y escenarios donde los mismos pueden estar determinados por: Grupos de usuario, mecanismo de autenticación usado, dirección de red origen de la petición, fecha y hora del acceso entre otras.



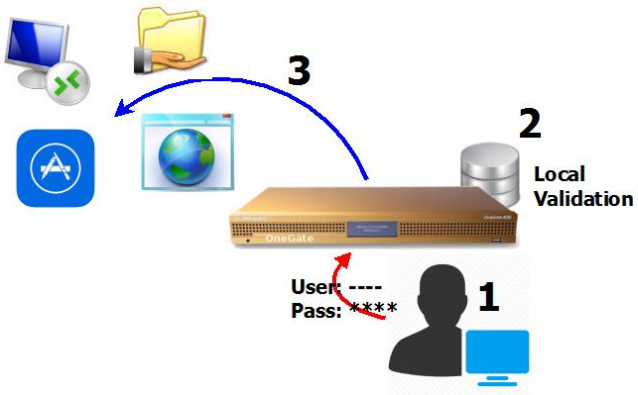
Integración con servicios de directorio

OneGate se integra fácilmente con servicios de directorio (LDAP, A/D, E-Directory), de esta forma se aprovecha la gestión de usuarios y grupos efectuada en dichos servicios de directorio, dado que la autenticación en OneGate y la presentación de aplicaciones a usuarios autenticados, se hace a partir de los grupos y usuarios existentes en los servicios de directorio mencionados.



Repositorio de usuarios interno

OneGate también cuenta con una base de datos interna para la creación de usuarios locales, esto facilita la presentación de aplicaciones y/o recursos a usuarios externos a la organización, sin que implique creación de los mismos en el servicio de directorio de la organización, sino de forma aislada y controlada dentro de OneGate.



Exposición segura de aplicativos a usuarios externos sin la creación, habilitación o administración de accesos VPN, evitando el acceso a la red local por parte de terceros.

OneGate basa enfoca su arquitectura bajo el modelo de cliente inseguro, de manera tal que sea un usuario interno o externo a la organización podrá hacer uso de los servicios sin necesidad de tener conexión directa a nivel de red y puertos, por ende, el uso y administración de VPNs tradicionales deja de ser exclusivamente necesario.

Esta característica es beneficiosa a nivel de seguridad dado que la naturaleza de las VPNs tradicionales no abarca aspectos importantes de la seguridad como la autenticación sólida, control de acceso basado en grupos o roles y mucho menos el enmascaramiento de aplicaciones o recursos a nivel de red, puertos y dominio.

Completo Single Sign On para aplicaciones Web y Escritorio remoto (RDP).

Luego de una autenticación frente al portal OneGate, el usuario podrá acceder a los aplicativos finales con tan solo dar click en cada uno de ellos sin que esto implique un nuevo ingreso de credenciales para la autenticación en dichas aplicaciones.

Esto facilita la asimilación y recepción de mecanismos de autenticación solida por parte de los usuarios ya que el proceso de autenticación (2-factor), se ejecuta una sola vez y no por cada recurso o aplicación.

Esto evita que el usuario tenga que digitar múltiples contraseñas en repetidas ocasiones reduciendo la posibilidad de malas prácticas como: contraseñas débiles, contraseñas expuestas, almacenamiento de contraseñas en el navegador.

Facilita, apoya o contribuye al despliegue de Sistemas de Gestión de Seguridad de la Información y cumplimiento de la normatividad o marcos referencia vigente.

En Colombia se han hecho avances respecto a la reglamentación o regulaciones vigentes que aplican sobre la los datos y sistemas informáticos, adicionalmente a nivel mundial existen marcos de referencia como ISO27001, Cobit entre otros aplicables o con relación al contexto tecnológico. Adicionalmente la Ley Estatutaria de Protección de Datos, 1581 de 2012 y la Ley 1273 de 2009, contemplan sanciones hasta por 2.000 salarios mínimos mensuales legales vigentes por violación de datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes; inclusive penas de prisión desde 48 a 96 meses. Todo esto puede resultar muy general o de difícil cumplimiento, adopción o ejecución, es allí donde OneGate se destaca como una solución útil, potente y bien adecuada para poder poner en práctica, dar cumplimiento de forma fácil de acuerdo a lo que plantean el contexto regulatorio y de buenas prácticas en el ámbito de seguridad de la información.

Restablecimiento de contraseña para usuarios en el repositorio local de la solución.

Mediante un enlace de restitución de contraseñas enviado al correo registrado para cada usuario en la solución, los usuarios estarán en la posibilidad de restituir su contraseña en caso de requerirlo.

Restablecimiento de contraseña para usuarios miembros de un servicio de directorio (Requiere LDAPS).

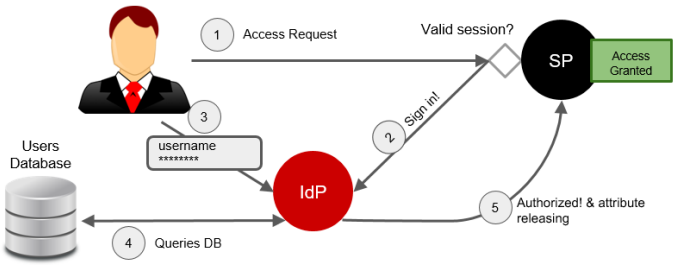
OneGate puede establecer relaciones de confianza con el servicio de directorio, de forma tal que pueda servir como intermediario con los usuarios finales para la restitución de contraseñas en el servicio de directorio. Al igual que con los usuarios locales OneGate envía un enlace de restitución de contraseñas al correo registrado en el servicio de directorio.

Registro de eventos de autenticación, acceso a aplicaciones o recursos y tiempos de actividad.

Siendo OneGate el único punto de entrada a las aplicaciones, facilita las tareas de trazabilidad de eventos o análisis forense dado que se tiene un punto inicial de referencia para acotar búsquedas y reducir el universo de posibilidades. Aunque presenta algunas variables importantes con respecto a la trazabilidad de usuarios, tiene la capacidad de enviar toda la información a un servidor de logs para su posterior análisis.

Federación de identidades como Proveedor de Identidad y como Proveedor de Servicios mediante SAML2.0

La federación de identidades permite a usuarios acceder a diferentes servicios en la nube efectuando una única autenticación en un Proveedor de Identidad (IdP), de esta forma la autenticación se centraliza en un único punto de control y por otro lado sin importar los servicios a los que se accede en diferentes proveedores de servicio (SP), no se requiere nuevamente el ingreso de contraseñas puesto que los proveedores validan con el proveedor de Identidad la autorización para la prestación del servicio. Todo a través de un protocolo estándar (SAML 2.0), para evitar que la organización quede sujeta a la utilización de una marca del mercado en particular.



Exposición o despliegue de variedad de aplicaciones y/o recursos:

A través de la solución OneGate es posible presentar diferentes tipos de servicios o recursos informáticos como:

- Aplicaciones Web (Con base en estándares).
- Escritorios remotos RDP mediante navegador web (HTML5).
- Escritorios remotos RDP mediante cliente RDP Windows.
- Carpetas compartidas SMB mediante navegador web.
- Acceso a conexiones SSH mediante túneles JAVA

Bajo el esquema de federación, OneGate permite gestionar la conexión a redes wifi para sus usuarios y usuarios visitantes estableciendo reglas de acceso a éstos a través de EDUROAM. Esta características está dirigida principalmente al área de las áreas de Investigación con foco en Colegios y Universidades. Bajo esta módulo no es necesario administrar usuarios (Estudiantes o Docentes), que provengan de Instituciones o Universidades que estén afiliadas a EDUROAM en el mundo.

Para más información de EDUROAM, visite: https://www.youtube.com/watch?v=1HQbU4KELtk

OneGate en Resumen: MG-OneGate es una aplicación integral que permite la adecuada identificación de los usuarios (autenticación doble factor) y gestión de acceso unificado a los aplicativos a través de la fácil creación de reglas de acceso orientada a grupos o roles (ACL – Access Control Lists), todo a través de un canal cifrado (un sólo certificado SSL TLS 1,2; para todos los recursos) y encapsulamiento. El acceso a los recursos se hace a través de un proxy inverso que permite ocultar las rutas o URL de los recursos.

MG-OneGate, entrega las aplicaciones de forma segura a los usuarios sin que ellos tengan que saber su origen; todo a través de direccionamiento de todos los recursos por el puerto 443 (SSL). Permite una auditoria más profunda de los recursos, controlando no solo la conexión de los recursos, sino además los usuarios que los acceden. MG-OneGate permite la integración del acceso de todos los recursos a través de una única credencial de usuario (SSO), de esta manera facilita el uso, la recuperación y la gestión de las credenciales de los usuarios, minimizando la carga de mesa de ayuda hasta en un 80%.

Con todas las características de gestión de acceso que MG-OneGate posee permite de manera confiable exponer los servicios a terceros a través de SP SAML (Proveedor de Servicios) y acceder a servicios en la nube sin necesidad de entregar la información personal de los usuarios configurando IdP SAML (Proveedor de Identidad). También, permite gestionar la conexión a redes wifi para sus usuarios y usuarios visitantes estableciendo reglas de acceso a éstos a través de EDUROAM.

2. DESCRIPCION TECNICA Y SU JUSTIFICACION

Caracteríticas Técnicas	Justificación
Proporciona soporte a cifrado mediante protocolo TLS 1,2 a través de un certificado multidominio de tipo Wildcard. Tiene la capacidad de cifrar comunicaciones hasta 2048 bits. Es una solución integral a través de un único appliance, no invasiva, sin requerimiento de plugins ni desarrollos que brinda esta capa de seguridad.	Le permite a la organización reducir costos, a la vez que mejora la gestión y administración causada por la adquisición de certificados individuales por aplicación y evita la administración y gestion individual de los mismos, Mediante un único certificado wildcard que eleva la seguridad para uno o varias aplicaciones a la vez.
La solución contiene una base de datos cifrada de usuarios incorporada sin limite de registros. Hacer parte integral de la solución y no se compone de elementos y/o módulos externos.	Facilita la administración de usuarios temporales y genera ahorros de adminsitración frente a los usuarios creados en el LDAP con el que cuente la entidad.
El S.S.O. de la solución tiene la capacidad del Self-Learning S.S.O., es decir, que permite aprender credenciales de forma automática para su posterior uso S.S.O. Adicionalmente, el S.S.O. brinda acceso autenticado a las aplicaciones finales y no sólo a nivel de red.	El Single Sign On permite utilizar una sóla autenticación sólida (Doble Factor) y brinda acceso a diferentes aplicativos de una red sin tener que realizar nuevamente inicio de sesión por aplicativo. Evita los riesgos generados por la administración por parte del usuario de un elevado número de credenciales. Esta es una de las brechas grandes en lo relacionado a un S.G.S.I. Es importante el self-lerning ya que perminte hacer S.S.O. aún si el usuario tiene diferentes credenciales en los aplicativos a los que accede. Así se pueden proteger credencieles de usuarios para evitar su suplantación.
Permite el acceso cifrado durante la comunicación a recursos web y cliente-servidor (Aplican restricciones), alcanzables a través de un único portal web. Tiene la capacidad de generar túneles dinámicos para exponer aplicativos cliente-servidor a través de la web.	El uso de un único portal de acceso con comunicación cifrada, permite a la entidad presentar servicios a los usuarios de forma fácil, evitanto el conocimiento y gestión del usuario de multiples url´s y dominios para acceder a los diferenteas aplicativos. Este portal debe ser web, dado que así facilita el acceso desde cualquier dispositivo y en cualquer momento si así se define en las políticas de seguidad de la organización o entidad. El uso de protocolos es fundamental para evitar la dependencia de la entidad frente a marcas o empresas. Así mismo, esta solución debe ser independiente a los aplicativos y/o soluciones que se quieren proteger por el mismo hecho que la seguridad debe ser independiente a ellas mismas. De igual manera, la solución de seguridad no debe manejar módulos independientes que se deban integrar para evitar sobre-costos y brechas de seguridad en integraciones entre los mismos.
Soporta los siguientes protocolos: TCP/IP, UDP/IP, HTTP, HTTPS, FTP, FTPS, SCP, SMB, Cliente-Servidor, RDP(Cliente HTML5), SAML 2.0, SSL/TLS, XML, WEB-Services, PKI, RADIUS, OPEN VPN, HTML, HTML5, OCSP, LDAP, LDAPS, NTLMv1, BGC-Tickets, OATH TOTP. Todo de forma integral, sin módulos o componentes externos.	El cumplimiento de estándares evita que la seguridad quede en manos del fabricante del aplicativo repositorio. La seguridad no debe limitarse a las funciones o caracteristicas seguras que pueda incorporar una aplicación cuyo proposito final es otro. Es necesaria la implementación de seguridad a través de una solución diseñada para ese fin que permita la aplicación de controles y políticas de seguridad.
La herramienta brinda soporte a auntenticaición fuerte o doble factor a través de métodos como:Soft token, Hard token, SMS token, Email token, Certificado PKI, Certificado Cliente, Kerberos, REST Web Service y autenticación Radius tales como Servidor RADIUS PAP, CHAP, PEAP/MSCHAPv2 Cliente RADIUS PAP, CHAP. Todo de forma integral sin módulos o componentes externos.	La autenticación fuerte (Doble Factor), es un requerimiento de seguridad para acceder a información crítica de las organizaciones y/o entidades, más aún cuando esta información es de personas y/o de su entorno. La ley 1273 de 2009 lo contempla en el artículo 269F acerca de la Violación de datos personales. De igual manera La Ley Estatutaria 1581 de 2012 Establece en sus principios rectores responsabilidades en el tratamiento de la información con medidas técnicas que otorguen seguridad evitando adulteración perdida o acceso no autorizado, así mismo en el Artículo 23. Establece Sanciones y Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción.
Permite la recuperación automática de contraseñas a través de email, dirigidos al usuario final.	Impacto directo positivo frente a los costos de mesa de ayuda y cumplimiento de las leyes anteriormente mencionadas. Las contraseñas son gestionadas directamente por el usuario y así se le garantiza la custodia de sus credenciales. Por esto, es importante contar con esta capa de seguridad sobre los aplicativos o repositorios de información.
Cumple con estándares ISO 27000 Series. Con foco en Control de Acceso, COBIT, SOGP.	Se debe ajustar a marcos de referencia para efectos de certificaciones y validaciones en cumplimientos legales.
Se integra sin desarrollos adicionales y tiene la capacidad de integrarse a múltiples servicios de directorio simultáneamente (Active Directory, eDirectory, LDAP en General. Además no es invasiva.	La integración con diferentes tipos de servicios de directorio garantiza la no dependencia a marcas y por ende a la independencia frente a tecnologias. Además de hacerlo de forma simultánea que permite colocar esta capa de seguridad a entornos ya existentes generando ahorros sustanciales.
Permite el redireccionamiento de todo el tráfico a través de un único puerto 443 (SSL).	Evita la exposición de multiples puertos hacia el usuario, puesto que todo el acceso a los servicios se hace a través de un unico puerto que garantiza el cifrado en la comunicación.
Permite realizar auditoría a través del envío de la información respectiva (Origen IP, Método de Autenticación utilizado, Fecha, Hora, recurso accedido, ID de sesión y Usuario) a un servidor Syslog.	Al contar con un único punto de acceso, toda la información de los usuarios podrá ser monitoreada y permite conocer detalles importantes sobre este control. Precisamente es aquí donde las leyes hacen enfasis para entender cómo se protegen los diferentes aplicativos.
Permite acceder a todos los recursos a través de subdominios de un único dominio base.	Facilita la implementación del enmascaramiento de url´s que evita los escaneos de puertos o de la red o conocer los detalles de direcciones IP y Servidores. Es una forma de incremetar la seguridad a un nivel mayor.
Permite la personalización de reglas de acceso a recursos web y cliente-servidor con base en roles de usuario a través de: métodos de autenticación, lugar de acceso, Dirección IP, hora, día, nivel de cifrado, etc. Este servicio está ntegrado y no pertenence a un módulo o componente externo.	Permitir la aplicación personalizada de controles y politicas facilita el cumplimiento de los lineamientos definidos en el S.G.S.I y garantiza el cumplimento legal a través de la implementación de mecanismos técnicos que eviten la pérdida o consulta de información por usuarios no autorizados. Es aquí donde cobra importancia la utlización de una solución de seguridad diseñada para tal fin.
Cuenta con alta disponibilidad con balanceo de cargas para atender 24/7, cluster que garantiza el servicio a pesar de fallos.	Facilita la implementación de planes de continuidad del negocio (BCP) y planes de recuperación de desastres (DRP)
Cuenta con alta disponibilidad con balanceo de cargas y cluster de modo activo/activo y activo/pasivo.	Garantiza la diponibilidad del servicio a la vez que se hace uso apropiado del hardware o software proporcionado por la solución. Aumenta la productividad y la disponiblidad de los servicios expuestos siempre manteniendo las políticas de acceso.
Cuenta con disponibilidad en formatos: VMWare, XEN, Hyper-V 2008-2012, Virtual Box y KVM.	La disponibilidad de la solución como appliance virtual facilida el aporvisionamiento y desaprovicionamiento de recursos de acuerdo al uso y demanda, a la vez que facilita la recuperación de la solución frente a desastres.
Es compatible con PKI para incorporar sistemas de Firmado digital como CA (Autoridad de Certificación) y CCP (Proveedores de Certificados Cliente)	Permite el despliegue de mecanismos de autenticación basados en certificado o firma digital. Esto garantiza que en el momento que se usen métodos de autenticación de mayor nivel de seguridad , el sistema lo pueda soportar. Visión de Futuro en Seguridad.
Brinda validación a servidores OCSP.	Permite la validación de autenticidad y validez de los certificados digitales constantemente. Esto evita que si un certificado no es válido, inmediatamente se generan los avisos de seguridad pertinentes.
Es una solución de tipo appliance que cuenta sistema operativo integrado y con interfaz de administración gráfica apra elc aso de Hardware. También tiene versión como Virtual Appliance.	Facilita la administración de la solución a traves de interfaz grafica ajsutable a la imagen corporativa deseada.

MobilityGuard AB
Lexbyvägen 22, 433 31 Partille, Suecia. Phone: +46 31 760 67 70
Carrera 22 Norte # 6a N – 24 Piso 4. Cali - Colombia. Tel 57 2 485 08 48
Jul - 2016