



Protegiendo Aplicaciones Legacy Host con Seguridad Moderna

CONTENTS

Perspectivas Modernas a la Seguridad	1
Aplicaciones Legacy Host Sin Seguridad	2
Seguridad Legacy Host de Primera Generación: SSL Directo-a-Host	2
Seguridad Legacy Host de Próxima Generación: Una arquitectura de múltiples capas	2
Beneficios de la Infraestructura de Seguridad de Attachmate	4
Amplia Compatibilidad de Plataforma	5
Seguridad no Intrusiva en Múltiples Capas para Aplicaciones Legacy Host	5
Acerca de Attachmate	6

Protegiendo Aplicaciones Legacy Host con Seguridad Moderna

Las empresas actuales, bajo la presión de garantizar la privacidad de la información y salvaguardar datos confidenciales, han creado sofisticadas infraestructuras IT de seguridad. Han implementado una estrategia de “defensa a profundidad”, poniendo múltiples capas de protección. Desafortunadamente, la defensa de los sistemas donde están almacenados los datos más críticos a menudo falla debido a métodos de seguridad anticuados e insuficientes.

Sin embargo existe una manera de llevar a estos host legacy cruciales dentro de una arquitectura moderna de seguridad. Este informe técnico presenta la evolución en la protección de aplicaciones legacy host y explica las ventajas de un enfoque actual para defender las aplicaciones de terminal.

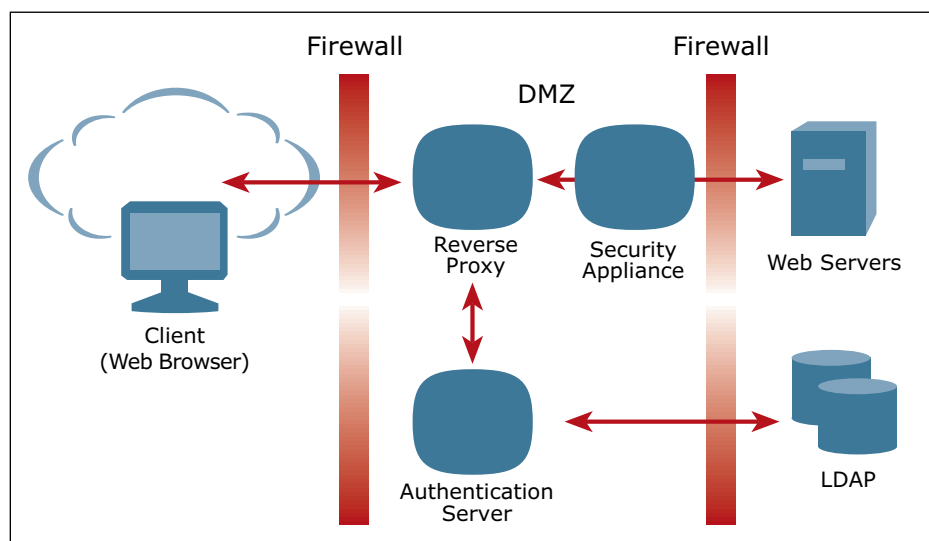
Perspectivas Modernas a la Seguridad

El enfoque moderno para la seguridad de la red se conforma de múltiples capas, por tanto implementan el principal aspecto de la seguridad de tipo “defensa a profundidad”. La empresa moderna emplea varias herramientas para defenderse contra diversos tipos de amenazas.

Múltiples medidas de seguridad

Esta arquitectura moderna en múltiples capas incorpora varias medidas de seguridad:

- **Encriptación.** Los datos son cifrados cuando pasan a través de una red no segura fuera del perímetro.
- **Manejo centralizado de identidades.** Un depósito LDAP empresarial maneja la información de identidad de todos los usuarios.
- **Control centralizado de acceso.** Se aplican directivas de autenticación y autorización en el perímetro para todo el tráfico entre clientes y servidores.
- **Auditoría centralizada.** El acceso a los recursos de la red es monitoreado de forma centralizada en el punto de control de acceso.
- **Monitoreo centralizado de amenazas.** El tráfico de entrada y salida es escaneado en el perímetro utilizando detección de intrusiones, inspección de contenido y otros dispositivos de seguridad para monitorear en busca de posibles ataques o fugas de información confidencial.



Modern security architecture uses defense in depth, putting in different layers, including reverse proxy, authentication, and authorization in the DMZ; network policies enforced with the security appliance (running content inspection, intrusion detection, etc.); and a secure enclave for backend servers.

Manejo centralizado de la seguridad

Tener varias medidas de seguridad es importante, pero es igual de importante cómo son manejadas estas medidas de seguridad. Una empresa descentralizada puede tener diferentes aplicaciones y diferentes servidores que son controlados por diferentes aplicaciones críticas. Puede ser un reto para un grupo central de seguridad el monitorear y aplicar las prácticas de seguridad que correspondan a cada uno de los nodos backend del servidor.

La arquitectura moderna de seguridad descrita arriba ofrece manejo centralizado de la seguridad. Todo el tráfico de red que pasa entre los clientes y los servidores backend debe pasar a través de una DMZ que es controlada por el personal central de seguridad. Esto crea un punto central de control para la asignación, monitoreo y aplicación de las directivas de seguridad de la empresa, independientemente de si las prácticas de seguridad están siendo aplicadas individualmente en cada nodo backend.

Aplicaciones Legacy Host Sin Seguridad

El acceso a aplicaciones legacy host tradicionalmente ha sido por medio de la utilización de puertos desprotegidos, como son Telnet y TPCA sobre el puerto 23 o INT1 y TPO sobre el puerto 102. Esta práctica presenta varios retos y riesgos de seguridad:

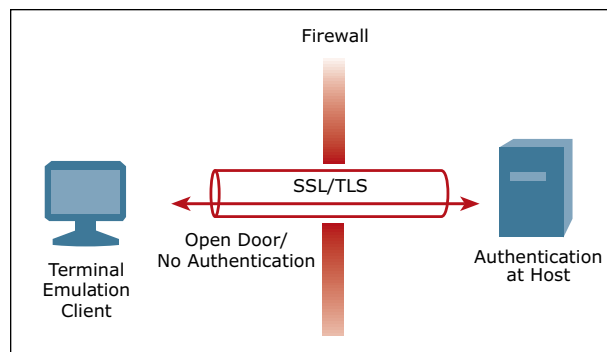
- **No existe confidencialidad de la información o contraseñas.** Sin la encriptación, los datos y contraseñas están expuestos.
- **Autenticación débil.** Muchos hosts están limitados a contraseñas de ocho caracteres sin hacer distinción de mayúsculas.
- **Autenticación descentralizada.** La autenticación basada en host es a menudo difícil de enlazar a LDAP, y usualmente esta desconectada de los sistemas de manejo de identidades utilizados en el resto de la empresa.
- **Control descentralizado de acceso.** El control de acceso solo ocurre en el host, así que no hay un control centralizado sobre el acceso a los recursos empresariales.
- **Auditoría descentralizada.** El acceso a los hosts es monitoreado solo por los mismos hosts.

Seguridad Legacy Host de Primera Generación: SSL Directo-a-Host

Las arquitecturas de seguridad legacy host de primera generación utilizan conexiones SSL directa del cliente al host. Esto proporciona una ventaja clave—los datos y las contraseñas están encriptados. Sin embargo, el túnel encriptado del cliente al host tiene el desafortunado efecto colateral de contrarrestar otras medidas de seguridad al dificultar el monitoreo del tráfico de red o aplicar cualquier clase de control de acceso en la DMZ.

Algunas de las limitaciones de la arquitectura SSL directo-a-host incluyen:

- **Autenticación descentralizada y débil.** La autenticación es todavía manejada en su totalidad por el host en la mayoría de las implementaciones SSL, así que muchos hosts están protegidos solo por contraseñas de ocho caracteres sin distinción de



First-generation host security provides SSL direct-to-host encryption, but there is no authentication until the connection has reached the host, giving intruders safe passage all the way to the host login screen.

mayúsculas. La autenticación host usualmente está separada de los sistemas de manejo de identidades utilizados en el resto de la empresa.

- **Control descentralizado de acceso.** El control de acceso solo ocurre en el host, por lo cual no existe un control centralizado sobre el acceso a los recursos de la empresa.
- **El tráfico SSL no autenticado pasa directamente al host.** El túnel SSL encriptado imposibilita monitorear la conexión en la DMZ y proporciona a los intrusos de un pasaje seguro hasta la pantalla de inicio de sesión del host. El personal central de seguridad tiene que dejar que pase el tráfico a través de la DMZ sin saber quién es el cliente, o qué clase de tráfico es, debido a que el tráfico está encriptado.
- **Auditoría descentralizada.** El acceso a los hosts solo es monitoreado por los hosts mismos.
- **Sin monitoreo centralizado de amenazas en el perímetro.** El tráfico entrante y saliente no puede ser escaneado con la inspección de contenido u otros dispositivos de seguridad porque el contenido está encriptado.
- **Control descentralizado de la seguridad.** La autenticación, el control de acceso y la auditoría solo pueden ser aplicados de forma individual en cada host, dificultándole al equipo central de seguridad el monitorear y obligar el uso de las directivas empresariales de seguridad.

En resumen, el SSL directo-a-host proporciona encriptación, pero dificulta el aplicar de forma centralizada el control de acceso y otras directivas de seguridad

Seguridad Legacy Host de Próxima Generación: Una arquitectura de múltiples capas

Por medio de una arquitectura moderna de múltiples capas, el software de emulación de terminal Reflection®, EXTRA!®, e INFOConnect® de

Attachmate® pueden ser usados con los componentes de seguridad de Reflection for the Web para proporcionar acceso protegido a las aplicaciones tradicionales de terminal.

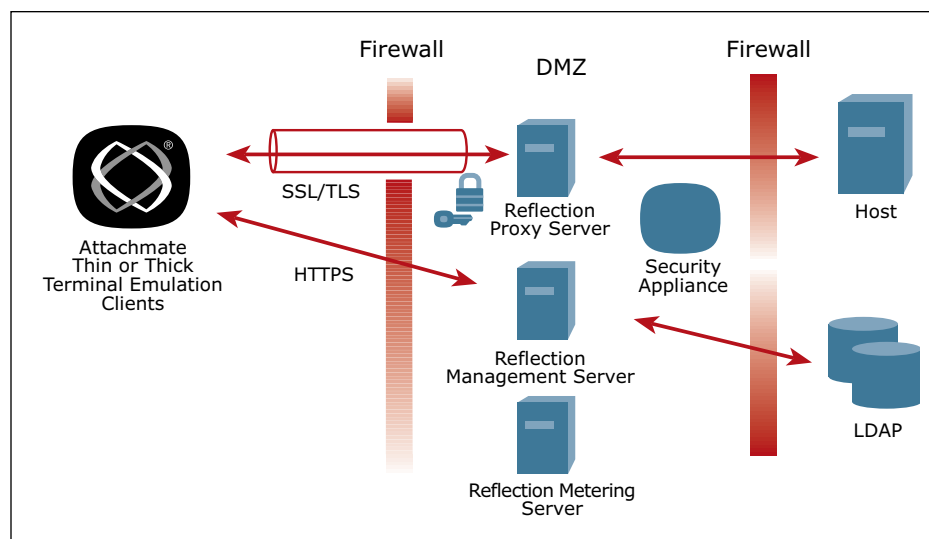
Reflection for the Web incluye los siguientes componentes:

- Reflection Management Server, aquí se controla de manera centralizada las configuraciones de los clientes y son manejados los enlaces de la empresa a la infraestructura centralizada de manejo de identidades.
- Reflection Security Proxy, recibe el tráfico SSL del lado del cliente y recibe tokens de autorización por el management server.
- Reflection Metering Server, rastrea el número de conexiones y tiene la opción de registrar cada host y puerto al que se ha conectado cada usuario, así como el tiempo total de la conexión.
- Emulación Reflection de cliente delgado, ofrece sesiones VT, TN3270, TN5250, NS/VT, y FTP cubiertas en SSL.

Las capas de la arquitectura moderna de seguridad de Attachmate incluyen:

- **Manejo centralizado de identidades.** Antes de acceder al host, un usuario debe primero ser autenticado por el Reflection Management Server, que valida las credenciales del usuario por medio del sistema de manejo de identidades empresarial, como LDAP, Active Directory, o un portal.

- **Control centralizado de acceso.** Antes de permitir la sesión, el Reflection Management Server verifica que el administrador haya concedido acceso a ese usuario a la sesión host. Los derechos de acceso pueden ser controlados por medio de la membresía de grupo LDAP.
- **Aplicación del control de acceso en el perímetro.** El Reflection Security Proxy (servidor proxy de seguridad) utiliza la exclusiva tecnología de token seguro de Reflection para verificar que el usuario este autorizado para conectarse al host antes de pasar la conexión a través de la DMZ. Los usuarios no autorizados nunca cruzan la DMZ.
- **Encriptación.** El cliente Reflection de emulación de terminal hace una conexión SSL al Reflection Security Proxy. La encriptación soportada puede llegar hasta AES 256-bits, y el código criptográfico es validado con FIPS 140-2.
- **Auditoría centralizada.** Debido a que los usuarios son autenticados y autorizados en el perímetro, el acceso a todos los recursos de red es monitoreado y registrado en un punto central—en el Reflection Management Server.
- **Monitoreo centralizado de amenazas en el perímetro.** Una opción comúnmente utilizada para implementar el Reflection Security Proxy es para decodificar todo el tráfico y pasarlo como texto plano Telnet desde una zona de red segura hacia el host. En este modo, todo el tráfico hacia y del host puede ser monitoreado usando la detección de intrusiones, la inspección de contenido y otros dispositivos de seguridad.



Next-generation host security puts an access control point in front of the host so that the user has to authenticate before getting onto the internal network. This control point can be centrally managed through integration with an enterprise identity management system such as LDAP.

Beneficios de la Infraestructura de Seguridad de Attachmate

A continuación se listan los beneficios de la infraestructura de seguridad en múltiples capas de Attachmate.

Manejo centralizado de la seguridad

Una ventaja clave de la arquitectura de seguridad de Attachmate es que permite el control centralizado sobre el tráfico de red que pasa entre los clientes y el host. En adición a cualquier método de autenticación que ocurra dentro del mismo host, Reflection habilita capas de autenticación, autorización y auditoría en la DMZ, donde pueden ser controlados y monitoreados de forma centralizada. Los problemas prácticos y logísticos asociados con la aplicación por separado de las directivas de seguridad en cada host backend individual se ven grandemente reducidos.

Integración con tu sistema existente de manejo de identidades

Reflection for the Web Management Server aprovecha tu inversión existente en un sistema de manejo de identidades.

Reflection interopera con todos los servidores típicos de LDAP:

- Active Directory
- Novell
- iPlanet/Netscape/SunOne
- IBM Directory Server
- IBM RACF
- OpenLDAP
- Otros servidores LDAP compatibles con RFC 2256

Reflection no es intrusivo; el acceso de solo lectura a tu directorio LDAP es suficiente. El acceso a tu host es controlado fácilmente usando tu estructura actual de usuarios y grupos LDAP.

Reflection también interopera con herramientas populares de autenticación web y portales:

- Portal WebSphere
- Portal BEA WebLogic
- Portal Plumtree
- Netegrity SiteMinder

A diferencia de algunos productos de la competencia, Reflection no hace que definas usuarios y grupos en tu producto de acceso host aparte de los usuarios y grupos

que ya has definido en tu directorio empresarial. Más bien Reflection aprovecha y facilita la integración con tu sistema existente de manejo de identidades.

La autorización exclusiva de token seguro proporciona la aplicación del control de acceso

Varios productos de la competencia ofrecen una sencilla puerta de enlace SSL o dispositivos de redirección. Sin embargo, todos ellos tienen una falla en común: Aceptan conexiones desde cualquier cliente habilitado con SSL, sin verificar que el usuario haya sido autorizado para conectarse al host.

En los productos de la competencia, los usuarios legítimos se autentican antes de obtener su sesión, pero un intruso con un cliente habilitado con SSL puede saltarse el paso de autenticación y simplemente conectarse a la puerta de enlace o el redireccionador, los cuales no verifican que el usuario haya sido autorizado para conectarse al host. Al no verificar esto el dispositivo automáticamente pasa la conexión directamente al host. El resultado es que el intruso pasa sin problemas todo el camino hacia el host.

Reflection Security Proxy, en contraste, requiere que los clientes prueben que ya han sido autenticados y autorizados para acceder al host. Cuando un cliente se autentica en el Reflection Management Server, el servidor verifica que el usuario este autorizado para la sesión solicitada y luego pasa al cliente un token firmado digitalmente (de tiempo limitado) que concede el acceso solicitado. EL proxy de seguridad verifica la firma digital del token utilizando cifrado de clave pública antes de pasar la conexión directamente al host.

Un intruso que intente hacer una conexión SSL al Reflection Security Proxy—sin primero ser autenticado y autorizado por medio del management server—le será negado el acceso al proxy. El intruso nunca podrá siquiera hacer una conexión de red al host.

Acceso a múltiples hosts por medio de un solo puerto

Varios productos de la competencia ofrecen una sencilla puerta de enlace SSL o dispositivos de redirección que mapean un puerto de escucha a un host backend. Si tienes varios host backend, tienes que abrir múltiples puertos de escucha, por tanto, múltiples puertos en el firewall.

Reflection Security Proxy permite a los clientes conectarse a múltiples hosts por medio de un solo puerto de escucha. Al utilizar una sola rendija en el firewall, por ejemplo, en el puerto 443, puedes habilitar el acceso a todos tus hosts y más tarde

agregar hosts adicionales sin cambiar nada en el firewall. Esto simplifica la configuración y reduce la carga administrativa para el personal de seguridad.

Un escenario alternativo: encriptación de punto a punto con control de acceso en el perímetro

Una arquitectura común para proteger el acceso al host es requerir tráfico encriptado al Reflection Security Proxy en la DMZ, y entonces permitir tráfico de texto plano de la zona segura al host. Esto permite la inspección de contenido del tráfico hacia y desde el host.

Algunas veces, sin embargo, existen razones para requerir conexiones SSL del cliente hacia el host. Las empresas pueden querer garantizar la integridad de los mensajes entre el cliente y el host, o pueden tener directivas que requieran encriptación en todas partes. Una sencilla arquitectura SSL directo-a-host permite la encriptación de punto a punto, pero tiene todas las desventajas que han sido señaladas arriba: no puede ser impuesto en el perímetro el control de acceso y la seguridad no puede ser administrada, monitoreada ni auditada de forma centralizada.

En la arquitectura Reflection, es posible tener encriptación de punto-a-punto así como manejar centralmente la administración, el monitoreo y la auditoría. Esta configuración puede ser establecida con marcar una sencilla opción del lado del cliente.

El Reflection Security Proxy requiere que los clientes usen la autorización de token seguro para probar que han sido autenticados y autorizados para conectarse al host. Solo después de que el token seguro ha sido validado por el proxy se permite al cliente abrir una conexión SSL directamente al host.

La conexión SSL resultante es una verdadera conexión de punto-a-punto, en vez de ser SSL del cliente al proxy y luego una conexión SSL separada del proxy al host.

Por medio de este mecanismo, Reflection logra lo que ningún otro producto en la industria puede hacer al permitir simultáneamente:

- Una conexión SSL de punto-a-punto, donde el cliente completa una sincronización (handshake) SSL directamente con el host destino.
- Manejar de forma centralizada el control de acceso, no se le permite al cliente pasar el proxy hasta que haya sido autenticado y autorizado por el proxy.

Desde luego, con esta configuración se pierde la posibilidad de hacer la inspección de contenido. [Nota: Existe, sin embargo, una forma de obtener la

inspección de contenido y una conexión SSL de punto-a-punto utilizando Reflection for the Web. Si necesitas información en cómo configurar esto, contacta al Soporte Técnico de Attachmate.]

Amplia Compatibilidad de Plataforma

Los servidores Reflection Management y Metering (administración y medición) son compatibles con los principales servidores web y servidores de aplicaciones. Reflection for the Web se envía junto con Tomcat, pero también puede ser implementado en IBM WebSphere, BEA WebLogic, Microsoft® IIS, y otros entornos populares de servidor. De forma similar, Reflection Security Proxy puede ser instalado en cualquier plataforma que soporte Java.

Reflection for the Web puede ser instalado en cualquier plataforma que soporte Java, incluyendo Windows, Linux, Solaris, HP-UX, y z/OS.

Los emuladores de cliente ligero de Reflection for the Web corren sobre cualquier plataforma que soporte Java, incluyendo OS X, Linux, y Windows. Todas las versiones comunes del cliente Java son soportadas, incluyendo Sun JRE 1.5 y anteriores, y la versión de 1.1 de la VM de Microsoft.

Reflection for the Web también soporta navegadores web populares, incluyendo Internet Explorer, Mozilla, FireFox, Safari, Opera, y Netscape. Para máxima seguridad y compatibilidad de plataforma, Javascript es soportado cuando está presente, pero no es requerido en las máquinas de los usuarios finales.

Seguridad no Intrusiva en Múltiples Capas para Aplicaciones Legacy Host

Las aplicaciones legacy host nunca fueron creadas para encajar en el mundo de las arquitecturas modernas de seguridad y acceso extendido de red. No obstante, utilizando el Reflection for the Web Management Server y el Servidor Proxy de Seguridad, es posible brindar una seguridad moderna en múltiples capas a las aplicaciones tradicionales de terminal de una forma no intrusiva, sin modificar las aplicaciones o los hosts en las cuales residen.

La arquitectura de seguridad Reflection ofrece muchas ventajas:

- Te permite agregar capas de seguridad enfrente de tu host.
- La seguridad de Reflection no es intrusiva—no hay necesidad de modificar las aplicaciones o los hosts en las cuales residen.

- La misma arquitectura de seguridad puede ser utilizada con los emuladores de cliente delgado y cliente robusto de Attachmate.
- El Reflection Management Server y el Servidor Proxy de Seguridad son compatibles con los balanceadores de carga comúnmente utilizados, permitiéndote agregar redundancia y escalar el manejo hacia una implementación más grande.

La arquitectura moderna de seguridad utiliza la defensa en profundidad, poniendo diferentes capas, incluyendo proxy inverso, autenticación, y autorización en la DMZ; aplicación de directivas de red con los dispositivos de seguridad (corriendo inspección de contenido, detección de intrusiones, etc.); y una zona segura para los servidores backend.

La seguridad host de primera generación proporciona encriptación SSL directa-a-host, pero no existe autenticación hasta que la conexión ha alcanzado al host, dando a los intrusos un pasaje seguro y directo hasta la pantalla de inicio de sesión del host.

La seguridad host de próxima generación pone un punto de control de acceso enfrente del host, así el usuario tiene que autenticarse antes de entrar en la red interna. Este punto de control puede ser manejado de forma centralizada por medio de la integración con un sistema empresarial de manejo de identidades como LDAP.

Acerca de Attachmate

Attachmate ayuda a los negocios a extender, manejar y proteger sus recursos IT. Ofrecemos un amplio rango de soluciones—desde productos para la emulación de terminal, integración legacy y administración del ciclo de vida de la PC hasta innovadoras herramientas para la administración de sistemas y seguridad. Con nuestra tecnología, más de 65,000 clientes alrededor del mundo están utilizando sus recursos IT de formas totalmente nuevas y valiosas. Conozca más en www.attachmate.com.mx.



Sede Central
1500 Dexter Avenue North
Seattle, Washington 98109
TEL +1 206 217 7500
FAX +1 206 217 7515

Oficina Central Para América Latina
México
TEL +52 55 9178 4970
FAX +52 55 5540 4886

Oficina Central Para EMEA
Países Bajos
TEL +31 71 368 1100
FAX +31 71 368 1181

Oficina Central Para España
Madrid
TEL +34 911517111
TEL +34 911517120

WEB WWW.attachmate.com.mx
EMAIL info-es@attachmate.com

Para obtener información sobre las oficinas regionales, visite www.attachmate.com.mx.