WHITE PAPER

attachmate

Protecting Legacy Host Applications With Modern Security

CONTENTS

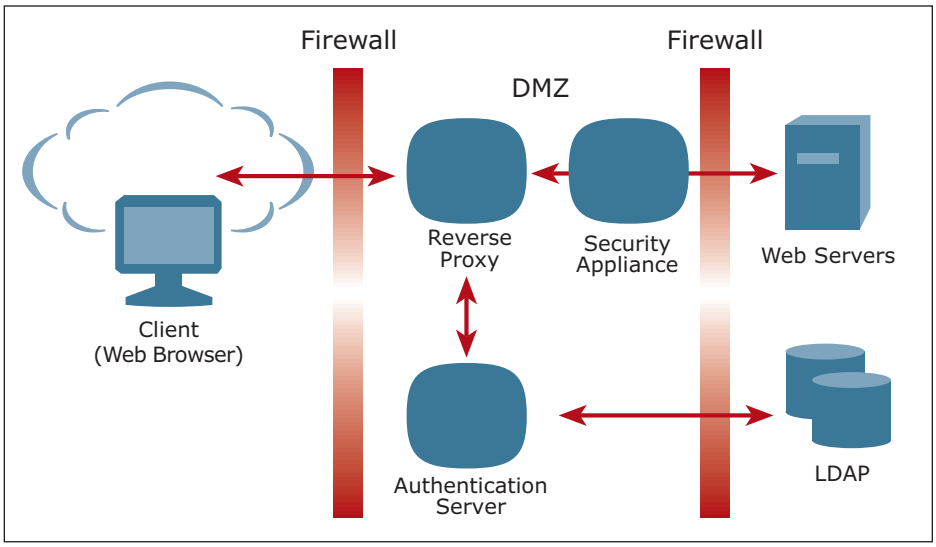
Protecting Legacy Host Applications With Modern Security

Enterprises today, under pressure to ensure data privacy and to safeguard sensitive information, have built up sophisticated IT security infrastructures. They implement a defense-in-depth strategy, putting in multiple layers of protection. Unfortunately, defending the systems where most of the critical data are stored often falls to antiquated and inadequate security methods.

There is a way, however, to pull these crucial legacy hosts into the modern security architecture. This white paper looks at the evolution of securing host applications and explains the advantages of an up-to-date approach to defending green-screen applications.

Modern Multi-Layered Approaches to Security

Modern approaches to network security are multi-layered thus implementing the security principal of "defense in depth." The modern enterprise employs multiple tools to guard against a variety of threats.



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.

The diagram shows a common security architecture for secure access to server-based applications:

Multiple security measures

The modern, multi-layered architecture incorporates a range of security measures:

- Encryption. Data are encrypted when passing through the nonsecure network outside the perimeter.
- Centralized identity management. An enterprise LDAP repository manages identity information for all users.
- Centralized access control. Authentication and authorization policies are applied at the perimeter to all traffic between clients and servers.
- Centralized auditing. Access to network resources is centrally monitored at the access control point.
- Centralized threat monitoring. Incoming and outgoing traffic is scanned at the perimeter with intrusion detection, content inspection, and other security devices to monitor for possible attacks or leaks of sensitive data.

Centralized management of security

Having multiple security measures in place is important, but equally important is how those security measures are managed. A decentralized enterprise may have different applications and different servers controlled by different lines of business. It can be challenging for a central security group to monitor and enforce the security practices applied at each of the backend server nodes.

The modern security architecture described above offers centralized management of security. All network traffic passing between clients and backend servers must pass through a DMZ that is controlled by the central security team. This creates a central point of control for applying, monitoring, and enforcing enterprise security policies, independent of

whatever security practices are being applied at each individual backend node.

Legacy Host Applications without Security

Access to legacy host applications has traditionally been through Telnet over port 23. This raises multiple security issues, including:

- *No confidentiality of data or passwords*. Without encryption, data and passwords are exposed.
- *Weak authentication*. Many hosts are limited to case-insensitive eight-character passwords.
- *Decentralized authentication*. Host-based authentication is often difficult to tie in to LDAP, and is usually disconnected from the identity management systems used in the rest of the enterprise.
- *Decentralized access control*. Access control happens only at the host, so there is no centralized control over access to enterprise resources.
- *Decentralized auditing*. Access to hosts is monitored only by the hosts themselves.

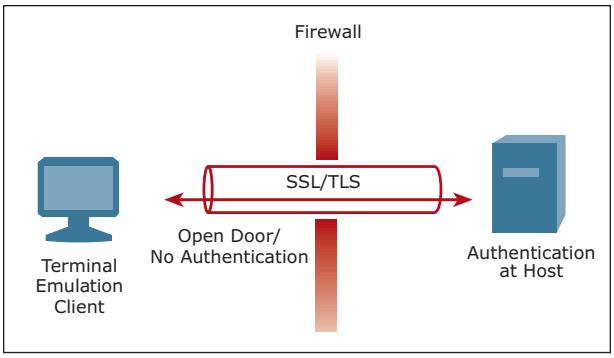
First-Generation Host Security: SSL Direct-to-Host

First-generation host security architectures use SSL connections directly from the client to the host. This provides one key advantage—data and passwords are encrypted.

However, the encrypted tunnel from the client to the host has the unfortunate side effect of defeating other security measures by making it difficult to monitor network traffic or apply any kind of access control in the DMZ.

Limitations of the simple SSL direct-to-host architecture include:

- *Weak, decentralized authentication*. Authentication is still handled completely by the host in most SSL deployments, so many hosts are protected only by eight-character case-insensitive passwords. Host authentication is usually divorced from the identity management systems used in the rest of the enterprise.
- *Decentralized access control*. Access control happens only at the host, so there is no centralized control over access to enterprise resources.
- *Unauthenticated SSL traffic is passed straight to the host*. The encrypted SSL tunnel makes it impossible to monitor the connection in the DMZ and provides intruders with safe passage all the way to the host logon screen. The central security team has to let traffic through the DMZ without knowing who the client is, or what the traffic is, because the traffic is encrypted.
- *Decentralized auditing*. Access to hosts is monitored only by the hosts themselves.
- *No centralized threat monitoring at the perimeter*. Incoming and outgoing traffic cannot be scanned with content inspection or other security devices because the content is encrypted.
- *Decentralized control over security*. Authentication, access control, and auditing can be applied only at each individual host, making it difficult for the central security team to monitor and enforce the use of enterprise security policies.



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.

In summary, SSL direct-to-host provides encryption, but can make it difficult to have centralizedenforcement of access control and other security policies

Next-Generation Host Security: Layered Security for Legacy Host Applications

Through a modern multi-layered security architecture, Attachmate Reflection® software enables access to traditional green-screen host applications. The layers of this architecture include:

- *Centralized identity management*. Before accessing a host, a user must first authenticate to the Reflection Management Server, which validates the user's credentials using the enterprise identity management system, such as LDAP, Active Directory, or a portal.

- *Centralized access control*. Before allowing the session, the Reflection Management Server verifies that the administrator has granted that user access to the host session. Access rights can be controlled through LDAP group membership.
- *Enforcement of access control at the perimeter*. The Reflection Security Proxy uses Reflection's unique secure token authorization technology to verify that the user is authorized to connect to the host before passing the connection through the DMZ. Unauthorized users never get through the DMZ.
- *Encryption*. The Reflection terminal emulation client makes an SSL connection to the Reflection Security Proxy. Encryption strengths up to 256-bit AES are supported, and the cryptographic code is FIPS 140-2 validated.
- *Centralized auditing*. Because users are authenticated and authorized at the perimeter, access to all network resources is monitored and logged at a central point—the Reflection Management Server.
- *Centralized threat monitoring at the perimeter*. One commonly used option for deploying the Reflection Security Proxy is to decrypt all traffic and pass it as plaintext Telnet through a secure network enclave to the host. In this mode, all traffic to and from the host can be monitored using intrusion detection, content inspection, and other security devices.

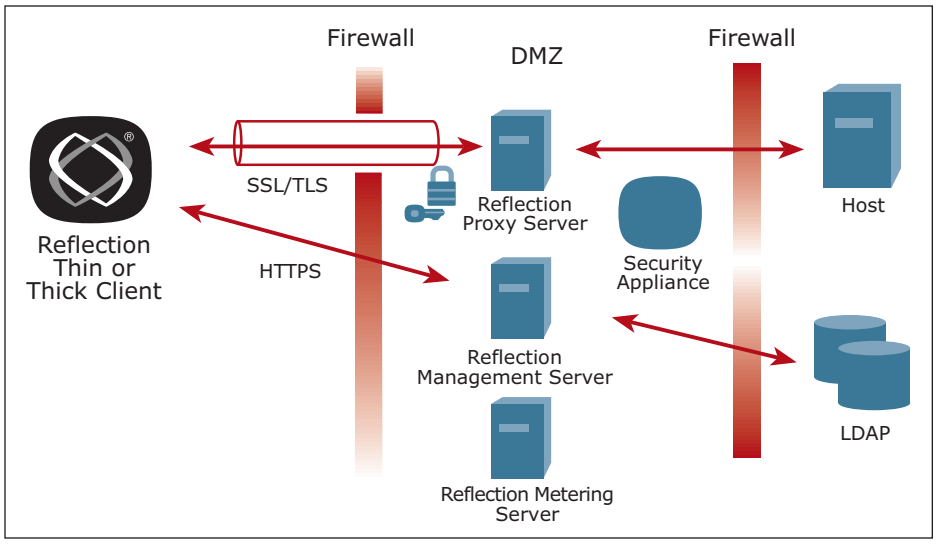
Reflection advantage: centralized management of security

A key advantage of the Reflection security architecture is that it allows centralized control over the network traffic passing between the clients and the host. In addition to any authentication that happens on the host itself, Reflection enables layers of authentication, authorization, and auditing in the DMZ, where they can be centrally controlled and monitored. The practical and logistical problems associated with enforcing security policies separately at each individual backend host are greatly reduced.

Next-Generation Host Security with Reflection for the Web and Windows-Based Reflection

Reflection security architecture comprises the following components in Reflection for the Web:

- Reflection Management Server, where centralized client configurations are controlled and which ties in to an enterprise's centralized identity management infrastructure.
- Reflection Security Proxy, which receives SSL traffic from the client side and receives authorization tokens dispensed by the management server.
- Reflection Metering Server, which tracks the number of connections and has the option of recording every host and port that every user connects to, as well as total connect time.



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.

- Reflection thin client emulation, which offers VT, TN3270, TN5250, NS/VT, and FTP sessions wrapped in SSL.

Reflection thick client emulation sessions can be used with the Reflection for the Web infrastructure, so that traditional emulation can enjoy the protections of the Reflection security architecture.

Integration with your existing identity management system

The Reflection for the Web Management Server leverages your existing investment in an identity management system.

Reflection interoperates with all common LDAP servers:

- Active Directory
- Novell
- iPlanet/Netscape/SunOne
- IBM Directory Server
- IBM RACF
- OpenLDAP
- Other RFC 2256-compliant LDAP servers

Reflection is nonintrusive; read-only access to your LDAP directory is sufficient. Access to your hosts is easily controlled using your existing LDAP user and group structure.

Reflection also interoperates with the popular portal and web authentication tools:

- WebSphere portal
- BEA WebLogic portal
- Plumtree portal
- Netegrity SiteMinder

Unlike some competing products, Reflection does not make you define users and groups in your host access product, separate from the users and groups you have already defined in your enterprise directory. Rather, Reflection makes it easy to integrate with and leverage your existing identity management system.

Unique secure token authorization provides enforcement of access control

Several competing products offer simple SSL gateway or redirector devices. However, these all have a common flaw: They accept connections from any SSL-enabled client, without verifying that the user has been authorized to connect to the host.

In competing products, legitimate users authenticate before getting their session, but an intruder with an SSL-enabled client can skip the authentication step and simply connect to the gateway or redirector, which does not verify that the user is authorized to connect to that host. Instead, the device automatically passes the connection through to the host. The result is that the intruder gets a free ride—all the way to the host.

The Reflection Security Proxy, by contrast, requires clients to prove that they have been both authenticated and authorized to access the host. When a client authenticates to the Reflection Management Server, the server verifies that the user is authorized for the requested session and then passes the client a time-limited, digitally signed token granting the requested access. The security proxy verifies the token's digital signature using public key cryptography before passing the connection through to the host.

An intruder who attempts to make an SSL connection to the Reflection Security Proxy—without first being both authenticated and authorized through the management server—will be denied access at the proxy. The intruder will never even make a network connection to the host.

Access to multiple hosts through a single port

Several competing products offer simple SSL gateway or redirector devices that map a listening port to a backend host. If you have multiple backend hosts, you have to open multiple listening ports, and thus, multiple ports in the firewall.

The Reflection Security Proxy allows clients to connect to multiple hosts through a single listening port. By using a single opening in the firewall, for example, on port 443, you can enable access to all of your hosts and later add additional hosts without changing anything on the firewall. This simplifies configuration and reduces the administrative burden for the security team.

An alternative scenario: end–to-end encryption with access control at the perimeter

A common architecture for secure host access is to require encrypted traffic from the client to the Reflection Security Proxy in the DMZ, and then allow plaintext traffic through the secure enclave to the host. This enables content inspection of the traffic to and from the host.

Sometimes, however, there are reasons to require SSL connections from the client all the way to the host. Enterprises may want to ensure message integrity

between the client and the host, or they may have policies that require encryption everywhere. A simple SSL direct-to-host architecture allows end-to-end encryption, but has all the disadvantages noted above: access control cannot be imposed at the perimeter and security cannot be centrally administered, monitored, and audited.

In the Reflection security architecture, it is possible to have end-to-end encryption as well as central administration, monitoring, and auditing. This configuration can be set up with a simple checkbox on the client side.

The Reflection Security Proxy requires clients to use secure token authorization to prove that they have been both authenticated and authorized to connect to the host. Only after the secure token has been validated does the proxy allow the client to open an SSL connection all the way to the host.

The resulting SSL connection is truly end-to-end, rather than being SSL from client to proxy and then a separate SSL connection from proxy to host.

Through this mechanism, Reflection achieves what no other product in the industry can do by simultaneously enabling:

- An end-to-end SSL connection, where the client completes an SSL handshake directly with the destination host.
- Centrally managed access control, where the client is not allowed past the proxy until both authentication and authorization are verified by the proxy.

Of course, with this configuration, the possibility of doing content inspection is lost. [Note: There is, however, a way to get content inspection and end-to-end SSL using Reflection for the Web. If you need information now on how to set this up, contact Attachmate Technical Support.]

Broad platform compatibility

The Reflection Management and Metering servers are compatible with the leading web servers and application servers. Reflection for the Web ships with Tomcat, but can also be deployed on IBM WebSphere, BEA WebLogic, Microsoft® IIS, and other popular server environments. Similarly, the Reflection Security Proxy can be installed on any platform that supports Java.

Reflection for the Web can be installed on any platform that supports Java, including Windows, Linux, Solaris, HP-UX, and z/OS.

The Reflection for the Web thin client emulators run on any platform that supports Java, including OS X, Linux, and Windows. All common Java client versions are supported, including the Sun JRE 1.5 and earlier, and the Microsoft 1.1 VM.

Reflection for the Web also supports the popular web browsers, including Internet Explorer, FireFox, Safari, Netscape, and Mozilla. For maximum security and platform compatibility, Javascript is supported when present, but is not required on end-user machines.

NonIntrusive Multi-Layered Security for Legacy Host Applications

Legacy host applications were never designed to fit into the world of modern security architectures and widespread network access. However, using the Reflection for the Web Management Server and Security Proxy Server, it is possible to bring modern multi-layered security to traditional green-screen applications in a nonintrusive manner, without modifying the applications or the hosts on which they reside.

The Reflection security architecture offers many advantages:

- It enables you to add layers of security in front of your host.
- Reflection security is nonintrusive—there is no need to modify the applications or the hosts on which they reside.
- The same security architecture can be used with Reflection thin client emulators or Windows-based thick clients.
- Both the Reflection Management Server andthe Security Proxy server are compatible with commonly used load balancers, allowing you to add redundancy and to scale up to handle a large deployment.

About Attachmate

Attachmate, owned by an investment group led by Francisco Partners, Golden Gate Capital and Thoma Cressey Equity Partners, enables IT organizations to extend mission critical services and assure they are managed, secure, and compliant. Attachmate's leading

solutions include host connectivity, systems and security management, and PC lifecycle management. Our goal is to empower IT organizations to deliver trusted applications, manage services levels, and ensure compliance by leveraging knowledge, automation, and secured connectivity. For more information, visit **www.attachmate.com**.

Corporate Headquarters
1500 Dexter Avenue North
Seattle, Washington 98109
TEL 206 217 7500
800 872 2829
FAX 206 217 7515

EMEA Headquarters
The Netherlands
TEL +31 71 368 1100
FAX +31 71 368 1181

Asia Pacific Headquarters
Australia
TEL +61 3 9825 2300
FAX +61 3 9825 2399

Latin America Headquarters
Mexico
TEL +52 55 9178 4970
FAX +52 55 5540 4886

WEB attachmate.com
E-MAIL info@attachmate.com

For regional office information, visit **www.attachmate.com.**