Unlimited Web Access Management

Challenge:

Secure web resources without the costly installation of software plugins or deploying bottleneck generating proxies.

Solution:

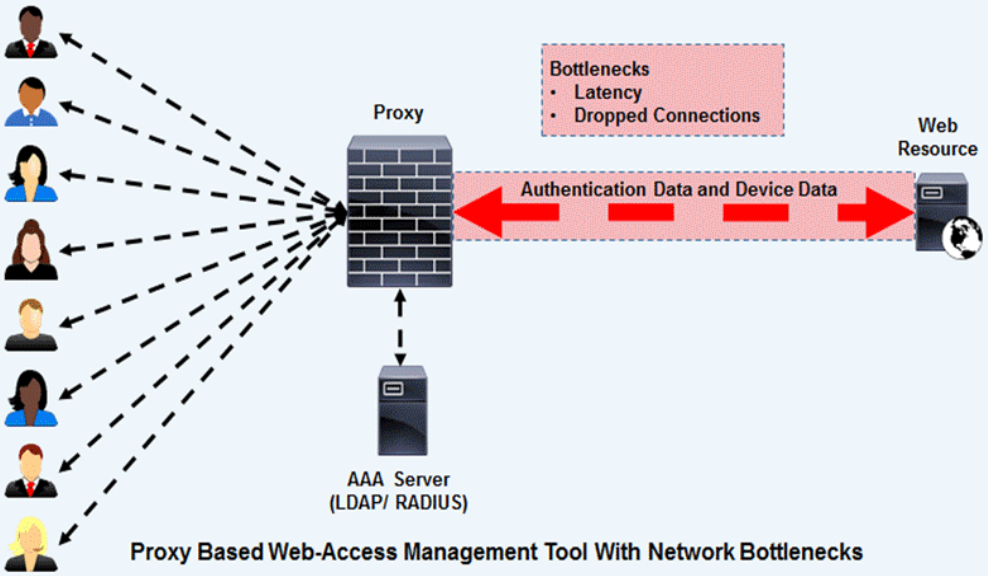
Deploy the SMRTe™ Web Access Management tool to secure web resources. The SMRTe is a Virtual Machine that can be simply deployed anywhere in the network without network re-architecture. After it authenticates a user via MFA it allows direct access to the web resource thereby removing bottlenecks.

Web Access Management tools are designed to secure access to web resources including web servers and web-based applications. TELEGRID's Secure Multi-web Remoting Tool – Enterprise (SMRTe) Model RWP-1802 is a Web Access Management tool that lets organizations secure web resource without the costs of designing software plugins or the bottlenecks inherent in proxies.

When a user logs into a Web Access Management tool their authentication credentials are sent to an Authentication, Authorization and Accounting (AAA) server like LDAP or RADIUS. The Web Access Management tool receives the AAA server's authorization response and determines whether to provide the user with access to the underlying web resource. Alternatively the Web Access Management tool can forward the authorization determination directly to the web resource in the HTTP headers.

Web Access Management tools also allow Single Sign-On (SSO) by letting users log in with one type of credential (e.g., PKI certificate, One-Time Password (OTP), etc.) and then logging that user into a web resource with a different type of credential. SSO coupled with Multi-Factor Authentication (MFA) drastically reduces security risks including insider threats. MFA consists of something you know (e.g., password, pin), something you have (e.g., smartcard, phone) and something you are (e.g., fingerprint). By providing 2 out of the 3 factors users are securely authenticated.

There are currently two methods to deploy Web Access Management tools – software plugins and proxies.



Proxy Based Web-Access Management Tool With Network Bottlenecks

Installation of a software plugin on an existing web resource, that has already been tested and certified, is problematic. Organizations are often unwilling to undertake software changes on critical web resources for fear of affecting uptime. Additionally many of an organization's web resources were developed by third parties and therefore cannot be easily or inexpensively changed.

The alternative method to deploy a Web Access Management tool is through a proxy (e.g., reverse web proxy, firewall, etc.). In this architecture web resources are placed behind a Web Access Management tool which retrieves a web resource on behalf of the user. The user does not know the IP address of the web resource and cannot access it directly. While this reduces the costs of designing software plugins, it also requires network re-architecture, which is not a simple task. More importantly, because all of the web resources sit behind the reverse web proxy, it has the potential to create a network bottleneck. This is a particularly important issue for organizations with web resources that are accessed by a large number (e.g., thousands) of users. For these types of installations, organizations must purchase expensive proxies or risk latency and dropped connections.

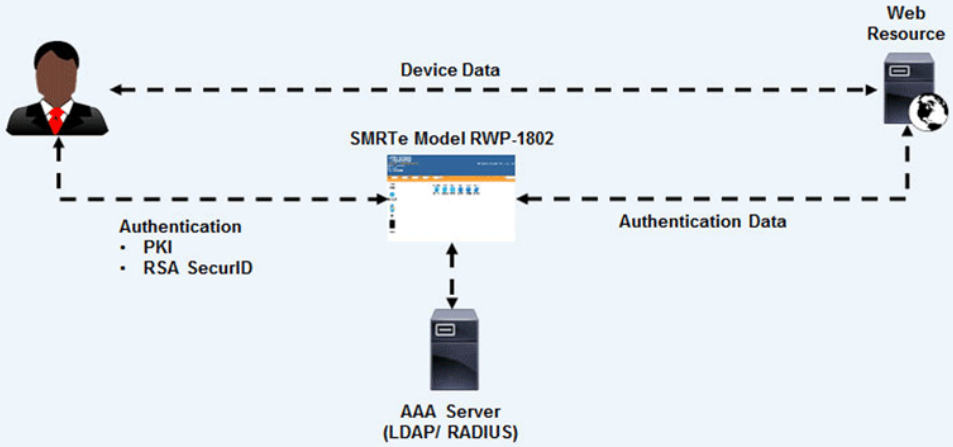
TELEGRID's patent-pending SMRTe securely authenticates the user and then provides direct access to the web resource thereby removing bottlenecks and latency. The SMRTe is not a software plugin and does not require any changes to the underlying web resource's code. The SMRTe is a Virtual Machine that can be placed anywhere in the network without requiring changes to the IP addresses of web resources.

The SMRTe enables SSO with MFA for secure user authentication. When a user logs into the SMRTe with their credentials they are presented with "one pane of glass" displaying all web resources in the network. When they click on a desired web resource the SMRTe, in conjunction with the existing AAA infrastructure, authorizes the user and gives them access to the web resource. Communication between the user and the web resource then occurs directly removing the possibility of the SMRTe becoming a bottleneck.

Even though devices and applications do not "sit behind" the SMRTe, like in proxy-based Web Access Management tools, the SMRTe's revolutionary design ensures that hackers cannot go around it and access the web resource directly. The SMRTe is able to protect access through its patent-pending technology which utilizes the existing AAA infrastructure and tokenization instead of passwords. This technology removes the possibility of a brute force password attack and the need for a password vault.

The SMRTe uses only FIPS 140-2 validated algorithms and modules for any and all cryptographic functions. The SMRTe enforces Security-Enhanced Linux (SELinux), a Linux kernel security module that provides a mechanism for supporting access control security policies, including DoD–style Mandatory Access Control (MAC).

The SMRTe was designed in compliance with Department of Defense Public Key Infrastructure (PKI) and Security and Technical Implementation Guides (STIGs).



SMRTe Web-Access Management Tool Without Network Bottlenecks

TELEGRID Technologies, Inc.
973-994-4440
sales@telegrid.com
www.telegrid.com

TELEGRID