## RCMA Employee Portal Solution RFP

10/8/2020

RCMA is seeking a solution that will provide our organization with the ability to allow remote users to connect safely to internal resources from outside the perimeter of our network. We are looking for a Secure Remote Access solution.

**Project Scope**

The scope and requirement of this solution are listed on the following pages.

**Timeline**

Project must be quoted within 10 days from the date of this RFP. Purchase decisions will be made the following week and deliverables received within 30 days of a confirmed purchase.

**Evaluation Criteria**

Proposals will be evaluated in a matrix style format based on the following criteria: cost, compatibility and ease of integration with existing systems, inclusion of items mentioned in the project scope, ability to deliver within the stated timeline and past experience with vendor.

Please contact Scott Olson for questions or clarification pertaining to this RFP at 813-753-4772 or by email at solson@rcma.org

**Project Scope**

The scope and requirement of this solution are as follows:

Must include 500 client licenses at a minimum.

**Appliance Manageability Requirements:**

The remote access security appliance shall be centrally manageable.

The central management solution shall contain a centralized policy that is synchronized to all child remote access security appliances.

The central management solution shall be capable of dynamically distributing user licenses to each child remote access security appliance.

The central management solution shall be capable of dynamically distributing the total client load to each child remote access security appliance.

The central management solution must support authentication via LDAP and LDAPS, including Active Directory, RADIUS, PKI, and SAML SSO.

The central management solution must contain reporting mechanisms that allow for showing the following connectivity metrics:

User count

User sessions

User ID/ Username

Connected Appliance

Session Lifetime

Session Connectivity Time

The solution console must be web-based

The event logs that each connected node records must be archivable and restored.

The central management solution and each individual remote access security appliance shall contain the ability to send events via email.

The central management solution and each individual remote access security appliance must Support log avoidance to Syslog servers.

The central management solution and each individual remote access security appliance must allow you to create administrative roles for solution management.

**Appliance Connectivity and Feature Requirements**

The remote access security appliance should be a system dedicated to performing remote connectivity through SSLVPN and IPSec where applicable.

The system must operate as a virtual appliance on Hyper V or Vmware. Currently RCMA operates using Hyper V technology.

The system shall allow at least 1.5 gigabit per second throughput.

Each remote access security appliance must contain a web form-based VPN console for remote user connectivity.

The remote access security appliance must contain a software client-based VPN application that is capable of auto selecting either an SSL VPN or IPSec connection protocol to the remote access server.

The software client-based VPN application must auto negotiate all VPN settings required to establish a remote session with the remote access security appliance.

The remote access security appliance shall be able to provision a custom client that has been configured with the appropriate connection requirements of the installed appliance(s) as to limit the scope of what the user must define in the client in order to make a connection.

The software client-based VPN application, or fully compatible substitutes, shall be available from both the appliance management console for deployment by the admin, or from the client users' operating system application store as to negate the need for manual software distribution.

The software client-based VPN application must be deployable by a software deployment tool. For example: IBM BigFix or AD DS Group Policy Objects.

The software client-based VPN application shall contain, as required or negated by choice of the administrator, bookmarks to specific internal and external resources that are accessible through the negotiated tunnel.

The software client-based VPN application shall be capable of opening a SSL VPN tunnel from anywhere the intended remote users initiate the session from AND the software client-based VPN application shall establish a secondary IPSec tunnel if it determines that the end-users internet access supports such a connection.

The web portal will also allow access to any TCP or UDP application in tunnel mode (Citrix, Terminal Services, VoIP, etc.) as defined by the admin.

The software client-based VPN application shall allow access to any TCP or UDP application in tunnel mode (Citrix, Terminal Services, VoIP, etc.) as defined by the admin.

The solution should have a special portal for mobile devices such as smartphones and tablets.

The solutions remote access portal shall be capable of custom branding and specifying custom design requirements including logos, colors, themes, layout, fonts, and the ability to organize all content therein.

The tunnel connection must support at least the following operating systems:

Microsoft Windows 10, 2012, 2016, and 2019

Linux

Mac OS

Android

Apple iOS

Apple iPadOS

The tunnel must operate on both TLS -SSL (Low TCP) at Layer 4-7 and for higher performance it will be able to failback to ESP (Encapsulating Security Payload) (Low UDP) at Layer 3

In web application accesses, internal addresses or computer names must be masked by the remote access security appliance.

The combined client access load shall point directly to a shared DNS name that all remote access security appliances, which are managed by the central management appliance, will respond to.

As the remote access security appliance accepts new, incoming connection requests, it shall evaluate the end client geolocation, IP address location, and connection quality including jitter, packet loss, and latency as to determine the best possible and/or closest remote access security appliance to the user assuring maximum performance and session stability.

**Appliance Policy Requirements**

The remote access security appliance shall be capable of configuring granular policies per any mix of user, subnet, host, range, web resource, http and https websites, RDP destinations, VNC connections, SharePoint sites, Exchange, Citrix VDI, VMware Horizon Clients, and form-based sites.

The remote access security appliance shall be capable of configuring granular policies from the user(s) or group(s) to individually defined resources.

The remote access security appliance shall be capable of configuring granular policies from any number of individually defined resources to the user(s) or group(s).

The remote access security appliance must support client to site directional traffic.

The remote access security appliance must support site to client directional traffic.

The remote access security appliance must have an endpoint control mechanism built in that supports MacOS, Windows, Linux, iOS, iPadOS, and Android.

The remote access security appliance's endpoint control mechanism must be able to detect installed software on the connecting client machines such as:

Anti-Virus Software

Any Program installed in the Windows “Program Files” directory

Any Program installed in the Windows “Program Files (x64)” directory

The system shall have a remote equipment inspection mechanism that validates at least:

- Files present on the remote computer
- Registry keys
- Membership in the Active Directory Domain
- Operating system version
- In-memory processes
- Presence of antivirus, antispyware or personal firewall
- For mobile devices Device IDENTIFIER (IMEI)
- Jailbreak detection on Apple IOS computers
- Root detection for Android computers

The inspection will not only be done at the time of access but on a regular basis.

The solution must have a method of cleaning up the cache of remote computers, using your own or third-party solution (Such a solution must be included).

Depending on the conditions of the remote computer it will enter a zone where connection privileges will be defined, if the computer does not meet the minimum requirements it will be sent to a quarantine zone where remediation policies can be applied.

The system must allow or restrict access to clients that have the antivirus up-to-date within a certain period of time, for example no more than 15 days.

Some remote users will only be able to enter allowed resources in a date range within a certain time range in the solution.

The remote user will only be able to access certain folders within a file sharing resource.

The remote access security appliance’s endpoint control mechanism must be able to detect software versions of any software or operating system and applicable patches that are installed on the connecting client machine.

Any and all values detected by the remote access security appliance’s endpoint control mechanism must be able to be defined in the appliance’s access control policy.

Access may be controlled by users or groups of users

The remote user will only be able to access the allowed resources based on their role or roles.

Access can be controlled through policies by source port or destination.

**Special Authentication Requirements**

The system will allow SAML 2.0 authentication for single sign-on of on-premises and cloud applications

The remote user must be able to authenticate using an X.509 digital certificate.

The remote user must be able to authenticate using, but not limited to, RSA Secure ID, Google Authenticator, Duo Security, One Login, AD DS ADFS, Microsoft Azure AD (Authenticator), etc…

The remote user must be able to authenticate using a token such as RSA SecureID, this authentication must be performed using a specialized agent that supports the solution for the token flag it offers.

Authentication can be Dual/Stacked, that is, the user can be validated first by one authentication method (for example, LDAP) and then by another (for example, RSA SecureID)

The system must support Captcha to prevent bot attacks and denial-of-service attacks.

The system must single sign on web applications, i.e. use VPN access credentials to access those applications.

The system must support biometric authentication present in cell phones and other mobile devices, including Apple laptops.

You must record an audit log about each authentication that each user performs.

You must save the data for each access to the resources required by each user.