Remote Control and Deep Packet Installation

https://campus.barracuda.com/doc/98217011/

Barracuda RMM remote control sessions occur over HTTP using the port on which the SCMessaging web service communicates (usually 80 or 443). This improves network security and reduces configuration requirements for hardened or compliance?sensitive environments.

Some firewalls under certain configurations will enforce deep packet inspection, which searches for protocol non?compliance in individual TCP packets. In the case of Barracuda RMM remote sessions, instead of regular HTTP packets, remoting packets are found. When this occurs, the security devices will not allow the communications to be successful, and remoting will cease to function correctly.

There are three possible solutions when this occurs:

1. **Switch to SSL.** The most favorable solution has the security device is unable to inspect packets between the Onsite Manager or Device Managers and the Service Center. Without the inspection occurring, all remoting should occur normally. If you are using SSL, purchasing a certificate from an authority offers many advantages over using self?signed certificates, removing the need to install certificates on each Onsite Manager or Device Manager manually, and guaranteeing compatibility with hosted PSA systems.
2. **Change the SCMessaging port.** Running SCMessaging on a port other than 80 provides you with the ability to create a rule on the security device specific to the communications between Barracuda RMM components. Remember that when you do this, you must enter the new address in Service Center under **System Settings** > **Communications Settings** and wait 5 minutes before making the change in IIS.
3. **Disable deep?packet inspection on the security device.** This is likely the least favorable solution because it mitigates the ability of the device to identify malware attacks. However, temporarily disabling inspection is useful for identifying it as the cause of the failures. If you are able, configuring a rule to disable inspections for packets coming from the Service Center IP address is favorable.