PROXY Pro RAS Edition

Security Hardening Guidelines

The PROXY Pro RAS Edition allows customers to independently operate and manage their own remote desktop support portal in-house in our on premise model. We thought it would be best to publish some guidelines and recommendations in and around securing an installation of the PROXY Pro RAS server. The web site that we've been using as the arbiter of "best practices" is the Qualys SSL Labs site. This site will contact any publicly addressable site/application on port 443 (only) and evaluate the SSL configuration found there. By exposing either IIS or the RAS server on a public port 443, tests can be run against our software.

In Windows, SSL support is handled in a module called "SChannel". This module and its configuration are *global* on the machine, and therefore changing the configuration to secure Web Console changes the configuration for all applications on the machine. As a result, we don't think it's appropriate that the PROXY installers change this global machine configuration, but it is our responsibility to call the administrator's attention to the issue and provide guidance on how to establish a good configuration.

Microsoft's guidance on configuring Windows is in their Support Knowledge Base article # 245030. Unfortunately, this does not provide guidance on what configuration should be used and instead documents a large number of registry keys that can be modified to change the configuration. As is, the information within the article wasn't directly helpful. During our exploration of this, we identified a software consulting company called Nartac Software had this same issue and has developed a utility program called IIS Crypto to address it. It's available for free at: https://www.nartac.com/Products/IISCrypto/Default.aspx

PROXY Pro RAS On-Premise customers are encouraged to follow these steps:

We perform these steps for the customer in the RAS Hosted model.

1. On the server machine to be configured, log into Windows as an administrative user of the machine.
2. Download the tool from https://www.nartac.com/Products/IISCrypto/(or access an already downloaded copy from somewhere).
3. Run the tool, and click the "Best Practices" button.
4. In the "Hashes" list, uncheck MD5 and SHA if it remained checked.
5. In the "Ciphers" list, uncheck "Triple DES 168/168" and "AES 128" if it remained checked.
6. Uncheck both boxes for TLS v1.0 and v1.1 leaving v1.2 enabled.
7. Click Apply.
8. Click the Close box in the upper-left hand corner of the window to close the utility.
9. Restart the machine. This is very important – the utility doesn't force or prompt for a restart, but the configuration changes will not take effect until after the machine is restarted.

Done. This is a one-time machine configuration change, at least until SSL best practices change again. Note well that this configures the SERVER side of SSL configurations only, so there's only value in doing this on machines that have SSL-based servers that use the Microsoft SChannel implementation. This specifically includes Internet Information Services (IIS) hosting Web Console, but excludes the Gateway Server, which uses OpenSSL for its SSL support.