SIPHON TAC

Using Proxies with Dovetail and the Dovetail Edge Server

Aled Treharne - 2018-11-23 - 0 Comments - in Dovetail

Many of our customers have stringent security requirements and in some cases, the customer assessment of risk may preclude directly connecting devices to a cloud system. Since Dovetail is only available as a cloud service, this presents issues in deploying devices into secure customer environments.

Security Model

It's worth touching briefly on the security model we use in Dovetail.

First of all, the current model we use to provide configuration and firmware to devices is a "pull" model. That is, every device is configured with Dovetail URL and instructed to check in periodically and check its current configuration agains the one on the server. As a result, all connections are initiated by the devices on the customer network and not by Dovetail.

Secondly, we use TLS connections with all of the devices supported by Dovetail. That gives us two advantages - firstly, the entire connection is encrypted preventing eavesdroppers from intercepting the configuration. The other advantage is that it allows us to use certificate authentication - every vendor installs a certificate on the device and cryptographically signs it during manufacture. This means we can a) validate that this device is trusted (because we trust the vendor's signing certificate) and b) the content of the certificate includes the MAC address, meaning that we can use that to authenticate the device.

On top of all of that, we set the configuration on the devices to validate the certificate intstalled on Dovetail so that both sides require valid and correct certificates to work.

This is the same security used for internet banking and many corporate high security VPN connections.

Corporate Proxies

For some of our customers, the security above isn't enough and they want to restrict access or filter the traffic through their own security systems. This is commonly done by using a proxy of some sort. Most of these proxies conform to RFC 2817 which describes a way for a proxy to provide proxying services but still allow a browser to connect securely to a remote server. This works well for modern browsers such as Chrome, Edge, Safari and Firefox.

However this presents us with two challenges:

1) We need a direct conversation with the device to be able to authenticate the certificates bidirectionally - this is achieveable using the correct type of proxy, but there are some corporate proxies that "hijack" the SSL connection. Those proxies don't work with Dovetail.

2) This requires device support for RFC 2817 which is uncommon and generally not supported accross the range of devices that Dovetail supports.

As a result, normal enterprise proxies aren't able to be used....so what is the answer?

Dovetail Edge Server

When we created Dovetail we recognised that our customers have locations where the security assessment deems it inappropriate to connect a device directly to the Internet and so we created the Dovetail Edge Server.

The Dovetail edge server consists of several components:

- Network readiness testing tool - providing a way to periodically check the quality of your network connection on a scheduled basis
- Configuration proxy - allowing local devices to connect to the edge server directly and receive configuration and firmware
- Management agent - providing a way to receive instructions from Dovetail without needing to provide a local interface

The Dovetail edge server establishes its own connection to Dovetail and, using the same security as devices use to connect, exchanges information on what it should do, whta tests to carry out and their results and any configuration information or firmware that devices need. We've designed the edge server carefully to ensure that there is no chink in the armor of the security we have in place - the ege server has its own certificate which it uses to authenticate to Dovetail making the connection between Dovetail and the edge server secure. When devices connect to the edge server, they're authenticated in the same way as they would if they connected to Dovetail - in fact, we use the same component in our cloud platform for public connections as we do in the edge server.

On top of all that the edge server also caches static files so optimising bandwidth usage and ensuring that your phones upgrade firmware as quickly as possible. We never store confidential configuration though, those are always passed from the cloud through to the devices, ensuring that we don't have any confidential customer information stored on the server.

The Dovetail edge server is available from Nuvias as a virtual machine in both VMware and Hyper-V formats. If you'd like a Dovetail edge server or want to know more about it, please get in touch.