Finally, if you don't already have equivalents, you may also want to have a virtualization solution (VMware Player, [download](http://www.vmware.com/products/player/overview.html), if you plan to evaluate/POC on your individual Windows PC or VMWare Fusion if using a Mac), a SOAP/REST client (I recommend soapUI, [download](http://sourceforge.net/projects/soapui/files/soapui/4.0.1/)), a SSH client (I recommend PuTTY.exe, [download](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html)) and a SFTP client (I recommend FileZilla Client, [download](http://filezilla-project.org/download.php)) available for working with your gateways. Note if you’re using a Mac, you may use SSH and scp directly from the terminal and do need an SFTP or SSH client.

Please ensure the following:

1. You have installed CA Policy Manager.
2. You have copied your evaluation license(s) for the SecureSpan Gateway to your file system for use later.
3. (Optionally) You have installed the additional supporting software recommended above (e.g. VMware Player, soapUI, PuTTY and/or FileZilla Client).

**Post Installation Steps:**

After these preparatory steps are completed, we can schedule some time for me to walk you through the following steps:

1. Creating your evaluation image.
2. Configuring your evaluation image if necessary.
3. Starting your evaluation image inside of VMware.
4. Configuring your evaluation image network settings.
   1. Will you be assigning the image a static or dynamic IP address?
   2. What is your network's default IP gateway address?
   3. What is your network's subnet mask?
   4. Do you have a list of one or more DNS servers available (recommended)?
   5. Do you have a list of one or more NTP servers available (recommended)?
5. Initializing your SecureSpan Gateway.
6. Licensing your SecureSpan Gateway.
7. Creating a simple HelloWorld proxy on your SecureSpan Gateway.
8. Enabling, licensing and configuring Enterprise Service Manager.
9. Deploying and configuring API Portal.
10. Placing the HelloWorld proxy under API Portal management.
11. (Optionally) Installing and configuring the SecureSpan Demo Environment.
12. (Optionally) Creating a SOAP proxy for the SecureSpan Demo Environment's Warehouse Service SOAP interface.
13. (Optionally) Creating a REST proxy for the SecureSpan Demo Environment's Warehouse Service REST interface.
14. (Optionally) Creating an LDAP identity provider using the SecureSpan Demo Environment LDAP instance.

**Ports used by the solution:**

If there will be firewalls, at a minimum, you should have the following TCP ports open from your workstation to your gateway(s) for the POC:

1. 22 for SSH to SecureSpan Gateway
2. 8080 for HTTP to SecureSpan Gateway
3. 8443 for HTTPS (with optional client certificate support, and Layer 7 Policy Manager's thick client connection) to SecureSpan Gateway
4. 9443 for HTTPS (with no client certificate support, and Layer 7 Policy Manager's browser-based interface) to SecureSpan Gateway
5. 8182 for HTTPS to ESM
6. 80 for HTTP to API Portal
7. 443 for HTTPS to API Portal

Here is a more complete list of TCP/UDP ports to consider:

|  |  |  |  |
| --- | --- | --- | --- |
| **TCP** | **UDP** | **Direction** | **Purpose** |
| 22 |  | Inbound | SSH (eth0 only) |
|  | 53 | Outbound | DNS (optional, though recommended) |
| 80 |  | Inbound | Default API Portal HTTP traffic listener |
|  | 123 | Outbound | NTP (optional, though recommended) |
|  | 161 | Inbound | SNMP (optional) |
| 199 |  | Inbound | SNMP (optional) |
| 443 |  | Inbound | Default API Portal HTTPS traffic listener |
| 2124 |  | Both | Node to node communication within a gateway cluster |
| 3306 |  | Both | MySQL (both gateways and API Portal) |
| 3307 |  | Both | MySQL Replication (gateways only) |
| 8080 |  | Inbound | Default gateway HTTP traffic listener |
| 8182 |  | Inbound | ESM server listener |
| 8443 |  | Inbound | Default gateway HTTPS (with optional client certificates) traffic listener, and default port for Policy Manager, ESM and API Portal connections |
| 8765 |  | Inbound | Process Controller listener (for remote management by ESM) |
|  | 8777 | Both | Multicast UDP for replay attack protection and one time SAML token use across a cluster (eth0 only) |
| 9443 |  | Inbound | Default gateway HTTPS (without client certificates) traffic listener, and default port for browser-based Policy Manager connections |
| ? |  | Outbound | LDAP (normally 389) |
| ? |  | Outbound | LDAPS (normally 636) |
| ? |  | Outbound | Service endpoint ports that gateway will direct traffic to |