**Network Provisioning Form for SaaS/Hosted eCMS**

|  |  |  |
| --- | --- | --- |
| **Contact Information:** | | |
| Customer Name: |  | |
|  | | |
|  | Email: | Phone: |
| Technical Contact: |  |  |
| Project Contact: |  |  |
|  | | |
| Date: |  | |

|  |  |  |
| --- | --- | --- |
| **External Network** | | |
| Primary ISP: | | Connectivity Type  (T1 minimum recommended): |
| Primary ISP Contact: |  | |
| Secondary ISP: | | Connectivity Type  (T1 minimum recommended): |
| Secondary ISP Contact: |  | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Internal Network** | | | | | | | |
| **NOTE: All networks must be broken down into /24 subnet ranges. We are not able to route any connections wider than a /24. Commonly used subnets may require a NAT to be in place. (both below have a net mask of 255.255.255.0)** | | | | | | | |
| Internal IP Ranges: Use/Notation (10.1.1.1/24 = 10.1.1.1 with a net mask of 255.255.255.0) | |  | **Internal IP Range** | |  | **Pingable IP for Testing** | |
| 1. |  | |  |  | |
| 2. |  | |  |  | |
| 3. |  | |  |  | |
| 4. |  | |  |  | |
| 5. |  | |  |  | |
| 6. |  | |  |  | |
| 7. |  | |  |  | |
| 8. |  | |  |  | |
| 9. |  | |  |  | |
| 10. |  | |  |  | |
| 11. |  | |  |  | |
| 12. |  | |  |  | |
| **Network Settings:** | | | | | | | |
| DNS 1: |  | | | Domain Name: | | |  |
| DNS 2: |  | | | NetBIOS Name: | | |  |

**VPN Configuration:** Fill in the un-shaded areas. All configuration settings presented are the preferred configuration. If you require a different configuration it can be arranged. Supported devices are any device that can act as an **IPSEC Peer**. Devices that act as an **IPSEC Client** are not supported

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Description** | **Customer Details** | **Datacenter Details** |
| **1** | **VPN/Firewall device make/model** |  | Cisco ASA 5516 |
| **2** | **Peer IP address** |  | 174.128.2.5 |
| **3** | **Authentication method: Pre-shared key** | (supplied by CGC prior to Tunnel Test) | |
| **4** | **Transform set** | 3DES + MD5 | |
| **5** | **DH Group (1 or 2)** | 2 | |
| **6** | **PFS (yes or no)** | Yes | |
| **7** | **ISAKMP lifetime (seconds)** | 86400 | |
| **8** | **Network addresses for IPSEC** | (See Above) |  |
| **9** | **Network addresses to be reached at the Data Center** |  | (supplied by CGC with VPN completed worksheet) |

**Legend**:

|  |  |  |
| --- | --- | --- |
| **#** | **Item** | **Information** |
| **1** | **VPN/Firewall device make/model** | Make and model of the VPN endpoint. Useful for setting up the tunnel options. |
| **2** | **Peer IP address** | Refers to the IPSEC device's registered Internet IP address. |
| **3** | **Authentication method: Pre-shared key** | Pre-shared key authentication exchange. |
| Note: Pre-shared key can be shared by secure means (phone). |
| **4** | **Transform set** | This is a combination of the encryption methods (des,des3) and the hash algorithm (sha or md5). |
| **5** | **DH Group (1 or 2)** | This is the Diffie-Hellman session key cryptography protocol. |
| **6** | **PFS (yes or no)** | Perfect Forward Secrecy ensures that a session key is from long-term |
| public/private keys. It is an optional feature of IPSEC. |
| **7** | **ISAKMP lifetime (seconds)** | Specifies the number of seconds a security association will live before expiring. |
| **8** | **Network addresses for IPSEC** | LAN IP addresses or subnets that will be allowed connectivity to the remote end. |
| **9** | **IP address to test VPN connectivity** | Used to initiate interesting traffic and test connectivity. |