Date:

|  |  |
| --- | --- |
| HKEX VPN PEER | CUSTOMER VPN PEER |
| Device (Make/Model): AWS | Device Vendor (Make/Model) [[1]](#footnote-1): |
| Device Platform: |
| Device Platform Software: |
| Test Target Host: (Default: 10.2.0.2 [DNS]) | Public IP: |

|  |  |  |
| --- | --- | --- |
| VPN PARAMETERS PREFERENCE | | |
| IKE Parameters | Default Settings | Client Optional Settings |
| IKE Negotiation Mode | Main Mode only | Main Mode only |
| IKE version [[2]](#footnote-2) | ikev2 | □ikev1 □ikev2 |
| Rekey margin time (seconds) [[3]](#footnote-3) | 540 |  |
| Rekey fuzz (percentage) [[4]](#footnote-4) | 100 |  |
| Replay window size (packets) [[5]](#footnote-5) | 1024 |  |
| PHASE 1 | | |
| IPSEC Parameters | Defaults Setting | Client Optional Settings |
| Authentication Method | Pre-shared key [[6]](#footnote-6)  (send separately) | To use HKEX pre-shared key |
| Security Association Lifetime (min)[[7]](#footnote-7) | 480 min | min (keylife) |
| Encryption Algorithm / Authentication Algorithm[[8]](#footnote-8) | AES-256 |  |
| Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms [[9]](#footnote-9) | SHA2-256 |  |
| Diffie-Hellman Group (DH Group) [[10]](#footnote-10) | Group 14 | Group |
| DPD timeout (seconds) [[11]](#footnote-11) | 30 |  |
| DPD timeout action [[12]](#footnote-12) | Clear |  |
| PHASE 2 | | |
| IPSEC Parameters | Defaults Setting | Client Optional Settings |
| Security Association Lifetime (min)[[13]](#footnote-13) | 60 min | min (keylife) |
| Encryption Algorithm / Authentication Algorithm | AES-256 |  |
| Hashed Message Authentication Code (HMAC) / Hash Algorithm / Integrity Algorithms | SHA2-256 |  |
| Diffie-Hellman Group (DH Group) | Yes, Group 14 |  |

(After HKEX received user input, we would set up customer gateway in AWS, public IP for tunnels will then be generate from that user in a configuration file(.txt))

|  |  |
| --- | --- |
| SECURED NETWORKS/HOSTS | |
| HKEX NETWORK / HOSTS / TARGET VPC CIDR Block | CUSTOMER NETWORK / HOSTS / Device Subnet [[14]](#footnote-14) |
| (Default: 10.2.0.0/22) |  |

|  |  |  |
| --- | --- | --- |
| CLIENT INFORMATION | | |
| Company Name: …… Fill in by Business partner……………………. | | |
| Customer Contact Name:  Primary contact -  Secondary contact – | Phone: | Email |
| Customer Support Contact : | Phone: | Email: |
| Additional comments: | | |

1. Supported Gateway Device type are from below vendor: Cisco Meraki, Cisco Systems, Citrix, Cyberoam, F5 Networks, Fortinet, Generic, H3C, IIJ, Juniper Networks, Microsoft, Mikrotik, Openswan, Palo Alto Networks, pfSense, SonicWall, Strongswan, WatchGuard, Yamaha, Zyxel. For more details of supported devices, please refer to (<https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html#CGRequirements> [↑](#footnote-ref-1)
2. Supported values: ikev1 or ikev2 [↑](#footnote-ref-2)
3. The period of time before phase 1 and 2 lifetimes expire, during which AWS initiates an IKE rekey. Supported values between: 60 and half of phase 2 lifetime. [↑](#footnote-ref-3)
4. The percentage of the rekey window during which the rekey time is randomly selected. Supported values between: 0 and 100. [↑](#footnote-ref-4)
5. The number of packets in an IKE replay window. Supported values between: 64 and 2048. [↑](#footnote-ref-5)
6. A 8-64 character string with alphanumeric, underscore(\_), and dot(.). It cannot start with 0. [↑](#footnote-ref-6)
7. Supported values between: 900 and 28,800 seconds, i.e. 15 and 480 minutes [↑](#footnote-ref-7)
8. Only these Encryption Algorithms for choosing, i.e. AES128, AES256, AES128-GCM-16, AES256-GCM-16 [↑](#footnote-ref-8)
9. Only these Integrity Algorithms for choosing, i.e. SHA1, SHA2-256, SHA2-384, SHA2-512 [↑](#footnote-ref-9)
10. Only these DH Group for choosing, i.e. 2, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 [↑](#footnote-ref-10)
11. The number of seconds after which a DPD timeout occurs. Supported values must be 30 or higher. [↑](#footnote-ref-11)
12. The action to take after dead peer detection (DPD) timeout occurs. By default, the IKE session is stopped, the tunnel goes down, and the routes are removed. Supported values: Clear, Restart and None [↑](#footnote-ref-12)
13. Supported values between: 900 and 3,600, i.e. 15 and 60 minutes, has to be less that Phase 1 Lifetime [↑](#footnote-ref-13)
14. This two CIDRs must not overlap with each other [↑](#footnote-ref-14)