**EOTSS Requirements**

Site-to-Site VPN Tunnel

Logo

Description automatically generated

Table of Contents

[Overview 1](#_Toc119421515)

[Technical Resource 1](#_Toc119421516)

[VPN Preliminary 1](#_Toc119421517)

[VPN Profile 1](#_Toc119421518)

[Routing 2](#_Toc119421519)

[Routing Protocol 3](#_Toc119421520)

[Connectivity Checklist 3](#_Toc119421521)

[Important Notes 3](#_Toc119421522)

[Additional Details 4](#_Toc119421523)

Overview  
The following form must be filled out in order to create a VPN Tunnel to the Commonwealth of Massachusetts network. VPN Tunnels connecting to this network must now conform to the following requirements:

1. Must use IKEv2
2. Must use AES256 bit encryption or higher (we do not support GCM)
3. Must use SHA256 or higher
4. Must use Group 14 or higher
5. Must be route based (no policy-based VPN will be supported)
6. Must use either Static Routes or BGP as the routing protocol
7. Must use for remote IKE Gateway IP Address 170.63.208.11/24 or 170.63.208.139/24

Technical Resource  
Please provide technical contact information below. Partner to fill in **BLUE** color cells in the form.

|  |  |
| --- | --- |
| Partner Contact Name |  |
| Partner Contact Phone Number |  |
| Partner Contact E-Mail Address |  |

|  |  |
| --- | --- |
| COMA Contact |  |
| COMA Phone Number |  |
| COMA Email |  |

# VPN Preliminary

To be completed by Technical Contact. Please fill in **BLUE** color cells in the form.

|  |  |  |
| --- | --- | --- |
| **Tunnel Endpoint** | **Preliminary** | **Partner Tunnel Endpoint** |
|  | VPN Appliance Model |  |
|  | Tunnel Peer IP |  |

# VPN Profile

Partner to fill in **BLUE** color cells in the form and mark **‘X’** where appropriate.

|  |  |  |  |
| --- | --- | --- | --- |
| **IKE Version: Only IKEv2 is supported**   |  | | --- | |  | |  | | |
| **Phase 1 (ISAKMP) Settings** | |
| Local Authentication (PSK) | **Shared over secured media** |
| Remote Authentication *(IKEv2 only)* | **Shared over secured media** |
| IKE Encryption Algorithm | **Only AES-256 or Higher Supported** |
| IKE Message Hash\PRF Algorithm  *(Hash changed to PRF in IKEv2)* | |  |  |  | | --- | --- | --- | | SHA256 | SHA384 | SHA512 | |  |  |  | |
| IKE Diffie-Hellman Group | |  |  |  |  |  | | --- | --- | --- | --- | --- | | 14 | 19 | 20 | 21 | 24 | |  |  |  |  |  | |
| IKE Lifetime Seconds  *(default 86400)* | 86400 |
| IKEv2 Integrity | |  |  |  | | --- | --- | --- | | SHA256 | SHA384 | SHA512 | |  |  |  | |
| **Phase 2 (IPSEC) Settings** |  |
| IPSec Encryption Algorithm Encapsulating Security Payload (ESP) | **Only AES-256 or Higher Supported** |
| IPSec Authentication / Integrity Algorithm / ESP  *(Integrity in IKEv2)* | |  |  |  | | --- | --- | --- | | SHA-256 | SHA384 | SHA-512 | |  |  |  | |
| IPSec Lifetime Seconds  (*default 28800)* | 28800 |
| IPSec Lifetime Kilobytes  *(default 4275000)* | 4275000 |
| PFS (Perfect Forward Secrecy) *Yes / No - Default* | |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | YES   |  | | --- | |  | | | | | NO   |  | | --- | |  | | | | | | If YES Group Number: | | | | | | | | |  |  |  | 14 | 19 | 20 | 21 | 24 | |  |  |  |  |  |  |  |  | |
| Dead Peer Detection  *Yes – Default /No* | |  |  | | --- | --- | | YES | NO | |  |  | |

# Routing

Specify Remote Routes that will access Commonwealth of Massachusetts, and what Commonwealth of Massachusetts routes you require access to.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **(IP Protocols & Ports Required)** | | | |
| **Partner**  **Source** | **Source Protocol/Port** | **COMA DST** | **Destination**  **Protocol/Port** | **Purpose** |
| (examples)  **172.16.0.0/16**  **172.16.0.1** | (example)  **ANY**  **UDP/389** | (examples)  **192.168.1.15/32**  **192.168.1.10/32** | (example)  **TCP/443**  **ANY** | (example)  **Partner subnet access to Webserver VIP over 443**  **Partner LDAP server listening on 389 to connect with destination host** |
|  |  |  |  |  |
|  |  |  |  | |  |  | | --- | --- | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |  |  | |
|  |  |  |  |  |

# Routing Protocol

Specify which Routing Protocol you would like to use:

|  |
| --- |
| Static: Yes or No |
| BGP: Yes or No |
| If BGP, what AS# would you like to use on your end: |
|  |

# Connectivity Checklist

|  |  |
| --- | --- |
| **Task** | **Notes** |
| VPN Phase 1 verification |  |
| VPN Phase 2 verification |  |
| Real traffic verification (i.e. Partner access to website) |  |
| Partner Specific\* |  |

Full connectivity testing is expected to be performed during activation process. All partner resources are required to be present and ready. Checklist parameters to be filled prior activation.

# Important Notes

* Please make sure that your interesting traffic matches to the above.
* VPN filtering will be implemented on Commonwealth of Massachusetts side; therefore, Protocol and Port is required.
* Allow 1-2 business days for Change control approval process once the VPN form is submitted.
* Once Change control is approved activation activity can be scheduled.

# Additional Details

If you have any other important information or details, please include them below.

|  |
| --- |
|  |