

Automated Commercial Environment

DECIDING WHICH CONNECTIVITY OPTION IS BEST FOR YOUR COMPANY

April 5, 2022



U.S. Customs and
Border Protection



DECIDING WHICH CONNECTIVITY OPTION IS BEST FOR YOUR COMPANY

There are three options to consider when deciding which method to use for a connection to the DHS/CBP Trade Partner Infrastructure:

Option #1: MQIPT (MQ Internet Pass-Thru)

Your company has access to the Internet and will:

- Desire a quick and easy modernized solution using encryption
- Support MQ Client

Connection Method:

Client connection via encryption public key certificates using ID-based cryptography. The client sends encrypted data via a public certificate to the receiver (server) which decrypts using a private key.

MQIPT Requirement:

- MQ Client v9.0.0.4 or higher
- Updated version of the MQ Support provided CBPPTGT program (if not running your own application code)
- MQ Support provided zipped MQIPT trade configuration package

NOTE: Connection information is located within the IBM MQ CCDT (Client Channel Definition Table) which is supplied as part of the MQIPT Trade package.

Other Software or Specification Required:

- Currently supported OS (e.g. Windows 10)
- Certificate and Keystore (provided by CBP MQ Support)
- IBM MQ Client Channel Definition Table (CCDT) – provided by CBP MQ Support

Benefits:

- The build and delivery of the "trade package" is being handled in an automated process by CBP MQ Support
- Changes are very minimal. Simply save trade package to the same location as the program and make minor changes to current ini file
- No additional cost, secure connection using encryption via DHS certificates, established and proven process/implementation
- MQIPT VIPs accessible via public internet

Limitations:

- None

Note: Trade Partners with multiple locations will be consolidated to use one SVRCONN channel and one certificate for all locations.

** The automation of MQ Client put/get connections is permitted at an interval of no less than 5 minutes.

Option #2: (Internet based IPSEC and IKEV2 LAN to LAN Connection)

Your company has high-speed Internet and will:

- Desire the most robust VPN connection via the Internet
- Support either MQ Client or MQ Server

Connection Method:

LAN / DSL / Cable Modem based Internet connection with Internet router with an available public IP address to dedicate to this connection

VPN Hardware Requirement (one of the following or equivalent):

- Cisco 900/1000 series routers with licensing that supports IPSEC and IKEV2 (estimated cost \$900)
- Cisco ISR 4K series routers with licensing that supports IPSEC and IKEV2 (estimated cost \$1,300)
- Cisco ASA (estimated cost \$1,000)
- For Cloud type VPN - Cisco CSR or VyOS VPN or similar with licensing that supports IPSEC
- Non-Cisco IPSEC device or Cloud Service Provider console VPN that supports AES256 IPSEC and IKEV2 and private to public NAT inside VPN tunnel

NOTE: If your company would like to use a Cisco (or non-Cisco) IPSEC device that is not listed above, please contact DHS/CBP's Network Support Team at 1-877-347-1638, option 1, to determine if the device meets DHS/CBP's requirements.

Other Software or Specification Required:

- AES 256 IPSEC Hardware Encryption
- IKEv2 Support

Benefits:

- Most robust type of VPN connection
- No recurring monthly leased line charges
- Utilizes existing, high-speed Internet connection
- Tunnel creation, to and from DHS/CBP, can be initiated from either side (when using MQSeries Server)
- Data flows at time of creation, rather than going into a queue (when using MQSeries Server)
- Multiple systems can send data to DHS/CBP without additional software (when using MQSeries Server)

Limitations:

- Not controlled and monitored at the same service level as a dedicated MPLS connection to DHS/CBP (scenario #2)

Note: This scenario can have a failover location, multiple locations, or extra client connections for testing!!

** The automation of MQ Client put/get connections is permitted at an interval of no less than 5 minutes.

Option #3: (MPLS based IPSEC LAN to LAN Connection)

Your company requires the assurance of a 24X7, always on, monitored connection with dedicated bandwidth and redundancy.

Connection Method:

- Dedicated and redundant MPLS* connections directly to DHS/CBP
- For AWS type commercial cloud connectivity via MPLS, DHS/CBP supports the use of AT&T Netbond

VPN Hardware Requirement (one of the following or equivalent):

- Cisco ISR 4221 with T1 Card (Cisco mfg# ISR4221-SEC/K9 & NIM-1MFT-T1/E1= / estimated cost: \$2,900)
- Cisco ISR 4331 with T1 Card (Cisco mfg# ISR4331-SEC/K9 & NIM-1MFT-T1/E1= / estimated cost \$3,900)
- For AWS Cloud type VPN - Cisco CSR1000V
- NOTE: If your company would like to use a Cisco (or non-Cisco) IPSEC device that is not listed above, please contact DHS/CBP's Network Support Team at 1-877-347-1638, option1, to determine if the device meets DHS/CBP's requirements.
- OPTIONAL: To accommodate trade partners that desire a backup connection for their dedicated circuit, use of an Internet VPN is supported as a secondary transport connection. This would require a separate VPN device selected from scenario #1.

Other Software or Specification Required:

- MQSeries Server
- Cisco IOS version level will be provided by DHS/CBP based on what is determined to be the most stable and secure code
- AES 256 IPSEC Hardware Encryption
- IKEv2 Support

Benefits:

- Most reliable type of connection
- Tunnel creation, to and from DHS/CBP, can be initiated from either side
- Data flows at time of creation, rather than going into a queue
- Multiple systems can send data to DHS/CBP without additional software
- Can be combined with Scenario #1 to enhance redundancy, in the event the MPLS connection goes down

Limitations:

- None

Details:

- Contact AT&T for costing (Verizon is no longer supported for new circuit requests).
- Pre-existing accounts – Contact your AT&T Account Representative for additional information.
- New accounts - Send E-Mail to DL-ATTOneNetOPS@att.com or call 855-559-8217, option 1

* MPLS: Multiprotocol Label Switching – Termed “VBNS” by Verizon and “AVPN” by AT&T