

# DHS/CBP TRADE VPN

## Deciding Which VPN Connection Type is Best for Your Company

Document Revision Level: 22 Revision Date: 10/16/2015  
OneNet Firewall Team Page 1 of 3

There are three scenarios that need to be considered when deciding which method to use to connect to the DHS/CBP Trade Partner VPN Infrastructure

### **Scenario #1: (Cisco EZVPN / MQ Client)**

Your company has Internet, will only need to send and retrieve data from one computer, and only needs to connect, briefly, to DHS/CBP a few times a day.

#### **Connection Method:**

LAN / DSL / Cable Modem based Internet connection and one of these three options:

- Cisco VPN Software Client version 4.8.01.0300 or later (Windows only)
- Cisco 891 (Cisco mfg# CISCO891-K9 / estimated cost: \$800) (other Cisco routers are acceptable if they support EZVPN - **ISR DOES NOT SUPPORT EZVPN**)
- Cisco ASA 5505 ONLY (Cisco mfg# ASA5505-50-BUN-K9 / estimated cost: \$ cost: \$500) - **NO other Cisco ASAs support EZVPN**

#### **Other Software Required:**

- MQSeries Client \*\*
- Potentially \$0 cost to establish connectivity to DHS/CBP
- Utilizes existing, high-speed Internet connection

#### **Limitations:**

- Cannot be used with MQSeries Server
- Connection needs to be manually initiated (can be scripted)
- Limited to “connect-put/get-disconnect” type connections
- Dropped connections will not auto-reconnect
- Connectivity to the WEB is blocked for that PC while it is connected to DHS/CBP
- Connectivity is limited to the locally connected LAN

**Note: This scenario can not have a failover, does not support multiple office locations, and does not support extra client connections for testing!!**

**DHS/CBP TRADE VPN**  
**Deciding Which VPN Connection Type is Best for Your Company**  
Document Revision Level: 22 Revision Date: 10/16/2015  
OneNet Firewall Team Page 2 of 3

**Scenario #2: (Internet based IPSEC LAN to LAN Connection)**

Your company has high-speed Internet and will:

- Desire the most robust VPN connection via the Internet
- **Run 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 891 (Cisco mfg# CISCO891-K9 / estimated cost: \$800)
- Cisco 1921 (Cisco mfg# CISCO1921-SEC/K9 / estimated cost: \$1,000)
- Cisco 2911 (Cisco mfg# CISCO2911-SEC/K9 / estimated cost: \$2,100)
- Cisco ASA 5505 - 5550 (Cisco mfg# ASA5505-50-BUN-K9 / estimated cost: \$500 ASA5550-50-BUN-K9 estimated cost: \$12,000 )
- NOTE: If your company would like to use a 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:**

- MQSeries Server
- AES 256 IPSEC Encryption

**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 #3)

**Note: This scenario can have a failover location, multiple locations, or extra client connections for testing!! MQ Client is NOT SUPPORTED in this scenario!**

# DHS/CBP TRADE VPN

## Deciding Which VPN Connection Type is Best for Your Company

Document Revision Level: 22 Revision Date: 10/16/2015  
OneNet Firewall Team Page 3 of 3

### **Scenario #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

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

- Cisco 1921 with WIC-1DSU-T1-V2 Bundle
  - Mfg# CISCO1921-T1 / estimated cost: \$1,300
- Cisco 2911 with WIC-1DSU-T1-V2
  - Mfg# CISCO2911 / estimated cost: \$2,200
- Mfg# WIC-1DSU-T1-V2= / estimated cost: \$700
- NOTE: If your company would like to use a 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.
- 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 #2 or #3.

#### **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 Encryption

#### **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 #2 to enhance redundancy, in the event the MPLS connection goes down

#### **Limitations:**

- None

#### **Details**

- Contact Verizon or AT&T for costing.
- Pre-existing accounts – Contact your Verizon Business Account Representative or AT&T Account Representative for additional information.
- New accounts - Call Verizon 888-200-6002, option 1 and request support for service.
- New Accounts – AT&T – Browse website  
<http://www.business.att.com/enterprise/Family/network-services/ip-vpn/?source=IEa225001ltpdsIP>

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

\*\* The automation of VPN Client and/or MQ Client put/get connections is permitted at an interval of no less than 5 minutes. In other words, please wait, or adjust your automated scripts to wait, at least 5 minutes between connections to DHS/CBP VPN/MQ.

**Note: MQ Client is NOT SUPPORTED in this scenario!**