



U.S. Department of  
Transportation  
Federal Aviation  
Administration

VNTSC- SWIM-ITWS-WSDD-1.1

Web Service Description Document  
System-Wide Information Management (SWIM)  
Integrated Terminal Weather System (ITWS)

Version No. 1.1

Date: March 17, 2011

Prepared for:  
Federal Aviation Administration  
Office of System Operations Programs  
800 Independence Ave, SW  
Washington, DC 20591

Prepared by:  
Volpe National Transportation Systems Center  
Traffic Flow Management Division  
55 Broadway  
Cambridge, MA 02142

Web Service Description Document  
**System-Wide Information Management (SWIM)**  
**Integrated Terminal Weather System (ITWS)**

Approval Signatures

<b>Name</b>	<b>Organization</b>	<b>Signature</b>	<b>Date Signed</b>

Web Service Description Document  
**System-Wide Information Management (SWIM)**  
**Integrated Terminal Weather System (ITWS)**

Revision Record

<b>Revision Letter</b>	<b>Description</b>	<b>Revision Date</b>	<b>Entered by</b>

## Table of Contents

1. Scope.....	1
1.1 Background.....	1
1.2 Intended Use.....	1
2. Applicable Documents.....	2
2.1 Government Documents .....	2
2.2 Non-Government Documents.....	2
3. Definitions .....	3
3.1 Terms and Definitions .....	3
3.1.1 Client .....	3
3.1.2 Service.....	3
3.1.3 Service Contract & Registry .....	3
3.1.4 Service Provider.....	3
3.2 Abbreviations and Acronyms.....	4
4. Web Service Properties and Capabilities.....	5
4.1 Service Profile.....	5
4.1.1 Service Provider.....	5
4.1.2 Service Consumers.....	5
4.1.3 Service Functionality .....	5
4.1.4 Security.....	6
4.1.5 Quality of Service .....	6
4.1.6 WSDL documents .....	7
4.2 Service Interfaces .....	9
4.2.1 Types.....	9
4.2.2 Messages .....	9
4.2.3 Operations .....	11
4.2.4 List of Interfaces.....	11
4.2.5 Endpoint — RetrievtwsSubscription .....	11
Appendix A. Connecting Clients to the SWIM-ITWS Web Service .....	12
A.1 How to Connect .....	12
A.1.1 SWIM-ITWS Sample Java Client and Test Tool .....	12
A.2 Information we need from our users.....	13
A.3 VPN Information.....	14

# 1. Scope

This Web Service Description Document (WSDD) describes the web service interface for System-Wide Information Management (SWIM) Integrated Terminal Weather System (ITWS) system.

## 1.1 Background

As part of the FAA's System Wide Information Management (SWIM) initiative, the SWIM Program Office has sponsored the SWIM-ITWS Segment 1 Service. The goal of the SWIM-ITWS Segment 1 Service is to distribute real-time ITWS data, encoded in XML, via standard Web Services interfaces to external NAS stakeholders. The products currently support by the SWIM-ITWS Segment 1 (S1) are listed in the SWIM-ITWS Comprehensive User Guide.

## 1.2 Intended Use

This WSDD is intended to be used by clients of the SWIM-ITWS services to facilitate the development and operation of service clients.

## 2. Applicable Documents

### 2.1 Government Documents

1. FAA–STD–063, XML Namespaces  
[http://www.faa.gov/air\\_traffic/nas/system\\_standards/](http://www.faa.gov/air_traffic/nas/system_standards/)
2. FAA–STD–064, Web Service Registration  
[http://www.faa.gov/air\\_traffic/nas/system\\_standards/](http://www.faa.gov/air_traffic/nas/system_standards/)
3. FAA–STD–065, Preparation of Web Service Description Documents  
[http://www.faa.gov/air\\_traffic/nas/system\\_standards/](http://www.faa.gov/air_traffic/nas/system_standards/)
4. FAA–STD–066, Web Service Taxonomies

### 2.2 Non-Government Documents

1. Web Services Description Language (WSDL) 1.1 W3C Note 15, March 2001  
<http://www.w3.org/TR/wsdl>
2. Web Services Description Language (WSDL) Version 2.0 W3C Recommendation 26, June 2007  
<http://www.w3.org/TR/wsdl20>
3. Web Service Description Requirements, W3C Working Draft, J. Schlimmer, 28 October 2002  
<http://www.w3.org/TR/2002/WD-ws-desc-reqs-20021028/>
4. World Wide Web Consortium (W3C) Web Services Description Language (WSDL)  
<http://www.w3.org/2002/ws/desc/>
5. W3C XML Schema  
<http://www.w3.org/XML/Schema>
6. Web Services Policy  
<http://www.w3.org/2002/ws/policy/>
7. ITWS SWIM Segment 1 Baseline Architecture Design, Version 1.8, September 22, 2009.
8. SWIM-ITWS Segment 1 Comprehensive Users' Guide Winter 2011 Release, Version 1.1, January 11, 2011.

## 3. Definitions

### 3.1 Terms and Definitions

#### 3.1.1 Client

A client is an external entity that interacts with a service. Typically a client makes a request of a service and receives a response from the service. The client may also request a subscription and receive messages when a service publishes information. A client may be a software system, software application, or another service.

#### 3.1.2 Service

The SWIM-ITWS System offers a common Subscription Service for all supported ITWS products. A defined request must be provided by the client that invokes the service, and the service returns a defined response to the client. The client will then use this response to subscribe to the SWIM-ITWS streaming weather data.

#### 3.1.3 Service Contract & Registry

A WSDL contract is defined that identifies the interface for the SWIM-ITWS Subscription service. The definition includes the input message format, the output message format, the location of the service, and other information that supports the definition. This information is available in the SWIM Services registry (NSRR). In the SWIM-ITWS system, the SWIM-ITWS Subscription Service is a SOAP-over-HTTP Request/Response Web service allows users to subscribe to the SWIM-ITWS Streaming Weather Data which follows a Publish/Subscribe pattern.

#### 3.1.4 Service Provider

A service provider is the entity that establishes, manages, and operates one or more services. In the context of this effort, ITWS is always the service provider and is never the client.

## 3.2 Abbreviations and Acronyms

API	Application Programming Interface
ARTCC	Air Route Traffic Control Center
COTS	Commercial Off-the-shelf
ERAM	En Route Automation Modernization
FEP	Front-end Processor
GML	Geography Mark-up Language
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
ITWS	Integrated Terminal Weather System
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol
MEP	Message Exchange Pattern
NAS	National Airspace System
NESG	NAS Enterprise Security Gateway
NSRR	NAS Services Registry and Repository
OGC	Open Geospatial Consortium
SOA	Service-oriented Architecture
SOAP	Simple Object Access Protocol
SvSD	Service Spécification Document
SWIM	System Wide Information Management
TCP/IP	Internet Protocol Suite
UDDI	Universal Description, Discovery and Integration
UML	Unified Modeling Language
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WMSCR	Weather Message Switching Center Replacement
WSDD	Web Service Description Document
WSDL	Web Service Description Language
WXXM	Weather Information Exchange Model
XML	eXtensible Mark-up Language

## 4. Web Service Properties and Capabilities

One of the main considerations for all ITWS-derived applications (including ITWSWeb) is that data has a strictly defined ‘freshness’ time, and data should not be displayed if it is stale. This reduces the chance of stale data being misinterpreted as fresh data. Some of the products’ ‘freshness’ times are relatively short: some data expire after 30 seconds. When developing derivative applications from this real-time data, you should pay particular attention to the expiration times that accompany every ITWS message.

### 4.1 Service Profile

The SWIM-ITWS services will provide clients with the ability to subscribe to a variety of supported SWIM-ITWS products. For the complete list of SWIM-ITWS products please refer to the SWIM-ITWS Comprehensive User Guide.

The service namespace is [urn:us:gov:dot:faa:weather:itws]

#### 4.1.1 Service Provider

The SWIM-ITWS System is being developed by the Department of Transportation’s Research and Innovative Technologies Administration’s (RITA) Volpe National Transportation Systems Center (VNTSC) in Cambridge, Massachusetts.

##### 4.1.1.1 Point of Contact

The point of contact for SWIM-ITWS Web Services is:

Name:	Tony Colon
Organization:	Volpe National Transportation System Center
Title:	Manager, SWIM ITWS Development Team
Phone:	(617) 494– 2647
Email:	tony.colon@dot.gov

#### 4.1.2 Service Consumers

Available through the FAA SWIM Program Office.

#### 4.1.3 Service Functionality

The SWIM-ITWS System offers a common SOAP-over-HTTP Subscription Web Service for all supported ITWS products. The client that invokes the service must provide a defined request. The request will include the subscription information for the ITWS product data that the client is subscribing to. The service returns a defined response to the client which includes the Publish/Subscribe (JMS) endpoint corresponding to the requested subscription. The client will then use this response to connect to the SWIM-ITWS Message Broker and consume the SWIM-ITWS streaming weather data.

#### 4.1.4 Security

##### 4.1.4.1 Roles

Not Applicable

##### 4.1.4.2 Access Control Mechanisms

Access to SWIM Services is constrained to recognized and trusted systems based on the IP addresses of each incoming request. The System allows only authorized clients to connect to and consume data. For more details on this please refer to the “How To Connect” section of the SWIM-ITWS Comprehensive User Guide. Role based authentication and authorization is not applicable to SWIM-ITWS Services.

##### 4.1.4.3 Security Policies

The SWIM-ITWS System requires all clients to use a secure FTI VPN connection. Additionally the SWIM-ITWS Services will check the IP address of each incoming request and allow only authorized clients to connect to and consume data. For more details on this please refer to the “How To Connect” section of the SWIM-ITWS Comprehensive User Guide. Role based authentication and authorization is not applicable to SWIM-ITWS Services.

#### 4.1.5 Quality of Service

See the System Wide Information Management (SWIM) Final Program Requirements Appendix Segment 1 ITWS Publication Capability, January 11, 2008 for specific quality of service information.

#### 4.1.6 WSDL documents

The SWIM-ITWS Subscription Web Service WSDL and Schema are listed below.

The following is excerpted from the SWIM-ITWS Segment 1 Comprehensive Users' Guide Winter 2011 Release, Version 1.1, January 11, 2011, Chapter 5, How to Connect, Section 5.2, WSDL and Schema for ITWS Subscription Web Service.

*Please note: Per FAA guidelines the actual IP address of the SWIM-ITWS Operational Server has been replaced with "XX.XX.XX.XX" in this document.*

```
<?xml version="1.0" encoding="UTF-8"?>
<wsdl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:http="http://schemas.xmlsoap.org/wsdl/http/"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:itws="http://faa.dot.gov.us/weather/itws"
xmlns:itwsdata="urn:us:gov:dot:faa:weather:itws" name="retrieve-itws-subscription-wsdl"
targetNamespace="http://faa.dot.gov.us/weather/itws">
  <wsdl:documentation>SWIM ITWS Subscription Service </wsdl:documentation>
  <wsdl:types>
    <xs:schema
      <xs:import namespace="urn:us:gov:dot:faa:weather:itws"
schemaLocation="RetrievalItwsSubscriptionDataModel.xsd"/>
    </xs:schema>
  </wsdl:types>
  <wsdl:message name="ItwsSubscriptionRequestMessage">
    <wsdl:part name="itwssubscriptionrequestpayload" element="itwsdata:ItwsSubscriptionRequest">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="ItwsSubscriptionResponseMessage">
    <wsdl:part name="itwssubscriptionresponsepayload"
element="itwsdata:ItwsSubscriptionResponseElement">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="ItwsSubscriptionFaultMessage">
    <wsdl:part name="itwssubscriptionfaultpayload" element="itwsdata:ItwsSubscriptionFaultElement">
    </wsdl:part>
  </wsdl:message>
  <wsdl:portType name="ItwsSubscriptionPortType">
    <wsdl:operation name="ItwsSubscriptionRequest">
      <wsdl:input message="itws:ItwsSubscriptionRequestMessage"/>
      <wsdl:output message="itws:ItwsSubscriptionResponseMessage"/>
      <wsdl:fault name="ItwsSubscriptionFault" message="itws:ItwsSubscriptionFaultMessage">
    </wsdl:fault>
    </wsdl:operation>
  </wsdl:portType>
  <wsdl:binding name="ItwsSubscriptionSOAPBinding" type="itws:ItwsSubscriptionPortType">
    <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
    <wsdl:operation name="ItwsSubscriptionRequest">
      <soap:operation soapAction="" style="document"/>
      <wsdl:input>
        <soap:body use="literal"/>
      </wsdl:input>
      <wsdl:output>
        <soap:body use="literal"/>
      </wsdl:output>
      <wsdl:fault name="ItwsSubscriptionFault">
    </wsdl:fault>
  </wsdl:operation>
</wsdl:binding>
</wsdl:definitions>
```

```

        <soap:fault name="ItwsSubscriptionFault" use="literal"/>
    </wsdl:fault>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="RetrieveItwsSubscription">
    <wsdl:port name="soap" binding="itws:ItwsSubscriptionSOAPBinding">
        <soap:address location="http://XX.XX.XX.XX:8192/RetrieveItwsSubscription"/>
    </wsdl:port>
</wsdl:service>
</wsdl:definitions>

<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2010 rel. 2 (http://www.altova.com) by Patricio O Colon (DOT) -->
<xs:schema xmlns:itwsdata="urn:us:gov:dot:faa:weather:itws"
xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="urn:us:gov:dot:faa:weather:itws"
elementFormDefault="qualified" attributeFormDefault="qualified">
    <xs:complexType name="ItwsSubscriptionRequestType">
        <xs:sequence>
            <xs:element name="ItwsSubscriptionId" type="xs:string"/>
            <xs:element name="ItwsProductId" type="xs:string"/>
            <xs:element name="ItwsMode" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ItwsSubscriptionResponseType">
        <xs:sequence>
            <xs:element name="ItwsUrl" type="xs:string"/>
            <xs:element name="ItwsDestination" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ItwsSubscriptionFaultType">
        <xs:sequence>
            <xs:element name="ItwsFault" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
    <xs:element name="ItwsSubscriptionRequest" type="itwsdata:ItwsSubscriptionRequestType"/>
    <xs:element name="ItwsSubscriptionResponseElement" type="itwsdata:ItwsSubscriptionResponseType"/>
    <xs:element name="ItwsSubscriptionFaultElement" type="itwsdata:ItwsSubscriptionFaultType"/>
</xs:schema>

```

## 4.2 Service Interfaces

The following sections describe the SWIM-ITWS web services in terms of the interfaces used to communicate with them. The messages and operations are detailed along with the data types used in the messages. The tables in the following sections describe the data types used in the SWIM-ITWS service messages.

### 4.2.1 Types

The Data Types for the SWIM-ITWS Subscription Service are defined in the **RetrievalItwsSubscriptionDataModel.xsd** schema listed above. Please see the Types column for explanation of each of these types in the next section.

### 4.2.2 Messages

The following messages are supported in the SWIM-ITWS Subscription message:

**ItwsSubscriptionRequestMessage**

**ItwsSubscriptionResponseMessage**

**ItwsSubscriptionFaultMessage**

Each message is further described in the tables below

#### 4.2.2.1 **ItwsSubscriptionRequestMessage**

	<b>Web Service Input Parameters</b>	<b>Data Type</b>	<b>Allowed Values</b>
1.	ItwsSubscriptionId	String	An alphanumeric string that contains a valid ITWS Subscription Id. Possible values for SubscriptionId's are provided in the table below
2.	ItwsProductId	String	This field is currently not used and reserved for future use
3.	ItwsMode	String	The possible values are XML, ZIP and OGC XML - returns the data stream in Canonical ITWS XML format ZIP – will return the data in ZIP format OGC – will return the data in OGC format

#### 4.2.2.2 ItwsSubscriptionResponseMessage

	Web Service Response Values	Data Type	Values
1.	ItwsUrl	String	URL for the JMS Broker, which contains the JMS endpoint for the subscription. For example: tcp://11.22.11.22:61616
2.	ItwsDestination	String	JMS Destination for Subscription. For example, ATL.HOTSPOTS.OUT, or ITWS.NIECFLOW.ZIP.OUT

#### 4.2.2.3 ItwsSubscriptionFaultMessage

	Fault Condition	Fault Message
1.	ItwsSubscriptionId was null or empty	Itws Subscription Id was null or empty
2.	ItwsMode did not contain a value of either "XML", "OGC", "ZIP"	Itws Mode was invalid: <mode value requested by client>
3.	The IP address of the client was not recognized by the SWIM-ITWS System	Security Failure - IP Address not allowed

#### 4.2.2.4 Possible values for SubscriptionId

Any of the following values may be provided for **SubscriptionId**

HOTSPOTS – this is a JMS Endpoint (Topic) for all sites

<ITWS-SITE>.HOTSPOTS – where <ITWS-SITE> is a specific ITWS Sitename. An example would be ATL.HOTSPOTS.

ITWS.<custom-subscription>– where .<custom-subscription is a custom subscription defined by the SWIM-ITWS team at request of a consumer with custom subscription requirements.

### 4.2.3 Operations

The following operation is supported in the Service:

#### **ItwsSubscriptionRequest**

### 4.2.4 List of Interfaces

The SWIM-ITWS Subscript on Web Service supports a single interface, namely, **RetrieveltwsSubscription**. The Operations, Messages and Types for this Interface have been described in the preceding sections.

### 4.2.5 Endpoint — Retrieveltws Subscription

#### **4.2.5.1 Associated Interface**

The **RetrieveltwsSubscription** endpoint is associated with the **RetrieveltwsSubscription** interface.

#### **4.2.5.2 Communication Protocol**

The endpoint communication protocol is HTTP.

#### **4.2.5.3 Messaging Protocol**

The messaging protocol is SOAP. Operational messaging data sent over SWIM is independent of operating systems and programming languages, and conforms to a predefined schema for communicating with the SWIM-ITWS services. Messaging data is encoded using XML.

#### **4.2.5.4 Network Address**

The network address is **XX.XX.XX.XX:8192/RetrieveltwsSubscription**. Please note: Per FAA guidelines the actual IP address of the SWIM-ITWS Operational Server has been replaced with “XX.XX.XX.XX” in this document. The actual address may be obtained by authorized users who have access to the SWIM Registry (NSRR)

## Appendix A. Connecting Clients to the SWIM-ITWS Web Service

The following is excerpted from the SWIM-ITWS Segment 1 Comprehensive Users' Guide Winter 2011 Release, Version 1.1, January 11, 2011, Chapter 5, How To Connect

### A.1 How to Connect

#### A.1.1 SWIM-ITWS Sample Java Client and Test Tool

##### Instructions on Installation and Configuration

The SWIM-ITWS Sample Java Client and Test Tool package contains source code and configurations for a sample Java Client that can be run from the command line on either Windows or Linux systems.

When run, it connects to the SWIM-ITWS Subscription Web Service which resides on the SWIM-ITWS Operational server to retrieve a JMS end-point. It then connects to the JMS endpoint, which resides on a SWIM-ITWS Message Broker, to read streaming weatehr data for the subscription and displays XML data on screen.

The client reads in a configuration file at start up and its run-time behaviour can be modified by changing the configuration file.

##### Steps to install the client

1. Copy the contents of the distribution itws-test-tool-vXX.zip into a Windows or Linux system which has been configured and authorized to connect to the SWIM-ITWS operational services and message broker.
2. Open a command window and change the directory to the location of the above folder.
3. Execute the following command

On Windows:

```
$ run-sips-client.bat
```

On Linux/Unix

```
# ./run-itws-client.sh (you may need to modify the permissions to permit execution)
```

4. The client should start up and connect to the SWIM-ITWS Prototype Service and read data from the JMS Topic called HOTSPOTS.ZIP.OUT. XML data should be displayed on the screen.

##### Configurations

The default subscription behavior of the client can be altered by modifying the file **client/sipsclient.props**. Please see the comments in this file for an explanation of each configuration option.

## **A.2 Information we need from our users**

We need the following information from you, prior to enabling your VPN connectivity:

1. Public IP address of VPN termination point.
2. Public IP address(es) of client machines.
3. (Optional) Public IP address of ping-able machine to be used to determine the state of the VPN.
4. Contact information for application user representative(s).
5. Contact information for the network administrator(s).
6. Hardware and Software to be used at the VPN termination point.
7. Your IT environment preferences (e.g. Microsoft and .NET, SunOS and Java, Oracle and JDeveloper etc.).

### **A.3 VPN Information**

The following text is excerpted from an previous version of the FTI External User Connectivity Guide. The FTI External User Connectivity Guide has been revised (the current version is ....) The excerpted sections included here provide a general overview of the processes and requirements for connecting to the SWIM-ITWS prototype. To obtain a copy of the current document detailing connectivity options, contact the Volpe Center SWIM-ITWS point of contact:

Tony Colon

55 Broadway

Cambridge, MA 02142

Email:

Tony.Colon@dot.gov

(Office) 617 494-2647

(Cell) 857 366-0165

(Excerpted information follows:)

## Getting Connected

The basic process for getting connected via an ED8 extranet gateway service includes:

1. Complete Initial Planning:

- Work with FAA sponsor program to gather the necessary information on the application operation including Interface Control Documents (ICDs) and other guidance material.
- Determine the preferred method for attaching to the ED8 gateway (see the section below for more detail).
- Exchange IP address information and concept of operations data (with NAS sponsor program and TSG engineers) necessary to configure the access and allow the application to connect to the ED8 gateway. This data will be documented via the FAA “IP Supplemental Form”.

Verify extranet VPN equipment for compatibility with ED8 gateway.

Complete and return any required program MOA/MOU.

2. Establish Connection:

- Work with the FTI Vendor (Harris) Ops IP staff to configure the access (VPN tunnel or DTS) between the external system access device and the FAA ED8 extranet gateway.

**Note:** the following section, “3. Get Certified” will not be required

3. Get Certified:

- In some cases, it will be necessary to certify your system before it is allowed to communicate with FAA operational (NAS) systems. This may be accomplished by connection to an interim test system. This step is FAA sponsor program dependent and often includes interoperability testing with the FAA sponsor program.

4. Begin Operation:

- Once the FAA application sponsor grants permission to operate, you will be allowed the appropriate access to exchange data. Please see section below “Support Concept” for additional information concerning steady state operations.

## Gateway Connectivity Options for External Users

The ED8 gateway provides for three different methods of attachment. They are described below:

### 1. Internet Based Virtual Private Network (VPN)

This method utilizes public networks, such as the Internet as a transport mechanism only. Connections between the external user and the ED8 gateway are secured using Virtual Private Networking based on IPSec. The section below entitled “VPN Technical Requirements” provides further detailed information. In this connection model the FAA provides the public Internet connection for the ED8 gateway. This enables an extranet connection mechanism with no external user equipment at the FAA ED8 gateway.

### 2. User Provided Dedicated Transmission Service (DTS)

This method allows an external user to provide a dedicated circuit and attach it to the ED8 gateway. The FAA provides T1/E1 interfaces (RJ-48C) integrated with the gateway to accommodate this type of connection. No equipment should exist at the FAA gateway location beyond the digital demarc (CSU/DSU equipment is integrated into the FAA gateway).

The following Carrier Services are supported:

- Private Line/Dedicated Transmission Service
- Frame Relay
- IP (carrier based MPLS VPN only)

The following Layer 2 encapsulation methods are supported:

- Cisco HDLC
- PPP
- Frame Relay Encapsulation

In order to provision a circuit up to the ED8 Gateway, the following information will be provided upon request to the external user: E911 address of the gateway, the building / room number of the digital demarc and the local point of contact for installation logistics.

The external user must support IPSec on DTS interfaces. The use of IPSec satisfies authentication requirements. See the section below entitled “VPN Technical Requirements” for detailed information. The use of VPNs on DTS interfaces also serves to provide a logical separation of FAA domains.

### 3. Local Ethernet Connection

This method is reserved for systems with an established point of presence physically collocated with the ED8 gateway. The gateway provides a standard LAN Ethernet switch to accommodate LAN-based connections.

**Note:** The FAA does not provide rack space, power or administrative support for external user-owned equipment. As such, this method is not suitable for external users preferring to install a user-managed router at the ED8 gateway at this time.

## VPN Technical Requirements

To establish and operate an access VPN service to the ED8 extranet gateway, external users must comply with all security configurations as well as be compatible with ED8 gateway equipment. IPSec encompasses a suite of protocols, however the FAA reserves the right to dictate particular choices to meet best practices and security mandates. In general, to establish extranet services users must:

- Provide one or more fixed public IP addresses for the access VPN to the gateway (to be provided via the IP Supplemental form for external end-users). It is the responsibility of the NAS sponsor program to provide the data, but it is the responsibility of the external user to coordinate with both the NAS sponsor program and the TSG engineering staff to obtain all required information and configure the access VPN tunnel.
- Comply with standard ED8 access VPN service / IPSec settings:
  - Encapsulation Security Payload (ESP)
  - Encryption: AES-256
  - Authentication: SHA-1
  - IPSec / IKE Authentication: Pre-shared secret and digital certificate
  - IKE phase 1: Diffie-Hellman group 5
  - Perfect Forward Secrecy (PFS): Diffie-Hellman group 1
  - Pre-shared secret key (to be exchanged at the time of VPN establishment)

**Note:** Ops IP Network does not use simplified mode, aggressive mode or VPN communities for ED8 access VPN tunnels.

- Conservatively configure security settings to permit only the required application traffic. The IP source, destination, and ports must be fully specified.

Example:

Client source IP:	x.x.x.x
Destination IP (Server):	y.y.y.y
Destination TCP Port:	3000

- Prohibit all other access.

## Equipment Compatibility

All ED8 access VPN tunnels created between the FAA and external end-user systems are based on IPSec. Vendor implementation variances could result in compatibility problems even though IPSec is an open suite of standards (see RFC 2401 for general information). The likelihood of vendor incompatibility has diminished significantly over the last several years.

Cisco appliances are used to decrypt/terminate ESP IPSec tunnels between the FAA and external users. Below is the vendor documentation listing its compatibility with other Cisco products as well as known alternative vendors for this functionality. The lists may not be complete and should not be regarded as mandatory. It is provided simply as a courtesy to potential end-users.

**PLEASE NOTE:** You should check that the product selected meets the minimum VPN Technical Requirements specified earlier in this document.

### Site-to-Site VPN Compatibility Between FTI Cisco Appliance and Other VPN Products

VPN Gateway	Versions Supported
Cisco ASA 5500 Series Appliances	Cisco ASA Software Version 7.0(1) and later
Cisco IOS Software Routers	Cisco IOS Software Release 12.1(6)T and later
Cisco PIX Security Appliances	Cisco PIX Security Appliance Software Version 6.0(1) and later
Cisco VPN 3000 Series Concentrators	Cisco VPN 3000 Series Concentrator Software Version 3.0 and later

The following products have been tested successfully by Cisco with the FTI selected Cisco Appliance for Key exchange and ESP encryption. This list will change over time as addition products are tested. You may wish to check with Cisco for the most recent list of tested products.

<b>VENDOR</b>	<b>PRODUCT</b>	<b>PRODUCT VERSION</b>	<b>OPERATING SYSTEM</b>
Check Point Software	*Checkpoint VPN-1/Firewall-1 NGX on SecurePlatform	R60	Customized Linux
Check Point Software	Checkpoint VPN-1/Firewall-1 NGX on SecurePlatform	R60 HFA03	SecurePlatform
Cisco Systems	Cisco 87x & 18X Integrated Service Routers	12.4(6)T2	Proprietary
Cisco Systems	*Cisco IOS Router Family Vers 12.4(1a)	12.4(1a)	Proprietary
Cisco Systems	Cisco IOS Router Family Vers 12.4(6)T	12.4(6)T	Proprietary
Cisco-Linksys	BEFVP41	2.0	Proprietary
FortiNet Inc.	FortiGate Family of Antivirus Firewalls	2.80	FortiOS V2.8
Huawei-3com	*Quidway SecPath Security Gateway Family	3.30	Proprietary
Intoto Inc.	iGateway	3.3SP1P25	Proprietary
Juniper Networks	Netscreen Security Gateway Product Group	5.0.0r4	Proprietary
Lucent Technologies	*Lucent VPN Firewall IPsec Product Group	8.0.302	Proprietary
Lucent Technologies	Lucent VPN Firewall IPsec Product Group	8.0.396	Proprietary
Secure Computing Corporation	Sidewinder G2 Firewall	6.1.0.00	Proprietary
Stonesoft Corporation	StoneGate Firewall	2.61	Customized Linux
TippingPoint, a division of 3Com	TippingPoint X505	2.2.4.6517	Proprietary