

FAA Telecommunications Infrastructure (FTI) NAS Boundary Protection System (NBPS)

User's Guide

Volume II- For Non-NAS Users



Telecommunications Services Team (TST), ATO-W

Federal Aviation Administration

*Revision 5
August 2013*

Table of Contents

1	Purpose.....	1
2	Roles and Responsibilities	2
2.1	External (Extranet) End-User	2
2.2	FAA Sponsor Program.....	2
2.3	FAA Telecommunications Services Team (TST).....	3
2.4	FAA Telecommunications Infrastructure (FTI) Vendor.....	3
3	Service Connection Establishment Process	5
3.1	Service Planning and Design	5
3.2	Service Interoperability Testing.....	6
3.3	Service Operational Connection Establishment.....	6
3.4	In-Service Operations	7
4	Gateway Connectivity Options for External Users.....	8
4.1	User-provided Dedicated Transmission Service (DTS)	8
4.1.1	User-Provided DTS – Ethernet Interface.....	9
4.1.2	User-provided DTS – Serial Interface	9
4.2	Internet-Based Virtual Private Network (VPN).....	10
4.3	Private Network Based Virtual Private Network (VPN)	10
4.4	External Service Connection Recommendations.....	11
5	External End-User Security Responsibilities.....	13
6	Support Concept.....	14
7	VPN Technical Requirements.....	14
8	Equipment Compatibility.....	14

List of Figures

Figure 1-1:	End-to-End Connection through a NAS Enterprise Security Gateway	1
Figure 3-1:	External Service Connection Provisioning Process	5
Figure 4-1:	External Connection Options to NAS Boundary Protection System (NBPS)	7
Figure 4-2:	Recommended External Connection Approach for Critical Services.....	11

1. Purpose

This document provides guidance to external system owners for provisioning IP-based service connectivity to a National Airspace System (NAS) system. For the purposes of this document any user/system not in the FAA’s NAS security domain is considered an external system. External connections to the NAS require boundary protection security controls as defined in FAA Order 1370.114 and associated guidance documentation. The FAA has established a NAS Boundary Protection System (NBPS) to implement required security controls. This guide identifies the steps required of External Users to interact with NAS systems via the NBPS.

1.1 Scope

Contents of this guide include:

- Methodology for initiating, tracking and controlling external NAS service connections.
- Administrative and technical processes and procedures associated with ordering and provisioning service connections between external entities and NAS programs.

1.2 Overview

The NBPS infrastructure provides a framework for supporting mandated security controls between NAS and non-NAS entities. It provides a standardized scheme for connecting and managing connections to external users, based on a layered security approach for implementing defense in depth. Direct external connections to NAS systems are prohibited by FAA security policies. The NBPS framework includes a buffer zone between NAS systems and external entities. At the writing of this guide, the NBPS infrastructure is limited to IP-based services.

The NBPS infrastructure includes: four NAS Enterprise Security Gateways (NESGs); a dedicated NBPS network for inter-gateway interactions (forming an NBPS external enclave); and two Internet Access Points (IAPs). NBPS operations enforce a layered security scheme and defense in depth security controls creating an information buffer within the external enclave that inhibits direct service connections between external entities and NAS systems. The External Interfaces of the four NESGs are the only authorized points of ingress to the NAS for external entities. NBPS interface and connection features described in this and related documents often use the terms NESG and NBPS inter-changeably, since the individual NESG gateways are the access points to NBPS capabilities. Figure 1-1 depicts authorized external connection options between a NAS system and an external system via an authorized NBPS egress point.

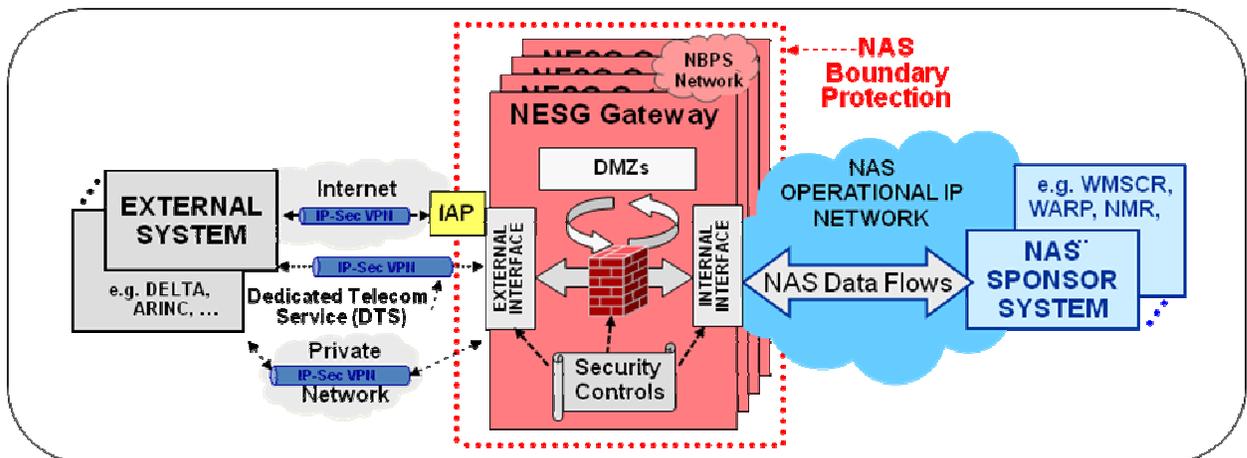


Figure 1-1: End-to-End Connection through a NAS Enterprise Security Gateway

2 Roles and Responsibilities

2.1 External (Extranet) End-User

An external end-user is a non-NAS organization that provides and/or consumes NAS data. External systems must comply with all FAA policies and technical requirements. External system owners must execute (sign) a Memorandum of Agreement (MOA) with the FAA. Associated NAS Sponsor programs define security controls to be used and list external users in an Interconnection Security Agreement (ISA) as required by FAA Order 1370.114. MOAs define business and service level agreements. ISAs define security controls used to manage external interfaces and connections. It is recommended that external organizations appoint a single point of contact to manage and oversee service connectivity to the NAS. This is particularly important if an external organization has multiple entities involved in the operation of the NAS interface and in cases where interfaces to multiple NAS systems may be required. Recommendations are that external entities evaluate all data flow needs it has with any NAS system and design a shared/common interface to the NBPS that is amenable to all of its needs.

2.2 FAA Sponsor Program

NBPS External Services provide a connection between a NAS system and an external entity. It is the responsibility of the NAS system participating in an external connection to act as the “Sponsor Program” for the external system, for legacy (non-SOA) IP services. These systems are referred to as a NAS Sponsor Programs (NAS-SP). NAS-SPs must adhere to the requirements in FAA Order JO 1370.114 for external boundary protection requirements for NAS systems that interface with external (non-NAS) systems. NAS-SPs manage the “application space” and data for all legacy external IP services. NAS-SPs act as the champion for establishing end-to-end connectivity to their external users.

Moving forward, the NEMS infrastructure (managed by AJM-312) is the NAS-SP for external users that leverage SOA services via the NEMS infrastructure and will act as the Point of Contact for all external access to NEMS services. External SOA service connections are enacted via the NBPS infrastructure in the same manner as legacy IP services since the SOA services are provisioned via an IP connection to the NAS. As mentioned in the previous paragraph it is recommended that an external entity develop a robust interface to the NBPS to handle all interactions with NAS systems; this is true of all SOA services as well as legacy IP services.

The NAS-SP (be it a specific NAS system for legacy IP services or AJM-312 for SOA services) provides application details (such as outreach briefings, service descriptions and ICDs) for the exchange of technical data required to establish an external service connection. The NAS-SP is also responsible for certifying the data quality, ensuring NAS system integrity and ultimately obtaining authorization to connect the external system to the NAS for releasing NAS data.

Summary: It recommended that a single set of shared connections between an external user and the NBPS be shared across multiple NAS systems, for both Legacy IP and SOA services. That is, if an external organization requires connections with multiple NAS systems, the various application layer services can and should be implemented over a shared IPsec VPN, implemented over the Internet or via DTS based connections. For cases in which the external interactions require availability greater than that of a single external connection (typically with an availability of .998 or less) a set of connections to multiple NBPS ingress points is

recommended. Various methods of connection control and associated service failover procedures are supported by the NBPS in conjunction with the NAS-SP; these procedures are dependent on the design and concept of operation (CONOPS) of the NAS-SP. This document provides guidance on allowable external connection alternatives to the NBPS, but external users are encouraged to interact with the NAS-SP providing the service to develop an agreed upon service CONOPS for a particular service flow.

2.3 Enterprise Engineering Services (AJM-312)

The Enterprise Engineering Services team of the Communication, Information and Network Programs (CINP) Division provisions and manages NAS telecommunications and NEMS messaging services for the FAA including those coming through the NAS Boundary Protection System (NBPS). CINP accepts external service connection requests from services provided by a NAS Sponsor Program (NAS-SP) and works with the Sponsor PO (and the external system owner as required) to define the required external service requirements:

1. Connection requirements of NAS-SP to the internal side of the NBPS ingress points (NAS Enterprise Security Gateway, NESG, internal interface), including:
 - a. Coordination of any new or modified NAS-SP system connections to the Internal DMZ of a NESG.
 - b. Configuration Management of all services offered via the connection.
 - c. All application layer data flows associated with each of the offered services.
 - d. For new external user connections to an existing NAS service this could reduce to configuration management of the NAS-SP IP Supplemental Form.
2. Connection requirements of external user/program to the external side of the NBPS ingress points (NESG external interface), including:
 - a. Coordination of any new or modified IP connection to the NBPS
 - b. All external application layer data flows associated with any NAS service being provisioned.
 - c. Coordination and configuration management of the CONOPS of any new service flow agreements with external users.
3. Security control requirements of the gateways and any required NBPS data flows between NESGs required for permitting desired information flows.
 - a. Coordinate with ISS Security (at service design time) to ensure all NAS-SP interactions with external users are via approved security controls.
 - b. Coordinate with NAS Data Release office to ensure all NBSP interactions with external users are approved for NAS information release.

Once the end-to-end service connection is understood, documented, approved (AODR approval for NAS-SP and NDRB for external entities) and funded, AJM-312 submits service orders for the required external service connectivity and any required external onramping services.

2.4 FAA Telecommunications Infrastructure (FTI) Vendor

External connections to the NBPS points of ingress are installed and operated by the FTI Vendor (Harris) and include all IP external connections to the external interface of an NESG and any required SOA onramping service.

Once external gateway services are requested and approved, the FTI Vendor will work directly with the external system technical staff to establish, configure and verify connectivity to the NBPS and subsequent application layer SOA interactions with SWIM.

For legacy IP service interactions, the Harris Ops IP staff operates the network level connection support services only, and is not involved in the design or specification of application layer services (this function is provided by the legacy IP NAS-SP). The external connection coordination function is supported by the NAS Service Connection Establishment Process as described in Section 3.

3 Service Connection Establishment Process

The basic process for provisioning external service interfaces to legacy IP NAS services via the NAS Boundary Protection System is outlined in the process flow depicted in Figure 3-1. The process includes three service phases:

- Planning and Design
- Interoperability Testing
- Implementation

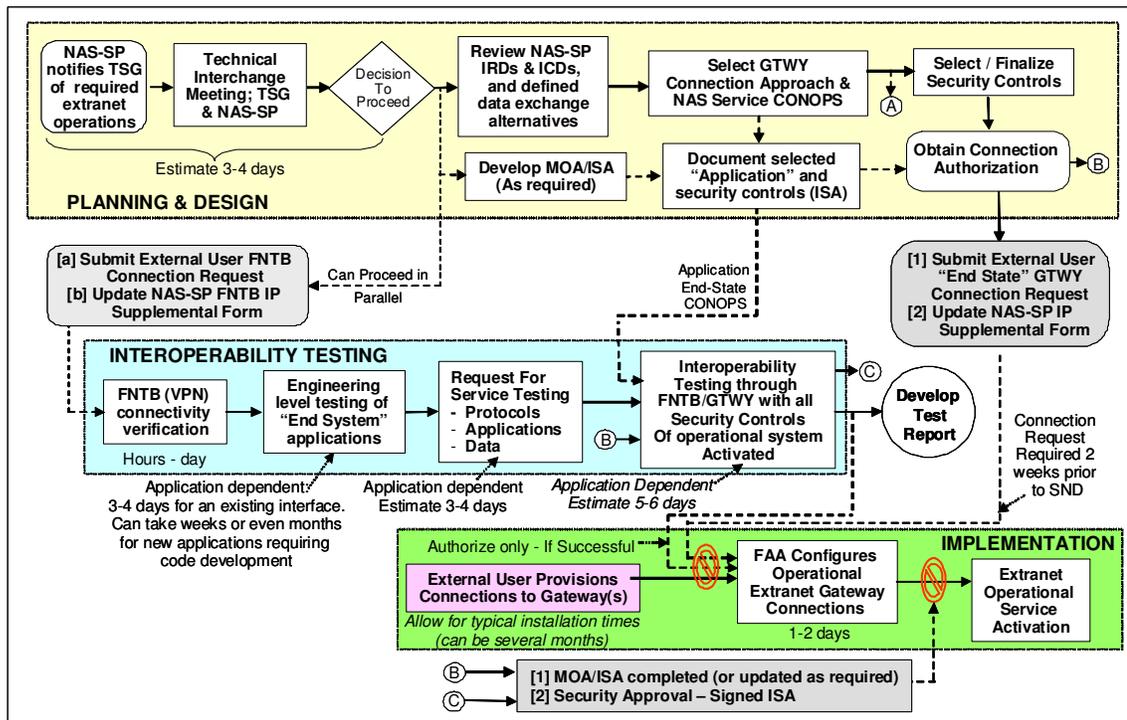


Figure 3-1. External Service Connection Provisioning Process

3.1 Service Planning and Design

For NAS-SP Program service initiation (including new NEMS Business Service Onramping):

- Coordinate with the NAS Sponsor program, any associated data stewards, AJM-312, AODR security office and NAS Data Release Office to clarify:
 - Classification of NAS data including data sensitivity ranking
 - Security control available (e.g. filtering, time delay, etc.)
 - Required service flows and associated connectivity requirements
 - Decision to proceed with extranet service provisioning including
 - POCs for subsequent activities
 - Roles and responsibilities
- Follow-on coordination with NAS-SP and data stewards to gather any necessary information on the application operation including Interface Control Documents (ICDs), Concept of Operations and other guidance material.
 - Develop a draft project plan for tracking critical activities

- Documentation of system architecture, integration with NBPS and available security controls in an ISA
- Follow-on coordination with NAS-SP and NDRB to determine release-ability of NAS data to various external user classes and associated security controls required per class.

For External Entity Requests to access an available NAS data service:

- Identify the external entity user class and verify release-ability of requested data to that user class and associated constraints and required security controls
- Determine the preferred method for attaching to an Enterprise Security gateway (see the section below for more detail on available options) and concept of use.
- Complete and return any required program Request for Service, MOA, NAS data release Request (Form 1200.5) and/or other documentation as required.
- Verify extranet VPN equipment compatibility with Enterprise Security Gateway.
- Exchange IP addressing information necessary to configure the access and allow the application to connect to an Enterprise Security Gateway.
 - Develop service request data for both end-state services and interoperability tests.
 - Document testing service data in a FNTB Connection Request Form and IP Supplemental Form.
 - Document operational service data in Ops IP Connection Request Form and IP Supplemental Form.

3.2 Service Interoperability Testing

In most cases, it will be necessary to test and/or certify an external system before it is allowed to communicate with a NBPS egress point. This may be accomplished by connection to a test system. This step is FAA sponsor program dependent and often includes interoperability testing between their test system/application and the external system. The FTI National Test Bed (FNTB) at the William J. Hughes Technical Center (WJHTC) in Atlantic City, NJ supports testing in a fully isolated environment.

The steps to be completed in this phase include:

- Coordinate test plan and projected schedule with NAS Sponsor program and TST testing personnel. Support completion of:
 - Test bed service requests
 - Sponsor Program IP Supplemental Form
- Establish test connectivity to the Enterprise Security Gateway in the FNTB.
 - Internet VPNs are also required for testing through the security gateway
- Perform a series of interface and application testing to validate application performance and the overall operational concepts (e.g. failover scenarios). These concepts must be verified while using the FNTB gateway with all identified security controls active.
 - For NEMS/SOA services this step includes verification of both IP service operation and Layer 7 NEMS onramping service verification.

3.3 Service Operational Connection Establishment

- If DTS connectivity is being used, implement the circuits and any planned equipment at

- the chosen Enterprise Security Gateway location(s).
- Realistic lead times for provisioning new DTS services to the selected security gateway locations should be accounted for in the project schedule.
 - Work with appointed FAA onsite personnel to deploy DTS solution which may or not include CoLo equipment.
 - Work with the FTI Vendor (Harris) Ops IP staff to configure access VPNs between the external system access device and the FAA Enterprise Security Gateway.
 - Required security configurations are documented in the Sponsor Program’s IP Supplemental Form.
 - External user connections are defined in associated Connection Request Forms.
 - Work with the FTI Vendor (Harris) Ops IP staff to configure and establish an application layer External Consumer Onramping service connection to the NBPS.
 - Control gates for cutover of end-to-end operational services include:
 - A Connection Request from the NAS Sponsor program (defining any new external connections required for the new external service) must be received 2 weeks prior to the intended service acceptance date.
 - Interoperability testing of the envisioned external connections (and all required security controls) at the FNTB must be completed and documented.
 - External DTS connections to the gateway (if required) must be completed.
 - External Consumer Onramping Service operational capability verification testing
 - Activation of gateway security controls to support end-to-end data flows requires:
 - Completion, signing and delivery of all required MOA and NDRB materials by external entity, typically coordinated by AJM-312 and NAS-SP.
 - Authorization from WAN enterprise security authority.
 - NAS Sponsor Program requires authority to release NAS data (obtained by completing the ISA process during service design phase).
 - Completion and delivery of IP supplemental data (documented in a Supplemental Form) containing all services and configuration/control information.

3.4 In-Service Operations

Once the FAA grants permission to operate, an external user will be allowed the appropriate access to exchange data with the NAS Sponsor Program system/application as defined in the service agreement (MOA). See Section 6 entitled “Support Concept” for additional information concerning steady state operations.

- Coordinate troubleshooting and/or operational issues through the NAS Sponsor Program, in accordance with the agreed operations concept.

4 Gateway Connectivity Options for External Users

Enterprise Security Gateways provide three methods of attachment, as depicted in Exhibit 4-1 and described below:

1. External User-Provided Dedicated Telecommunications Service (DTS)
 - a. Implemented via an Ethernet interface with an External User Access Device (router) located at one or more NAS NBPS facilities
 - b. Implemented with a serial interface from an External User Access device located remotely at External User facilities
2. External User-Provided Internet VPN service connection
3. External User-Provided Private Network service connection

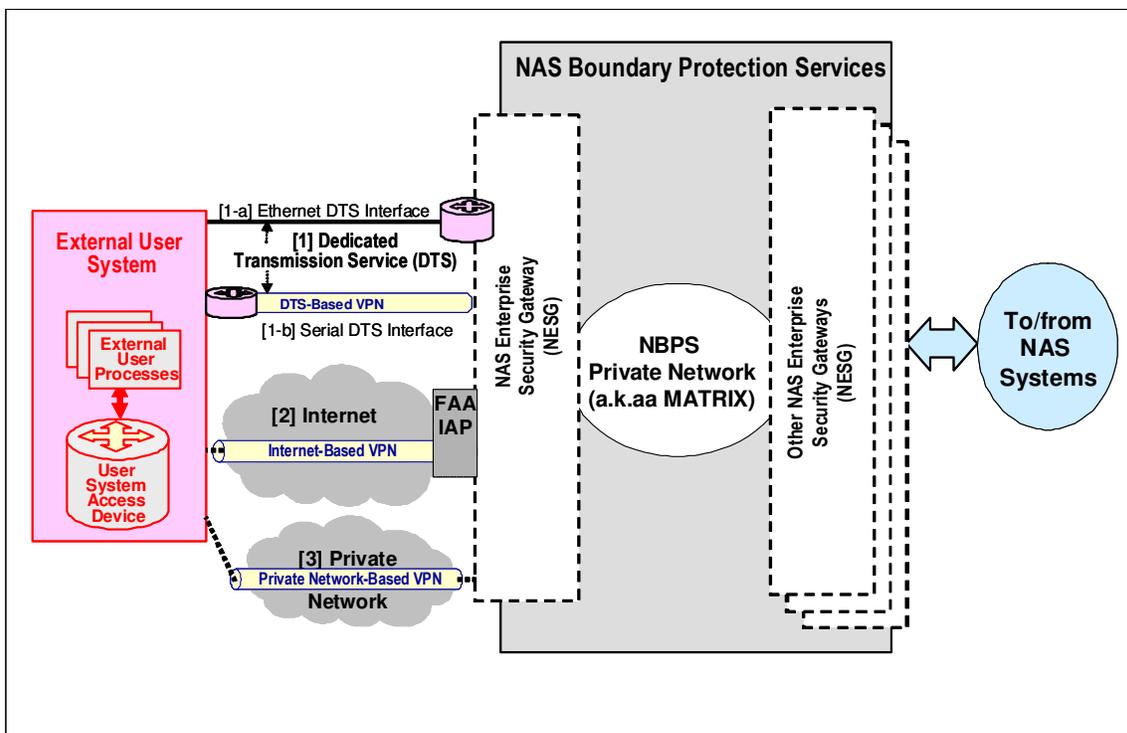


Figure 4-1: External Connection Options to NAS Boundary Protection System (NBPS)

4.1 User-provided Dedicated Transmission Service (DTS)

This method allows an external user to provide a dedicated circuit and attach it to the external interface of an Enterprise Security Gateway.

There are two approaches for supporting external DTS connections:

1. Connectivity via local Ethernet interface to external user router located within FAA facility; collocation equipment has been established to support the external routers.
2. Connectivity via serial interface to a remote external user router and the FAA NESG facility via the DTS connection.

4.1.1 User-Provided DTS – Ethernet Interface

This method allows an external user to connect to an Enterprise Security Gateway with a LAN based Ethernet interface. This method is suitable for external users with an established point of presence physically collocated with an FAA security gateway (example: user has an installed network router). The gateway provides a standard Ethernet switch (Cisco) to accommodate local LAN connections. Connections between the external user and the security gateway are secured using Virtual Private Networking based on IPsec.

The FAA permits the installation of external user equipment at FAA facilities hosting external gateways consistent with the guidelines set forth in this document. There are additional requirements pertaining to the physical installation of external user (user owned) routers at FAA facilities as follows:

- External user equipment (routers) must fit and mount in a standard 19” network equipment cabinets. The cabinet is supplied by the FAA.
- External user CSU / DSU equipment should be integrated into the routing equipment.
- External users will be allocated up to 2U of rack-mounted space for user owned equipment. Where possible, the equipment footprint should be minimized to 1U.
- External users requiring redundant equipment will be allocated an additional 2U (maximum) of rack space.
- External users must provide all mounting hardware for their equipment including; mounting ears, screws and speed clips. Shelving is not provided by the FAA.
- Storage space for “un-mounted” spare equipment is not provided to external users.
- All equipment installations shall accompany a simple network diagram indicating required cabling, interface assignments, system owner and function.
- All required cabling shall be supplied by the external user. This includes; power cords (110v/15A at 6’ minimum length), Ethernet cable between the FAA network switch and the user router (straight through configuration), and Telco cabling between the user router and the circuit provider (normally RJ-48C).
- All external user equipment shall be labeled with sufficient information to uniquely identify its owner, including but not limited to the company name, point of contact and phone number for operational support.
- User equipment must operate on electrical source power of 110V AC at 15A. The FAA makes available generator backed-up power on a best effort basis.
- External users must make arrangements for on-site physical installation of equipment. An FAA escort will be required during on-site visits.
- Phone lines (POTS) for remote dial-up access are not supplied by the FAA.
- Installation of other external user equipment (such as PCs or servers) is not permitted.

4.1.2 User-provided DTS – Serial Interface

This method allows an external user to connect a dedicated circuit to the external interface of an Enterprise Security Gateway via a serial interface. The FAA provides T1/E1 interfaces (RJ-48C) integrated with the gateway to accommodate this type of external service connection. No external user 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

T1 Interfacing Physical Specifications:

- Line code: binary 8-zéro substitution (B8ZS) per ANSI T1.408
- Line framing: extended super frame format (extended super frame (ESF) 24-frame multi frame) per ANSI T1.408

In order to provision a circuit up to an Enterprise Security Gateway, the following information will be provided upon request to the external user:

- E911 address of the gateway
- Building and room number of the digital demark
- Local point of contact for installation logistics

The external user must support IPsec on the DTS interfaces. The use of IPsec satisfies various security requirements. See Section 7 entitled “VPN Technical Requirements” for detailed information. The use of VPNs on DTS interfaces also serves to provide a logical separation of FAA domains. If an external user has a need to connect to multiple FAA/NAS systems, these service connections can (and in most cases should) share a physical connection to the security gateway.

4.2 Internet-Based Virtual Private Network (VPN)

This method utilizes the public Internet as a transport mechanism only. Connections between the external user and an Enterprise Security Gateway are secured using Virtual Private Networking based on the IPsec protocol. See Section 7 entitled “VPN Technical Requirements” for further detailed information. In this connection model the FAA provides the public Internet connection for the security gateway via an FAA managed Internet Access Point (IAP). This enables an external connection mechanism with no external user equipment at the FAA facility.

4.3 Private Network Based Virtual Private Network (VPN)

This method utilizes an external user provided private network service as the wide-area / long-haul transport mechanism. Connections between the external user and an Enterprise Security Gateway are secured using Virtual Private Networking based on the IPsec protocol. See Section 7 entitled “VPN Technical Requirements” for further detailed information. In this connection model the FAA provisions access to the private network as required at the security gateway. A private network access device is typically required at the FAA security gateway facility.

4.4 External Service Connection Recommendations

Selection of an appropriate external connection is dependent on the criticality and survivability needs of the external services to be implemented over the connection. In general, it is recommended that external users consolidate their services via a common service access infrastructure and that the service access infrastructure is design to satisfy the most rigorous of the services. Features to be considered include:

- NAS Enterprise Security Gateways have been designed to provide highly redundant and survivable service, but the rated external service connection availability is .998
- An external service connection to an NESG is in series with the external connection transmission technology used. Typical assumptions include:
 - DTS connections have a standard availability of .998
 - Internet connections have a stand availability of .998
- NAS Boundary Protection Service (NBPS) has been implemented with four NESGs and a segregated network that interconnects the individual gateways into a common infrastructure access infrastructure;
 - All NAS external services are available at the external interfaces all NESG gateways, located at (ATL, SLC, OEX, and ACY).
 - Two NESG locations (OEX and ACY) are collocated with NAS Internet Access Points (IAPs) and support Internet VPN connectivity.

In general, it is recommended that access to the NBPS be implemented via dual connections.

For external users that require a high availability service it is further recommended that the dual connections are implemented via different (independent) technologies (e.g. one DTS connection and one networked connection) and are terminated at different gateways.

Figure 4-2 depicts a recommended External User connection methodology if high availability and resilience against catastrophic failure is required for the external service being supported.

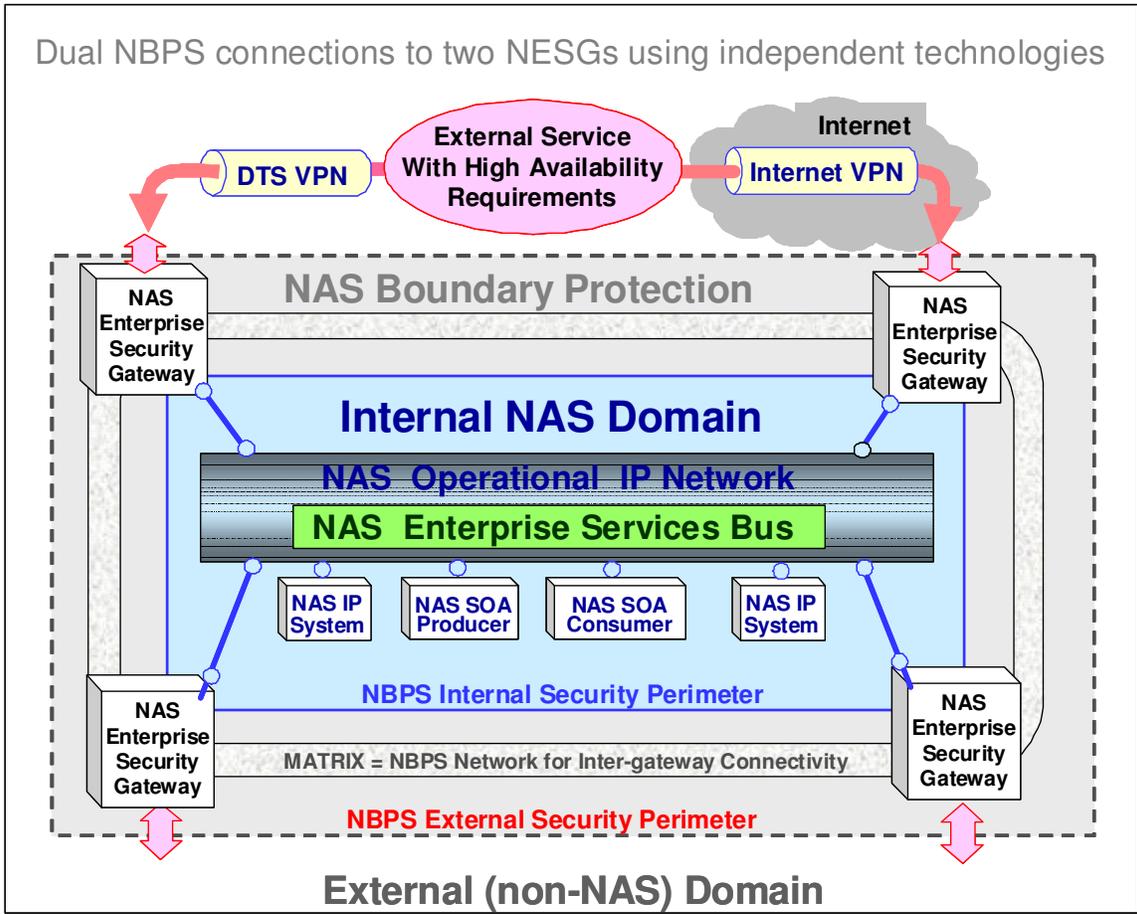


Figure 4-2: Recommended External Connection Approach for External Services with High Availability Requirements

5 External End-User Security Responsibilities

External services are used to establish virtual connections between NAS systems and external systems not directly attached to the NAS infrastructure. External services thus facilitate the extension of the NAS network “intranet” into an “extranet” by using non-FAA transport resources (such as the Internet or Dedicated Transmission Services, DTS). Each end of an external service connection must be secured from hostile attack. Some NAS programs require periodic audits to certify compliance with established security requirements. The security requirements can vary by NAS program, depending upon the sensitivity of the data. Complete detail for a specific NAS program is provided in the MOA and/or service level ICDs as developed by the sponsoring NAS system for external users.

For the purpose of general guidance, the following notes are considered standard practice in the establishment of security controls for isolating processes that will connect to a NAS system via an FAA Enterprise Security Gateway:

1. External systems are required to install security controls to protect any application processing environment that interfaces to a NAS system via extranet services. The objective of external system security controls is to isolate the external processes, access devices and the associated external service interface from other external systems and un-trusted user access.
2. External system security controls are required to have the following properties:
 - Established and documented security policies.
 - i. Have a documented security policy.
 - ii. Demonstrate adherence to all security policies.
 - iii. Security policy must allow only approved traffic flows.
 - iv. Security policy must be granular enough to specify filtering based on source IP address, destination IP address, and ports.
 - Security controls must protect the application environment and associated access device that implements the user-side of the NAS Service Delivery Point (SDP).
 - i. Security controls and access device must either be on the same platform, or
 - ii. Security controls must be between the access device and the Internet.
 - Security controls must maintain logs that store data necessary to analyze a potential attack.
 - i. Logs must show detailed data on connection attempts and VPN negotiations.
 - ii. Logs must be made available to FAA upon request.
 - Security controls must employ minimum firewall functionality such as state full inspection.
 - The client hosts (platforms for the external application processes and access device) participating in the access VPN must be protected from unauthorized access and Internet attack.
3. An external user must run the VPN and security control software on a machine that runs a secured and hardened operating system.
4. The user must maintain the remote end access VPN security control and additional firewall operating system software at a currently supported version and apply all appropriate system and security patches.

6 Support Concept

FAA Sponsor Programs maintain operations staff and monitor the health of their program's applications and associated external service instantiations. Individual application support groups act as the one-stop hotline for interaction with external customers, providing all coordination and assistance for application based operations. Ops IP Network operations provide support only after it has been determined to be a network / external service connectivity issue. FTI does not monitor individual user VPN sessions and is not aware of the "state" of user applications in general. For these reasons it is critical that all support be coordinated through the NAS sponsor program to engage application experts.

7 VPN Technical Requirements

To establish and operate an access VPN service to an FAA Enterprise Security Gateway, external users must comply with all security configurations as well as be compatible with security 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:

- Employ a site-to-site VPN. Client based VPN solutions are not accepted. Moreover, the FAA provides no external user hardware or software to support VPNs.
- Provide one or more fixed public IP addresses for the access VPN to the gateway (to be documented in the NAS Sponsor program's 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 TST engineering staff to obtain required information and configure the VPN tunnel.
- The Enterprise Security Gateway requires each external user to use a separate IP address, to communicate with each NAS sponsor program; i.e., if the user needs to communicate with two sponsor programs/systems, it will need to use two separate IP addresses on its side.
- Comply with standard Enterprise Security Gateway 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: Version 1
 - 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: The NAS Ops IP Network does not use simplified mode, aggressive mode or VPN communities for external user access VPN tunnels to the FAA Enterprise Security Gateway.

- 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.

8 **Equipment Compatibility**

All external user 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.

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