Secure Internet Access Solution

Edition: 1.00
Edition date: 07-12-2025
Classification: White
Reference nr: N/A

TABLE OF CONTENTS

1 Executive summary

(1) EUROCONTROL has enabled access to selected new B2C services over secured Internet connection (Internet as transport), using secure protocols (Transport Layer Security (TLS)) and a reverse proxy security layer to ensure confidentiality and integrity of data in transit. This approach provides:

a) **Transport Encryption**: All traffic is encrypted end-to-end using industry-standard Transport Layer Security (TLS).

b) **Traffic integrity**: All traffic is protected from tampering using the Transport Layer Security (TLS) integrity mechanisms.

c) **Server Validation**: Browsers verify the service's certificate to ensure authenticity.

d) **Controlled connectivity**: Only outbound connections from ANSP networks to EUROCONTROL NM services are required; no inbound connections from the Internet are required.

e) **Network isolation**: We recommend placing user workstations in a dedicated network zone that does not communicate with other systems.

f) **High availability**: EUROCONTROL services are designed for 99.99% availability, ensuring continuity and reliability.

(2) The Internet is the transport, but security is enforced at the protocol level and by putting in place strict outbound-only rules to NM URLs.

(3) Importantly, no inbound connections from the Internet to ANSP networks are required. All communication is strictly initiated outbound from the ANSPs to EUROCONTROL NM services, ensuring zero exposure of local systems.

(4) This means that while the Internet carries the traffic, all protection is ensured through strong encryption, certificate validation, and strict access control to EUROCONTROL NM services.

(5) This security model is the same approach used by major financial institutions, governments, and critical infrastructure operators worldwide. Providing strong, modern protection even though the Internet is used only as the transport layer.

2 Why this approach?

(1) Transport Layer Security (TLS) is a globally recognized protocol, widely used for secure communication. By leveraging it:

a) We provide a secure alternative for accessing NM services over the Internet.

b) We maintain strong encryption equivalent to that used by financial institutions and other critical infrastructure services.

c) We simplify connectivity for ANSPs without compromising security.

(2) This approach is aligned with recognised cybersecurity best practices, using strong encryption, controlled outbound connectivity, and network isolation to ensure secure access to EUROCONTROL NM services.

3 How it works

(1) Users access EUROCONTROL NM services via HTTPS URLs.

(2) The URL is resolved to an IP address.

(3) Traffic travels over the public Internet and is encrypted end-to-end.

(4) The browser checks the server's certificate to confirm the site is authentic.

(5) Traffic passes through a reverse proxy, which enforces HTTPS, filters malicious traffic, and forwards legitimate requests to EUROCONTROL NM services.

(6) Additional security layers, including firewalls and monitoring, remain in place at EUROCONTROL Connectivity Edge.

(7) All communication is encrypted (HTTPS/TLS); ANSP networks accept no inbound connections, and EUROCONTROL protects NM services using a reverse proxy and DDoS filtering.

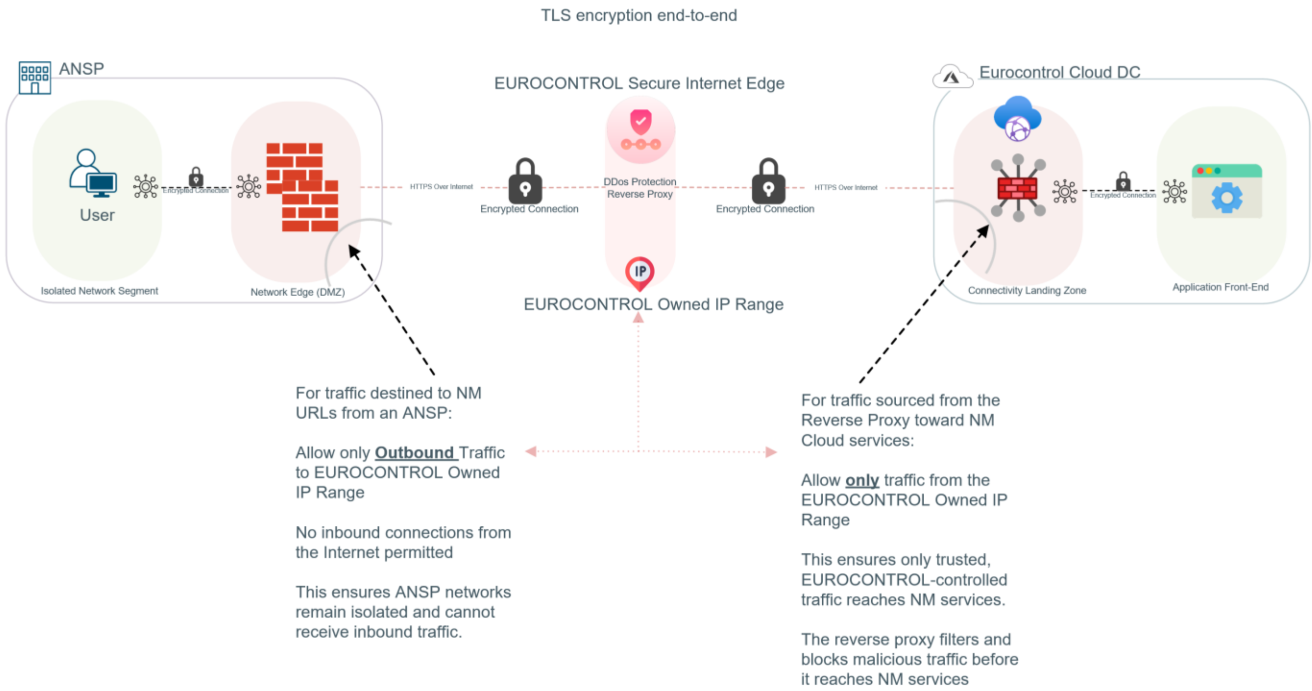

Figure 1 - Secure Outbound-Only Access Model

(8) The diagram above illustrates the outbound-only security model. ANSP workstations initiate encrypted HTTPS connections to a EUROCONTROL-owned IP range. No inbound connections to ANSP networks are possible. Traffic passes through a dedicated, DDoS-protected reverse proxy layer, where only validated and encrypted requests are forwarded to NM services.

4 What stakeholders need to do

(1) Two options for firewall configuration:

   a) IP-based allowlisting

      i) Allow outbound traffic to the EUROCONTROL-owned subnet (91.224.186.0/24)[1] on your external firewall.

      ii) Recommended for environments where firewall rules are managed by IP addresses.

   b) URL-based allowlisting

   c) Allow outbound HTTPS traffic to the official NM services URLs.

   d) Recommended for modern firewalls that support FQDN-based rules.

(2) Additional best practice recommendations for critical infrastructure:

   a) Outbound-only policy: Block any inbound connections from the Internet to local workstations.

   b) Restrict outbound scope: Only allow outbound connections to the published NM URLs or the EUROCONTROL-owned subnet (91.224.186.0/24).

   c) Network segmentation: Place user workstations in a dedicated network zone that does not communicate with other types of systems.

5 Benefits for stakeholders

(1) No special hardware or IPsec tunnels are required.

(2) Global accessibility with strong security.

(3) Compliance with modern cybersecurity standards.

(4) Reduced attack surface through isolation and outbound-only rules.

[1] Also, to be published in the user access and technical guides.

6 Concerns vs. Mitigation

Concern	Mitigation
Internet exposure	HTTPS/TLS encryption, reverse proxy filtering, and outbound-only rules.
Data confidentiality	End-to-end encryption.
Firewall complexity	Simple allowlisting: a single /24 subnet or NM URLs.
Network Segregation	Dedicated network zone for user workstations.
Availability of local connectivity	Responsibility of ANSPs to ensure stable and highly available Internet access, as today.
Service availability	EUROCONTROL NM services are designed to ensure at least 99.99% uptime.

7 Frequently asked questions

The following answers address common questions from ANSPs and clarify why this security model is safe, compliant, and widely adopted in other critical sectors.

(1) Q: Is this safe?

A. *Yes. HTTPS/TLS combined with a reverse proxy security layer is the global standard for secure web traffic and is used by financial institutions and critical infrastructure operators.*

(2) Q: Do we need VPNs?

A. *No, HTTPS already provides strong encryption, integrity, and authentication, so a VPN is not required for these services.*

(3) Q: Will performance suffer?

A. *No. HTTPS is optimized and widely supported, with performance comparable to normal web browsing.*

(4) Q: Is the same proposed configuration applicable only for the B2C new NM services URLs:

A. The solution applies to both B2C and B2B new NM services URLs; rollout will follow a phased approach: first B2C, then B2B at later stages.

(5) Q: Does this solution affect connectivity to any existing NM services?

A. No. This solution applies to eEAD and other new NM B2C digital products rolled out in subsequent stages.

SUPPORTING
EUROPEAN
AVIATION

www.eurocontrol.int