# 🇺🇸 CRYPE Network, Firewall & Proxy Configuration Guide

**Enterprise & Security Review Version**

## 1. Document Purpose

This document provides IT and security administrators with a complete and structured overview of:

- Network architecture of CRYPE
- Required outbound ports and protocols
- Recommended firewall configuration
- Proxy and TLS inspection requirements
- Data protection and encryption architecture

**CRYPE does not require:**

- Inbound firewall rules
- Port forwarding
- Static public IP configuration
- Proprietary tunneling mechanisms

All communication is initiated as outbound connections.

## 2. CRYPE Network Configuration – Admin Quick Rule Block

For environments where administrators want to quickly configure firewall access for CRYPE, the following outbound rules are sufficient for full functionality.

### Required outbound connections

| Protocol | Port | Destination | Purpose |
|---|---|---|---|
| TCP | 443 | backend.go.crype.eu | API communication |
| TCP | 443 | signal.go.crype.eu | Signaling |
| TCP | 443 | turn1–turn5.go.crype.eu | TURN relay fallback |
| UDP | 443 | turn1–turn5.go.crype.eu | STUN / NAT traversal |
| UDP | 3478 | turn1–turn5.go.crype.eu | STUN / TURN |
| UDP | 49152–65535 | Dynamic remote endpoints | P2P media transport |

### Important notes

• No inbound firewall rules are required
• No port forwarding is required
• Connections are outbound only and stateful
• Direct peer-to-peer (P2P) communication is preferred when UDP is permitted

Allowing outbound **UDP 443** enables direct peer-to-peer communication and reduces dependency on TURN relay servers.

## 3. Communication Architecture Overview

CRYPE uses standard protocols based on:

- WebRTC
- STUN
- TURN
- TLS
- DTLS
- SRTP
- SCTP
- HTTPS
- WSS

The system follows a priority-based connectivity model:

1. Direct P2P (UDP) – preferred
2. TURN Relay over UDP – fallback
3. TURN Relay over TCP – fallback

Media is always end-to-end encrypted between endpoints.
TURN servers forward already end-to-end encrypted media packets and do not have access to decryption keys.

### Local Network (LAN) Communication Behavior

When endpoints are located within the same local network segment (e.g., same subnet or routable internal network), CRYPE establishes direct peer-to-peer communication using local ICE host candidates.

In such scenarios:

- **Media and data traffic remain entirely within the local network.**
- No TURN relay infrastructure is used.
- No external media routing occurs.
- No inbound firewall rules are required.

WebRTC prioritizes direct UDP-based peer-to-peer connectivity in local environments.

Internet connectivity is required only for signaling (see 5.2 Signaling Server)

This ensures that local network communication within secured enterprise or healthcare networks does not traverse external relay systems when direct local connectivity is possible.

# 4. NAT Behavior and Peer-to-Peer Connectivity

WebRTC attempts to establish direct peer-to-peer (P2P) communication between endpoints whenever possible.

To discover reachable network paths, WebRTC uses the **ICE framework (Interactive Connectivity Establishment)** which includes:

- **STUN** – determines the public IP address and port mapping of a client
- **TURN** – provides relay connectivity when direct communication is not possible
- **ICE candidate gathering** – tests possible network paths between endpoints

In most network environments, NAT devices allow peer-to-peer connectivity once an outbound mapping has been created.

However, some NAT implementations behave differently and may prevent direct peer-to-peer connectivity.

## Symmetric NAT

In symmetric NAT environments, a unique public port mapping is created for each destination.

**Example:**

Client internal address

192.168.1.10:52344

Mapping created when contacting a STUN server

Public mapping: 84.132.10.5:62000

When the same client sends traffic to another endpoint, a different mapping may be created:

Peer destination → new mapping
84.132.10.5:62045

Because the STUN server only reports the first mapping, the remote peer may attempt to send traffic to the wrong port.
In such cases the NAT device discards the packets.

### Impact on WebRTC Connectivity

In symmetric NAT environments:

- direct peer-to-peer connectivity may fail
- ICE may not find a valid candidate pair

When this occurs, WebRTC automatically falls back to **TURN relay connectivity**.

### TURN Relay Fallback

In TURN mode, media traffic flows through the TURN server instead of directly between endpoints.

Peer A → TURN Server → Peer B

This guarantees connectivity but introduces:

- additional latency
- increased external bandwidth usage
- dependency on relay infrastructure

### Typical Environments Using Symmetric NAT

Symmetric NAT is commonly found in:

- enterprise firewalls
- carrier-grade NAT (mobile networks)
- some ISP routers
- hotel or campus networks

CRYPE automatically detects these conditions and switches to TURN relay when necessary.

## 5. Performance & Time-Critical Data Transmission Considerations

CRYPE is designed for secure real-time communication, but it may also be used for the transmission of large data volumes between endpoints.

In enterprise, healthcare, industrial, and operational environments, data transfers may be:

- Performance-sensitive
- Time-critical
- Operationally urgent
- Required in emergency or escalation scenarios

**The selected connectivity mode (Direct P2P vs. TURN relay) has a direct impact on throughput, latency, and infrastructure dependency.**

## 5.1 Direct P2P Mode (Recommended)

When outbound UDP connectivity is permitted and direct peer-to-peer (P2P) communication can be established:

- Data flows directly between endpoints.
- No intermediate relay infrastructure is involved.
- Network path length is minimized.
- External bandwidth usage is reduced.
- Transfer throughput is limited primarily by endpoint network capacity.

This mode provides:

- Maximum performance
- Minimum transmission time
- Lowest latency
- Reduced external dependency
- Improved scalability

For large data transmission and time-critical scenarios, direct P2P connectivity ensures the shortest and most efficient network path between communicating parties.

## 5.2 TURN Relay Mode (Fallback)

If direct UDP connectivity is restricted, CRYPE automatically falls back to TURN relay.

In relay mode:

- All data is forwarded via the TURN server.
- The data stream traverses an additional external network hop.
- External bandwidth consumption increases.
- Relay infrastructure load increases.
- Transfer duration may increase depending on available bandwidth, turn server location, latency conditions, and overall network topology. The performance impact depends primarily on available upstream capacity at both endpoints and external relay path characteristics.

TURN relay ensures reliable operation in restrictive network environments. However, it introduces additional infrastructure dependency that may impact throughput during large data transmission.

## 5.3 Impact on Time-Critical or Emergency Data Transfer

In environments where data transmission supports:

- Clinical decision workflows
- Incident response coordination
- Industrial operations
- Engineering collaboration
- High-volume content distribution

network efficiency becomes operationally significant.

Allowing direct UDP-based P2P communication:

- Reduces transmission path complexity
- Minimizes latency accumulation
- Reduces reliance on centralized relay infrastructure
- Improves overall responsiveness under load

In emergency or escalation scenarios, minimizing additional relay hops reduces potential performance bottlenecks.

## 5.4 Administrative Recommendation

For environments where:

- Large data volumes are expected
- High throughput is required
- Operational continuity is critical
- Time-sensitive communication may occur

**enabling outbound UDP 3478 and 443 (and associated WebRTC ports 49152-65535) is strongly recommended.**

If UDP remains restricted, CRYPE continues to operate reliably over TURN relay (TCP/TLS 443). However, for large or time-critical data transmission, direct P2P connectivity provides measurable performance and scalability advantages.

# 6. Connectivity Modes (Admin Decision Matrix)

This section defines what must be allowed and what the operational result will be.

## 6.1 Level 1 – Optimal Configuration (Recommended: Primary P2P Mode)

### Firewall Rule Requirement

Administrators must implement outbound allow rules for the following Fully Qualified Domain Names (FQDNs). FQDN-based allowlisting is strongly recommended instead of static IP-based rules.

### Implement outbound firewall rules as follows:

| Protocol | Port | Destination | Purpose |
|---|---|---|---|
| TCP | 443 | signal.go.crype.eu | Signaling |
| TCP | 443 | backend.go.crype.eu | API |
| TCP | 443 | go.crype.eu | Web Client (optional) |
| TCP | 443 | wa-whiteboard.crype.eu | CRYPE Whiteboard App |
| TCP | 443 | news.crype.eu | CRYPE Announcements |
| TCP | 443 | crype.eu | CRYPE Video backgrounds |
| UDP | 443 and 3478 | turn1.go.crype.eu<br>turn2.go.crype.eu<br>turn3.go.crype.eu<br>turn4.go.crype.eu<br>turn5.go.crype.eu | STUN/TURN + NAT traversal |
| UDP | 49152–65535 | Dynamically negotiated remote endpoints | P2P media transport |

## Firewall Notes (WebRTC Ephemeral Ports)

The UDP port range 49152–65535 refers to dynamically allocated client-side ephemeral outbound ports used by WebRTC for peer-to-peer media and data transport.

This configuration:

- Requires outbound rules only
- Does not require inbound firewall rules
- Does not require port forwarding
- Does not expose internal services

Connections are established outbound and remain stateful. The firewall permits return traffic only for established sessions.

Peer-to-peer media connections use dynamically negotiated remote IP addresses (ICE candidates) and therefore cannot be statically allowlisted.

FQDN-based allowlisting applies only to CRYPE infrastructure endpoints.

IP-based allowlisting of CRYPE infrastructure is not recommended due to potential cloud infrastructure changes.

## Result

- **Direct P2P communication**
- **Minimal relay usage**
- **Minimal external bandwidth consumption**
- **Lowest latency**

**This configuration significantly reduces dependency on TURN infrastructure.**

## 6.2 Level 2 – Functional Configuration (Relay Mode)

If UDP is restricted but HTTPS CONNECT is permitted:

## Allow outbound:

| Protocol | Port | Destination | Purpose |
|---|---|---|---|
| TCP | 443 | signal.go.crype.eu | Signaling |
| TCP | 443 | backend.go.crype.eu | API |
| TCP | 443 | go.crype.eu | Web Client (optional) |
| TCP | 443 | wa-whiteboard.crype.eu | CRYPE Whiteboard App |
| TCP | 443 | news.crype.eu | CRYPE Announcements |
| TCP | 443 | crype.eu | CRYPE Video backgrounds |
| TCP | 443 | turn1.go.crype.eu<br>turn2.go.crype.eu<br>turn3.go.crype.eu<br>turn4.go.crype.eu<br>turn5.go.crype.eu | STUN/TURN + NAT traversal |

## Firewall & Proxy Requirements

If clients operate behind an **explicit HTTP/HTTPS proxy**, the following conditions must be met:

• The proxy must allow **HTTPS CONNECT tunneling to TCP port 443** for the CRYPE servers. This allows clients to establish encrypted TLS connections through the proxy.

• After the CONNECT tunnel is established, the proxy must **not enforce HTTP protocol validation**.
TURN over TLS uses **standard TLS encryption on port 443**, but the encrypted channel **does not contain HTTP protocol traffic**.

• If **TLS inspection / SSL inspection** is enabled, administrators must ensure that these mechanisms **do not block or modify TURN-over-TLS connections**.

Typical security features that may block TURN include:

- HTTP protocol enforcement on port 443
- TLS inspection with protocol validation
- Application-layer filtering that allows only HTTP traffic on port 443

In such environments, administrators should configure an **exception or inspection bypass rule** for the CRYPE TURN servers.

### Result

- Media traffic is relayed via the **CRYPE TURN server using TLS over TCP 443**.
- Media streams remain **end-to-end encrypted** between endpoints.
- Relay operation increases **external bandwidth usage**, since media traffic passes through the relay server.
- Latency may be slightly higher due to the additional network hop.
- CRYPE remains **fully functional and stable**, even in restrictive network environments.

## 6.3 Level 3 – Highly Restricted Configuration

CRYPE media connectivity may be impacted if one or more of the following conditions apply:

- Outbound UDP traffic is blocked
- TURN over TLS (TCP 443) is blocked or restricted
- HTTPS CONNECT tunneling is not permitted in proxy environments
- TLS inspection interferes with DTLS, SRTP, SCTP, or TURN over TLS traffic

# Operational Result

- CRYPE may be unable to establish media connectivity.

CRYPE signaling requires standard HTTPS and WebSocket Secure (WSS) connectivity over TCP 443.

TURN relay over TLS requires TCP 443 with unrestricted TLS transport capability, as TURN traffic does not contain HTTP payload.

Media connectivity is prevented only when both:

- Direct UDP-based P2P communication, and
- TURN over TLS fallback

are restricted or modified by network policy.

# 7. Detailed Protocol and Service Reference

## 7.1 API Server

- URL: https://backend.go.crype.eu
- Protocol: HTTPS
- Port: 443 (TCP)
- Encryption: TLS 1.2 / 1.3
- Direction: Outbound

---

## 7.2 Signaling Server

- URL: wss://signal.go.crype.eu
- Protocol: WebSocket Secure (WSS)
- Port: 443 (TCP)
- Encryption: TLS 1.2 / 1.3
- Direction: Outbound

Uses standard TLS and SNI.
No proprietary encapsulation.

## What is Signaling?

Signaling is used exclusively for session negotiation and connection establishment between end-points.

Signaling traffic:

- Exchange of connection candidates (ICE information) previously discovered locally (e.g. via STUN).
- Coordinates session setup parameters
- Does not transport media content
- Does not carry audio, video, or data streams

All media and data streams are transmitted separately using WebRTC peer-to-peer channels secured by DTLS and SRTP/SCTP.

The signaling server does not decrypt or process media content.

---

## 7.3 STUN

- URL: stun:turn.go.crype.eu
- Ports:
  - 3478 UDP (preferred)
  - 443 UDP (fallback)
  - TCP fallback if UDP unavailable
- Direction: Outbound

Purpose: NAT detection and candidate discovery.

### 7.4 TURN

- URL: turn:turn.go.crype.eu
- Ports:
    - 3478 UDP (preferred)
    - 443 UDP (preferred fallback)
    - 443 TCP/TLS (last fallback)

- Direction: Outbound

TURN forwards already end-to-end encrypted WebRTC traffic (SRTP media and SCTP data channels) without decryption. **No media decryption or inspection is performed.**

TURN over TLS uses standard TLS with SNI and does not encapsulate HTTP semantics within the encrypted channel.

---

### 7.5 WebRTC-Media Transport (P2P and TURN via UDP)

- Transport: UDP
- Protocols:
    - SRTP (media)
    - SCTP (data channels)
    - DTLS (key exchange)
- Port range: 49152–65535 (client ephemeral outbound)

No fixed inbound port openings required.

## 8. FQDN-Based Whitelisting (Strongly Recommended)

CRYPE infrastructure may operate in dynamic cloud environments. IP addresses may change.

Use FQDN-based rules for:

- **signal.go.crype.eu**
- **backend.go.crype.eu**
- **go.crype.eu**
- **wa-whiteboard.crype.eu**
- **news.crype.eu**
- **crype.eu**
- **turn1.go.crype.eu**
- **turn2.go.crype.eu**
- **turn3.go.crype.eu**
- **turn4.go.crype.eu**
- **turn5.go.crype.eu**

IP-based allowlisting is discouraged unless mandated by enterprise policy.

# 9. Proxy Configuration Guidance

If clients operate behind an **explicit HTTP/HTTPS proxy**, administrators must ensure that outbound TLS connections over TCP port 443 can be established to the CRYPE services.

The complete list of required destinations is provided in **Section 6 (FQDN-Based Whitelisting)**.

Administrators must ensure that:

- outbound TCP 443 connections through the proxy are allowed
- the proxy permits **HTTPS CONNECT tunneling** to these destinations
- TLS inspection does **not block or modify these connections**
- firewall policies do **not enforce HTTP-only traffic on TCP port 443**

TURN relay connections use TLS encryption on port 443 but **do not carry HTTP protocol traffic inside the TLS session**.

If TLS inspection is enabled, administrators should configure an **inspection bypass rule for the TURN servers listed in Section 6**.

## Not Required

The following measures are **not mandatory** for operating CRYPE:

• Application-specific proxy bypass rules
• Custom tunneling mechanisms or proprietary protocols
• Manual proxy configuration inside the CRYPE application

## Behavior of CRYPE Applications

The installed **CRYPE desktop application** automatically uses the proxy settings configured at the operating system level (e.g., Windows, macOS, or Linux).

Mobile CRYPE applications also rely on the **native networking stack of the operating system**, which automatically applies the configured proxy or network settings.

In most environments, no separate proxy configuration inside the application is required.

## 9.1 Enabling P2P in Proxy-Based Environments

In many enterprise and healthcare environments, web traffic is routed through an explicit HTTP/HTTPS proxy.

While proxies typically do not transport UDP traffic, direct peer-to-peer (P2P) communication can still be enabled without removing or disabling the proxy.

CRYPE recommends the following approach to enable primary P2P connectivity while maintaining proxy-based web security policies.

## Recommended Configuration Strategy

Maintain the existing proxy configuration for standard web traffic, but allow controlled outbound UDP traffic for WebRTC communication in your firewall.

Specifically:

- Permit outbound UDP 443 to: turn1.go.crype.eu, turn2.go.crype.eu, turn3.go.crype.eu, turn4.go.crype.eu, turn5.go.crype.eu
- Permit outbound UDP 3478 to turn1.go.crype.eu, turn2.go.crype.eu, turn3.go.crype.eu, turn4.go.crype.eu, turn5.go.crype.eu
- Permit outbound dynamic UDP ports 49152–65535 (client-side ephemeral ports)

No inbound firewall rules or port forwarding are required.

## Security Considerations

- Only outbound connections are established (for signaling, media, and data channels).
- No services are exposed within the internal network.
- Media streams remain end-to-end encrypted using DTLS and SRTP.
- TURN relay remains available as fallback if direct P2P negotiation fails.
- Proxy policies for HTTP/HTTPS traffic remain unchanged.

This approach enables direct endpoint-to-endpoint communication while preserving centralized web traffic inspection.

## Alternative Approach (If UDP Is Globally Restricted)

If enterprise policy restricts outbound UDP globally, administrators may implement a proxy bypass rule for CRYPE infrastructure domains:

- **signal.go.crype.eu**
- **backend.go.crype.eu**
- **go.crype.eu**
- **wa-whiteboard.crype.eu**
- **news.crype.eu**
- **crype.eu**
- **turn1.go.crype.eu**
- **turn2.go.crype.eu**
- **turn3.go.crype.eu**
- **turn4.go.crype.eu**
- **turn5.go.crype.eu**
-

This allows direct connectivity for CRYPE services while maintaining proxy enforcement for other internet destinations.

### Operational Impact

Enabling outbound UDP 443 significantly reduces reliance on relay infrastructure and minimizes external bandwidth usage.

If UDP remains restricted, CRYPE operates reliably via TURN over TLS (TCP 443), but media traffic will be relayed instead of transmitted directly between endpoints.

## 10. Typical Enterprise Firewall Issues with WebRTC

Enterprise firewalls may include advanced security features such as application inspection, TLS interception, protocol enforcement, or deep packet inspection.
These features can unintentionally interfere with WebRTC-based communication even when the required ports are open.

Administrators should review the following common firewall behaviors.

---

### 10.1 TLS Inspection / SSL Interception

Many enterprise firewalls intercept TLS connections in order to inspect encrypted traffic.

However, WebRTC uses protocols such as **DTLS, SRTP and SCTP**, which are not traditional HTTPS traffic.

If TLS inspection attempts to intercept these connections, the media transport may fail.

**Recommended configuration**

Disable TLS inspection (or create an exception) for CRYPE FQDNs:

- backend.go.crype.eu
- signal.go.crype.eu
- turn1–turn5.go.crype.eu

---

### 10.2 HTTP-Only Protocol Enforcement on TCP 443

Some firewalls enforce policies that only allow **HTTP or HTTPS traffic on TCP port 443**.

TURN over TLS uses standard TLS encryption on port 443 but **does not contain HTTP semantics**.

If the firewall performs strict protocol validation, TURN relay connectivity may be blocked.

**Recommended configuration**

Ensure that application-layer inspection or protocol enforcement does not require HTTP payload for TLS connections to CRYPE TURN servers.

---

## 10.3 UDP Restrictions

Some enterprise networks restrict outbound UDP traffic or only allow UDP for specific services.

WebRTC requires UDP connectivity to establish optimal peer-to-peer communication.

If UDP is blocked, CRYPE will fall back to TURN relay over TCP/TLS, which increases latency and external bandwidth usage.

**Recommended configuration**

Allow outbound:

- UDP 443
- UDP 3478
- UDP ephemeral ports (49152–65535)

---

## 10.4 Proxy-Only Internet Access

Some organizations force all internet traffic through an HTTP/HTTPS proxy.

Since proxies typically transport only TCP traffic, direct UDP-based peer-to-peer connections may not be possible.

In such environments CRYPE will operate using TURN relay over TLS (TCP 443).

**Recommended configuration**

Ensure that:

- HTTPS CONNECT tunneling is permitted
- TLS traffic to CRYPE TURN servers is allowed
- Non-HTTP TLS payload is not blocked

---

## 10.5 Application Identification / Application Control

Modern firewalls use application identification engines (e.g., App-ID or Application Control) to classify traffic.

WebRTC traffic may be classified as:

- unknown-udp
- unknown-tls
- non-web traffic

Some security policies automatically block unknown applications.

**Recommended configuration**

Ensure that policies do not block WebRTC-related traffic to CRYPE infrastructure.

---

### Examples of Firewall Features

The following firewall features may affect WebRTC connectivity.

| Vendor | Feature |
|---|---|
| Fortinet | SSL Inspection, Application Control |
| Palo Alto | SSL Decryption, App-ID |
| Sophos | TLS Inspection, Web Filtering |
| Check-Point | HTTPS Inspection |
| Cisco | TLS Decryption |

---

### Operational Impact

When WebRTC traffic is blocked or restricted by firewall inspection features:

• Direct peer-to-peer communication may fail
• Media traffic may be forced through TURN relay servers
• Latency may increase
• External bandwidth usage may increase

For optimal performance, allow UDP connectivity and avoid protocol enforcement that assumes HTTP semantics on TLS port 443.

## 11. TLS Inspection (SSL Inspection) and Deep Packet Inspection (DPI)

If TLS inspection (also known as **SSL inspection, TLS interception, or TLS decryption**) is enabled on the firewall or security gateway, the following requirements must be considered.

CRYPE relies on encrypted real-time communication protocols that may not contain standard HTTP payload. Security devices performing TLS interception, protocol validation, or application-layer inspection must not interfere with these protocols.

Administrators must ensure that:

- **DTLS traffic is not terminated or modified** by TLS inspection mechanisms
- **SRTP media streams are not altered or blocked**
- **SCTP data channels (encapsulated within DTLS)** are not blocked or modified
- **TURN over TLS connections are not blocked** due to the presence of non-HTTP TLS payload

Administrators should also verify that **no application-layer inspection, protocol enforcement, or DPI functionality enforces HTTP-only validation on TCP port 443 connections to** turn.-go.crype.eu.

Blocking or filtering **non-HTTP TLS traffic on TCP port 443** may prevent TURN relay connectivity and therefore disrupt media communication in restricted network environments.

## 12. Data Protection & Encryption Architecture

CRYPE implements:

- End-to-end encryption for media
- Endpoint-generated encryption keys
- No media decryption on relay servers
- No proprietary tunneling mechanisms

Encryption standards:

- TLS 1.2 / 1.3
- DTLS 1.2 / 1.3
- SRTP
- SCTP (secured via DTLS)

TURN servers act solely as encrypted packet forwarders.

## 13. Troubleshooting Checklist for Administrators

If calls fail:

1. Verify outbound TCP 443 connectivity to:
    - signal.go.crype.eu
    - backend.go.crype.eu
    - go.crype.eu
    - wa-whiteboard.crype.eu
    - news.crype.eu
    - crype.eu
    - turn1.go.crype.eu
    - turn2.go.crype.eu
    - turn3.go.crype.eu
    - turn4.go.crype.eu
    - turn5.go.crype.eu
2. Verify HTTPS CONNECT permitted (if proxy used)
3. Verify non-HTTP TLS allowed on port 443
4. Verify UDP 443 permitted outbound and not restricted by security policy or application control

5. Ensure that TLS inspection (SSL inspection / TLS interception) is disabled for CRYPE FQDNs or that an appropriate exception is configured on the firewall.
6. Check firewall logs for dropped UDP ephemeral ports

## 14. Summary for Security Review

CRYPE:

- Uses only standardized protocols
- Requires outbound-only connections
- Does not require inbound firewall rules
- Supports strict proxy environments
- Preserves end-to-end encryption
- Does not decrypt media on infrastructure servers

The optimal configuration includes outbound UDP 443 to enable direct peer-to-peer communication and reduce dependency on TURN relay servers.