

TURING AI

Network & Cybersecurity Report

Turing devices are designed to be easy to manage and maintain via our cloud-based management platform. In the majority of installations, no specific network and/or security changes are required in the customer environment.

If any issues are encountered, please verify the following specific network ports and protocols at the customer network/firewall layer for communication.

Current Deployment Network Requirements (07-23-2026):

- **HTTP API's**
 - HTTPS(443) to 13.53.44.71 and 34.212.199.23 gw.turingvideo.com Outbound
 - HTTPS(443) to 35.84.153.58 app.turingvideo.com Outbound
 - HTTPS(443) to 34.212.199.23 device.turingvideo.com Outbound
 - HTTPS(443) to 34.211.96.66 ws.turingvideo.com Outbound
- **OTA**
 - SSH(22) to 13.56.217.169 zeno.turingvideo.com Outbound
 - HTTPS(443) to 13.56.217.169 zeno.turingvideo.com Outbound
 - HTTPS(443) to 52.11.167.25 harbor.turingvideo.com Outbound
 - HTTPS(443) to 34.209.253.212 zeno2.turingvideo.com Outbound
- **NVR and Camera remote web access**
 - Outbound HTTPS(443) to 35.164.21.146 access.turingvideo.com
 - Outbound TCP 8024 and UDP 8024 access.turingvideo.com
- **Video streaming for live view and playback (via Cloud)**
 - Bridge

Domain	IP Address	Port	Protocol	Direction
s1.stream.turingvideo.com	172.238.210.114	1935	TCP	Outbound - Bridge (RTMP)
s2.stream.turingvideo.com	172.233.177.16	1935	TCP	Outbound - Bridge (RTMP)
s3.stream.turingvideo.com	172.233.181.228	1935	TCP	Outbound - Bridge (RTMP)
s4.stream.turingvideo.com	172.233.181.235	1935	TCP	Outbound - Bridge (RTMP)

- User

Domain	IP Address	Port	Protocol	Direction
s1.stream.turingvideo.com	172.238.210.114	443	TCP	Outbound - User (HTTPS)
s1.stream.turingvideo.com	172.238.210.114	8000	UDP	Inbound + Outbound - User, bidirectional
s2.stream.turingvideo.com	172.233.177.16	443	TCP	Outbound - User (HTTPS)
s2.stream.turingvideo.com	172.233.177.16	8000	UDP	Inbound + Outbound - User, bidirectional
s3.stream.turingvideo.com	172.233.181.228	443	TCP	Outbound - User (HTTPS)
s3.stream.turingvideo.com	172.233.181.228	8000	UDP	Inbound + Outbound - User, bidirectional
s4.stream.turingvideo.com	172.233.181.235	443	TCP	Outbound - User (HTTPS)
s4.stream.turingvideo.com	172.233.181.235	8000	UDP	Inbound + Outbound - User, bidirectional

Domain	IP Address	Port	Protocol	Direction
srs-1.turingvideo.com	35.81.107.235	1935	TCP	Outbound (RTMP)
srs-1.turingvideo.com	35.81.107.235	8000-8015	UDP	Outbound
srs-1.turingvideo.com	35.81.107.235	443	TCP	Outbound (HTTPS)
srs-1.turingvideo.com	35.81.107.235	4096-65535	UDP	Inbound
srs-2.turingvideo.com	52.39.116.187	1935	TCP	Outbound (RTMP)
srs-2.turingvideo.com	52.39.116.187	8000-8015	UDP	Outbound
srs-2.turingvideo.com	52.39.116.187	443	TCP	Outbound (HTTPS)
srs-2.turingvideo.com	52.39.116.187	4096-65535	UDP	Inbound

- Notes

- Port 1935/tcp (RTMP) is the bridge pushing its stream out to the server — outbound only. TCP is connection-oriented, so return traffic rides the same outbound session; no separate inbound rule is needed.
- Port 443/tcp is standard HTTPS signaling initiated by the user — outbound only, for the same reason.
- Port 8000/udp carries the actual WebRTC media stream for users and must be explicitly opened both inbound and outbound. UDP is stateless, so unlike TCP a one-way rule will silently break the stream.

- **Video streaming for live view (via local streaming)**
 - These ports of bridge should be open
 - port 1935 UDP
 - port 8000
- **Media Storage and other AWS services**
 - Outbound and Inbound HTTPS(443) to *.s3.amazonaws.com
 - Outbound and Inbound HTTPS(443) to *.s3.us-west-1.amazonaws.com and *.s3.us-west-2.amazonaws.com
 - Outbound and Inbound HTTPS(443) to *.s3.us-west-1.amazonaws.com and *.s3.us-west-2.amazonaws.com
 - Outbound and Inbound HTTPS(443) to *.s3.us-west-1.wasabisys.com
- **System libraries**
 - NTP: ntp.ubuntu.com for system time sync
- **OpenAPI and webhook**
 - Inbound and outbound HTTPS(443) to 44.237.117.177

Note: Our VISION BRIDGE Internal network (docker) uses 172.16.0.0. If customer network contains this network, we will need to change the docker network to a non-conflicting network such as 192.168.38.x / 29

Example Use for docker0:

192.168.38.2

255.255.255.248

Compliance & Certifications:

NDAA



✓	Organizational Security Compliance and Certifications	● SOC 2 Type II Compliant ● Leverage Vanta Platform for compliance
---	---	---

		automation • Third-Party Audits
✓	Hardware Security and Compliance	• NDAA Section 889

FAQ (07-17-2024):

1. Can you see all our camera feeds?

We can not view the feeds with the current setup. While it is possible to forward all RTSP streams to ssh port if the customer needs to, Turing does not do it by default for it is not needed for the algorithmic detections in the **Turing Vision** application. The customer can also block the ssh port for it.

2. Why do you need us to open the ports?

- **Port 22 (Inbound and outbound):** SSH connection, to provide support and send software and algorithm updates to the Turing Vision server.
- **URL access**
 - **AWS S3: Outbound** connection to s3.us-west-2.amazonaws.com and s3.us-west-1.amazonaws.com is required for Turing vision platform to upload AI-based alerts and clips to provide real-time notifications to a user so that one can review them from any device. We use the AWS S3 bucket to securely store all respective video clips for the customer's respective tenant. Currently, AWS does not provide a static IP for S3 storage.
 - **Turing Video Gateway:** Allow an **outbound** connection to gw.turingvideo.com. We can provide a static IP address if preferred. Turing video gateway supports encrypted traffic through TLS 1.3 and SSL.
- **RTSP:** Turing Vision server must have access to all their RTSP streams from the customer's local DVR/NVR. All video storage of recordings will remain in the DVR/NVR

3. Is it necessary to keep Port 22 open?

Customer needs to only keep the ssh Port 22 open on the Turing server for us to debug or fix any issues on it. If the customer prefers so, the customer can only open it to us when we need to use Zeno to ssh into it. This will require our support team to coordinate with the customer to fix bugs and push out updates

4. What do you use to protect the communications on this port? How is it encrypted?

- Turing video gateway supports encrypted traffic through TLS 1.3 and SSL
- The SSH port 22 is encrypted and password-protected

5. What kind of push updates are being done? How frequently?

Currently, we do updates every sprint that is every month. This OTA includes both feature and security updates.

6. Security of the server -- will it cause a security risk to my network?

All the ports of our server are closed even to Turing except SSH port 22. There is **no security risk** to the customer's network. If a customer is concerned about the SSH port, one can open it to us only when needed instead of keeping it open all the time.