Connectors - network flows

Network flows

This page lists the network flows required by the Trustelem connectors (Trustelem Connect and Trustelem ADConnect) and explains how to check that they are correctly opened.

All traffic is outbound only, over TCP port 443, in TLS, and is always initiated by the connector installed in your network. No inbound rule and no port forwarding are required on your side.

Destinations to authorize

Allow outbound traffic from the machine hosting the connector to the following destinations:

Destination	Used for
`*.trustelem.com`	All connections from the connector to the Trustelem platform.
`relay-fr-01.wallix.com`	Connections going through the Trustelem relay.
`relay-fr-02.wallix.com`	Connections going through the Trustelem relay.

Write your rules against these DNS names, not against IP addresses. The connector resolves the names at each connection and never uses a hard-coded address. Most firewalls and proxies support FQDN-based rules, and it is the only form of rule that keeps working on its own.

Rules written with IP addresses are the most frequent cause of connector outages. They have to be updated by hand whenever the platform changes an address, an update is easy to miss, and the failure does not appear at the moment of the change but at the connector's next reconnection, which makes it hard to relate to its cause.

If your equipment cannot filter on DNS names

Only in that case, authorize the following addresses:

DNS address	IP addresses to authorize
`*.trustelem.com`	`185.4.44.22`, `185.4.46.20`, `185.4.46.21`, `185.4.46.22`
`*.trustelem.com` (active on 29 September 2026)	`185.4.44.114`, `185.4.44.117`
`relay-fr-01.wallix.com`	`98.66.169.89`
`relay-fr-02.wallix.com`	`20.39.241.157`

`185.4.44.114` and `185.4.44.117` come into service on 29 September 2026. Authorize them now, in addition to the addresses already in place: add them, do not replace the existing ones, so that your connector keeps working before and after that date.

Authorize all of them, not only the address you observe in use: the platform answers on several of them and the one served to you can change at any time. Keep this list under review, and check it against this page whenever a connector stops connecting.

The `relay-fr-*` entries are only used when the connector goes through the Trustelem relay. If they are already allowed on your firewall, keep them.

If the connector exits through an HTTP proxy, the proxy must allow the `CONNECT` method to these destinations on port 443, and the proxy must not intercept the TLS session (see "TLS inspection" below).

Checking the flows

Run these checks on the machine hosting the connector.

1. Name resolution

```
nslookup admin.trustelem.com
nslookup connect.trustelem.com
```

The answer must be one of the addresses listed above. If it is not, a local override is in place (see "Local DNS override" below).

2. Connectivity test

On Windows, open the Trustelem Connect or ADConnect configuration tool and use the connection test.

On Linux:

```
./connect check <your sync id>
```

or, if you exit through a proxy:

```
./connect check <your sync id> http://proxy.example.local:3128
```

The report shows which step failed:

Result	Meaning
`Network: false`	The connection could not be opened at all: the traffic is blocked or not routed.
`Network: true`, `CanTLS: false`	The connection reaches the server but the TLS session fails: proxy or TLS inspection.
`CommOK: true`	The flows are correct.
`RemoteIP`	The public address your traffic is seen coming from.

A `ping` is not a valid test: ICMP is blocked on most networks, and a successful ping says nothing about port 443, TLS or the proxy.

Common causes of failure

Firewall rules written with IP addresses. By far the most common cause. A rule that lists only part of the addresses above, or an address that is no longer in the list, silently blocks the connector. Symptom: the connection is never established (`Network: false`, timeout). Replace the rule with one based on the DNS names if your equipment supports it.

Proxy allowlist. An outbound proxy that filters the destination of the `CONNECT` method rejects the tunnel even though the name resolves correctly. Symptom: the connector reaches the proxy but the tunnel is refused, usually with a 403.

TLS inspection. The connector authenticates the server with a pinned certificate. Equipment that intercepts and re-signs the TLS session breaks this authentication. Symptom: `Network: true` but `CanTLS: false`. These destinations must be excluded from TLS inspection.

Local DNS override. An entry for a `trustelem.com` name in the `hosts` file of the machine hosting the connector, or a static record in an internal DNS zone or on a forwarder, keeps the connector pointed at an address that is no longer in service. Symptom: the connector resolves an address that is not in the list above. Also check that your resolvers honour the TTL of the records and do not cache them indefinitely.

Routing and tunnel selectors. Policy routes, IPsec traffic selectors or SD-WAN rules that cover only part of the destination addresses send the rest through a path with no NAT or no authorization. Symptom: some addresses answer and others do not.

When a change of network configuration takes effect

A connector holds a long-lived connection. A change on your network, in either direction, is not visible immediately: an already established connector keeps working until its next reconnection, an agent restart or a server reboot, which may be hours later.

After changing a firewall, proxy or DNS rule, restart the connector service to confirm that it can reconnect, rather than waiting for a spontaneous reconnection.

If the connectivity test fails, send the full report to Trustelem support and we will help you identify the blocking equipment.

Revision #1
Created 7 June 2026 08:50:55 by WALLIX Admin
Updated 22 September 2026 10:36:42 by WALLIX Admin