Handbook on what to do if Iceland is disconnected

How much of Atlas Cloud would survive a cable outage?

DATA
Firewall logs, 9 to 25 June 2026 (17 days)

FUNDING
Student Innovation Fund (NSN), grant 2513207-1101

SCOPE
Atlas Cloud's own network, as a case study

About Atlas. Atlas is Iceland's sovereign public cloud: virtual machines, Kubernetes, storage and backups, hosted only in Iceland. **atlascloud.is**

QUESTION AND APPROACH

Iceland reaches the internet through a handful of submarine cables with no overland fallback. The project asked a narrow, measurable question: if every cable failed at once, which of Atlas Cloud's *own* network connections would keep working? Rather than a tabletop exercise, the project built an idempotent Python pipeline over production firewall logs. Each permitted connection is classified by endpoint (Atlas-internal, Atlas-owned, Customer, Anycast, Iceland, Foreign), then labelled **survives** (both ends domestic), **breaks** (a foreign end, or a CDN whose origin is abroad), or **uncertain** (public anycast DNS resolvers such as 1.1.1.1, whose survival depends on an in-country node at RIX).

Of 34.9M permitted events, four days (14, 15, 23 and 24 June) were excluded as unrepresentative. The remaining **13 days hold 2,186,144 Atlas-sourced events**; customer traffic is out of scope.

How to read this report. Atlas is the case study: the measurements and findings describe Atlas's own network. The first steps on page 2 are written for any organisation that runs systems in Iceland.

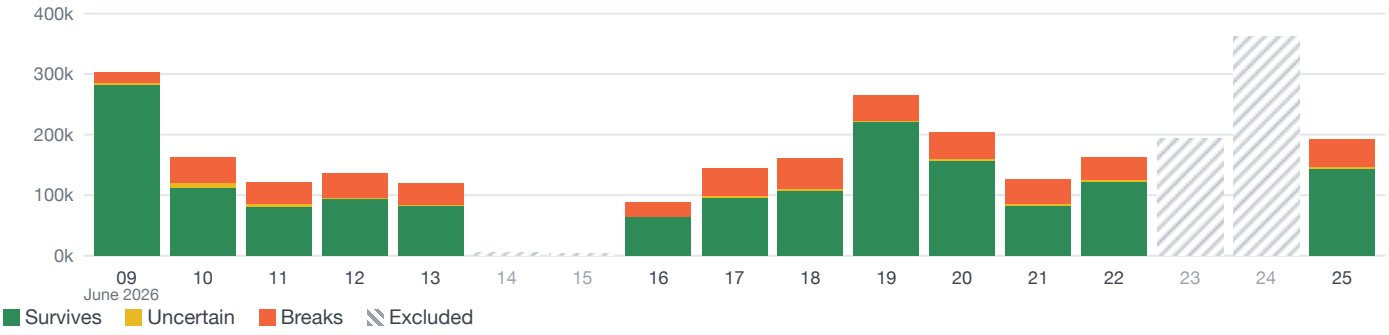
75.3%
Survives: stays in Iceland
1,646,390 events

22.7%
Breaks: foreign or CDN-fronted
497,295 events

1.9%
Uncertain: anycast DNS resolvers
42,459 events

26.7%
Breaks on the median day
(daily range 5.6% to 31.8%)

DAILY ATLAS-SOURCED TRAFFIC BY DISCONNECT OUTCOME



The 22.7% headline is event-weighted and pulled down by two heavy, mostly domestic days (9 and 19 June); excluding them gives 27.1%. "Roughly a quarter to 30% breaks on a normal day" is the more defensible framing.

WHAT BREAKS, AND HOW FAST

DEPENDENCY	EVENTS	IMPACT ON DISCONNECT	FELT WITHIN	LOCAL SUBSTITUTE
Your own foreign-hosted DNS (Cloudflare, AWS, Azure, etc.)	n/a	Domains with nameservers abroad, .is included, stop resolving within minutes as short TTLs expire	Immediate	✓ Yes
Foreign authoritative DNS (Route 53, registries)	130,407	.com/.net names stop resolving as caches expire; .is (ISNIC) survives	Hours	✗ No
OS package updates	127,316	OS patching stalls	Weeks	✓ Yes
Foreign NTP (port 123)	126,176	Clock drift; TLS, Kerberos and logs degrade over time	Weeks	✓ Yes
Remote-access relay (London)	128,697	Mostly keepalives; peers in Iceland may connect directly, but the foreign control plane blocks new sessions	Varies	✓ Yes
Public anycast resolvers (mostly 1.1.1.1)	42,459	Hosts pointing only at 1.1.1.1 lose *all* name resolution, including Icelandic names	Uncertain	✓ Yes
GitHub (AS36459)	27,343	Source control and CI stop	Weeks	✓ Yes

Counts are firewall events, not bytes or business value: chatty keepalive protocols are over-weighted and bulk transfers under-weighted, so rows are ranked by kind and failure tempo, not volume.

This is a public report for the public good and may be shared freely under **CC BY 4.0**.

KEY FINDINGS

1. **Exposure is real but bounded.** Roughly three quarters of Atlas's own traffic never leaves Iceland. The rest traces to a short, named list of dependencies, not a vulnerability spread across the estate.
2. **DNS is the only hard, fast-failing dependency.** Atlas both recurses directly to foreign authoritative nameservers (certain failure) and forwards about 25% of lookups to Cloudflare 1.1.1.1 (uncertain). A 1.1.1.1 outage alone, cables intact, would blind any host configured with it as sole resolver.
3. **Most breaking traffic has a domestic substitute.** Time sync, OS package mirrors, source control and remote access can all be pointed at local sources. Authoritative DNS for foreign domains cannot: those nameservers and their targets are abroad by definition.
4. **Customers are likely more exposed than Atlas.** Firewall-wide figures that include customer traffic show higher exposure than Atlas's own traffic. Customer traffic was outside this study's scope.

WHAT TO DO IF ICELAND IS DISCONNECTED: THE FIRST STEPS

Every step must be in place **before** a disconnect. None can be set up once the cables are down.

#	ACTION	ADDRESSES
1	Run a domestic recursive resolver and configure it as primary or fallback on every host; never rely on 1.1.1.1 alone	Hours-tier DNS failure; 1.1.1.1 blast radius
2	Domestic time source (local stratum-1 or Icelandic NTP pool) for all hosts	Clock sync
3	Local OS mirror, kept in sync while connected	OS patching
4	Run identity and remote-access services in Iceland: a self-hosted identity provider (e.g. Keycloak or Authentik) and self-hosted coordination and relay servers for the VPN	Logins and remote access without a foreign control plane
5	Replace source control with a local alternative: a self-hosted Git forge (e.g. Forgejo or GitLab) mirroring GitHub, with local CI runners	Source control and CI
6	If you host systems for others, offer them a domestic resolver too	Customer exposure (finding 4)

WHAT IS MISSING

Open questions

- **HTTPS deep dive.** Dependencies on port 443 (remote-access control planes, monitoring checks, vendor telemetry, cloud-hosted APIs) cannot be told apart by port and need flow or host-level analysis.
- **Which anycast resolver answers locally.** Whether 1.1.1.1, Google and Quad9 are served from a node in Iceland decides the uncertain bucket.
- **A local resolver as an option.** Assess a domestic recursive resolver as primary or fallback and measure how much of the DNS exposure it removes.
- **Event counts, not bytes or criticality.** A chatty keepalive and a critical nightly backup weigh the same today. Volume and business impact per dependency are still unmeasured.
- **Customer traffic.** Atlas customers' own dependencies were out of scope and need a separate analysis.

Improving the data going forward

- **Export flows with byte counts** (NetFlow/IPFIX from the firewall) so dependencies can be ranked by volume, not only by connection count.
- **Log DNS queries and TLS server names** at the resolver and proxy, so HTTPS traffic can be attributed to a named service instead of an IP range.
- **Map hosts to services and owners** in an inventory, so each dependency translates to the business function that stops when it breaks.
- **Collect continuously** across months rather than weeks, to catch monthly and quarterly jobs, and from more vantage points than one firewall.
- **Validate with a controlled cut-off**: block foreign egress for a test segment and compare observed failures with the predicted ones.

ATLAS This is a public report for the public good and may be shared freely under **CC BY 4.0**.