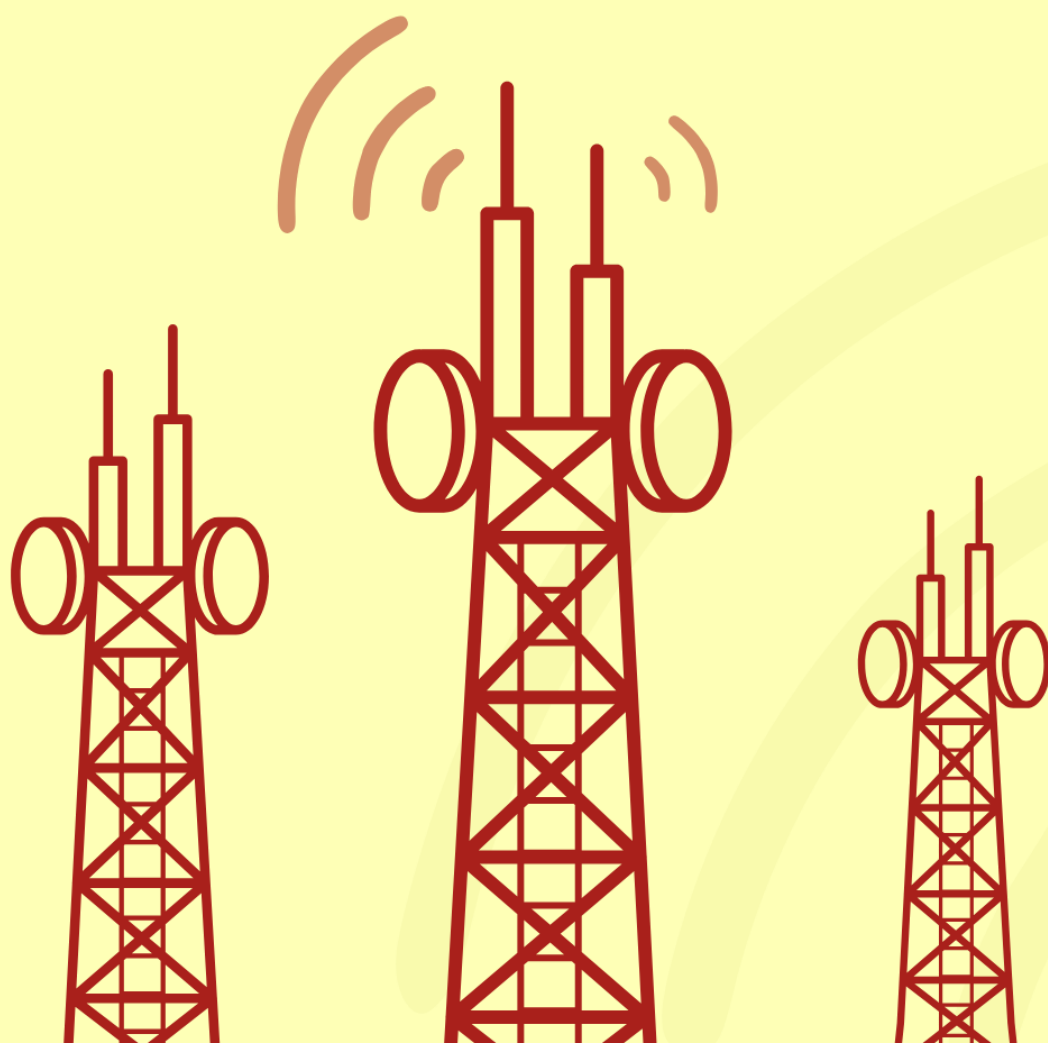


PANDUAN

REAKSI TERHADAP
GANGGUAN AKSES
INTERNET DAN
SENSOR/BLOKIR
SAAT BERAKTIVITAS





SAFE net

Defending Digital Rights in Southeast Asia

PANDUAN

REAKSI TERHADAP GANGGUAN AKSES INTERNET DAN SENSOR/BLOKIR SAAT BERAKTIVITAS

Kenali • Pahami Jenisnya • Siapkan • Deteksi • Bereaksi • Laporkan

1. Pendahuluan

Akses internet adalah prasyarat kebebasan berekspresi, hak atas informasi, dan partisipasi publik. SAFEnet, organisasi masyarakat sipil pembela hak-hak digital di Asia Tenggara, mendefinisikan hak-hak digital sebagai hak asasi manusia yang berlaku di ranah digital — mencakup hak untuk mengakses internet (right to access), hak untuk bebas berekspresi (right to express), dan hak atas rasa aman (right on safety). Pelanggaran hak-hak digital dipahami sebagai segala upaya yang secara sengaja mengganggu terpenuhinya hak-hak tersebut — termasuk pembatasan akses internet, pemidanaan ekspresi, serangan terhadap aset digital, dan pelanggaran privasi.

Panduan ini disusun oleh SAFEnet agar setiap orang — warga biasa, aktivis, jurnalis, mahasiswa, maupun pengelola komunitas — memahami jenis-jenis gangguan akses internet dan tahu persis apa yang harus dilakukan saat mengalami atau menemukannya: baik saat beraktivitas di lapangan, maupun saat menjalani keseharian sebagai warganet.

1.1 Tujuan dan Sasaran

- **Tujuan umum:** membekali pengguna internet dengan pemahaman tentang ragam gangguan akses serta kemampuan mengenali, mendokumentasikan, dan melaporkannya sebagai bagian dari pembelaan hak-hak digital.
- **Tujuan khusus:** (a) memahami definisi dan kategori gangguan akses menurut SAFEnet; (b) mengenal satu per satu jenis gangguan — dari sensor konten hingga shutdown total; (c) mampu menggunakan alat deteksi seperti OONI Probe; (d) memiliki prosedur reaksi untuk tiap jenis insiden; (e) mengetahui kanal pengaduan yang tepat.
- **Sasaran:** warga pengguna internet secara umum, pembela HAM, jurnalis dan pers mahasiswa, organisasi masyarakat sipil, peserta aksi, serta pengelola komunitas — tanpa memerlukan latar belakang teknis.

1.2 Cakupan Isi

- Definisi gangguan akses internet menurut SAFEnet dan kategori pemantauannya (infrastruktur, layanan, kebijakan).
- Elaborasi satu per satu jenis gangguan: sensor/blokir situs, blokir konten spesifik, pembatasan platform, throttling, shutdown lokal, shutdown total.
- Jenis-jenis internet shutdown dan pihak yang biasanya bertanggung jawab.
- Persiapan sebelum beraktivitas, alat deteksi OONI Probe (dengan tangkapan layar), dan SOP reaksi per jenis insiden.
- Empat skenario nyata — termasuk skenario warga biasa, bukan hanya peserta aksi — lengkap dengan langkah tindak lanjutnya.
- Kanal pelaporan dan advokasi.

2. Definisi Gangguan Akses Internet

SAFEnet mengelompokkan gangguan terhadap hak akses internet ke dalam tiga kategori berikut ini.

Kategori	Definisi
Infrastruktur	Akses terganggu karena masalah infrastruktur, seperti jaringan telekomunikasi bermasalah atau tidak berfungsi sebagaimana mestinya, maupun tidak adanya operator/blankspot. Ini merupakan perspektif tanggung jawab penyedia layanan dan pemerintah.
Kebijakan	Akses terganggu karena masalah regulasi dan kebijakan, misalnya aturan UU ITE dan aturan terkait, kebijakan pemerintah pusat/daerah yang membatasi/memblokir akses layanan, termasuk kebijakan platform digital yang membatasi dan/atau menghapus konten/akun. Termasuk kebijakan platform men-takedown konten, men-suspend, atau mem-banned berdasarkan standar komunitas kebijakan platform maupun atas permintaan pemerintah.
Layanan	Akses terganggu karena masalah ketidakmampuan mengakses layanan oleh masyarakat — misalnya biaya layanan mahal, diskriminatif, atau tidak ramah

Kategori	Definisi
	terhadap golongan rentan, disabilitas, dan miskin; termasuk lambannya atau bermasalahnya operator/customer service dalam berkomunikasi dan merespons pengguna. Kategori ini berperspektif masyarakat/pengguna.

2.1 Definisi Pelanggaran Hak Akses

PELANGGARAN HAK AKSES

Pelanggaran hak untuk akses internet dibatasi pada kondisi di mana terjadi hambatan dalam upaya mengakses internet pada suatu tempat tertentu dan jangka waktu tertentu, oleh kelompok masyarakat tertentu, yang diakibatkan oleh faktor kesengajaan, pengabaian, kelalaian, dan/atau kelambanan dari aktor pemerintah atau aktor non-pemerintah terkait layanan internet.

2.2 Kategori Dampak

Dampak dari gangguan akses dikategorikan ke dalam empat area berikut:

Kategori Dampak	Contoh Dampak
Komunikasi	Warga tidak bisa menghubungi keluarga/kolega, koordinasi bantuan darurat terputus, informasi krisis tidak sampai ke masyarakat.
Ekonomi	Transaksi digital dan UMKM daring terhenti, pekerja lepas/daring kehilangan penghasilan, biaya tambahan untuk akses alternatif (mis. Starlink berbayar per jam saat darurat).
Pelayanan	Layanan publik berbasis digital tidak dapat diakses, respons aduan ke penyedia layanan lambat, warga di wilayah adat/3T terhambat berpartisipasi karena layanan intrusif tapi tidak inklusif.
Pendidikan	Pembelajaran jarak jauh (PJJ) terputus, siswa/mahasiswa di daerah blankspot tertinggal akses materi dan ujian daring.

2.3 Contoh dari Ketiga Kategori

- **Infrastruktur:** putusnya kabel bawah laut yang membuat Papua tanpa akses internet berminggu-minggu; kerusakan massal BTS akibat bencana alam (banjir, gempa); penghentian layanan internet gratis publik seperti JakWifi yang memutus akses warga kalangan bawah.
- **Kebijakan:** pemutusan/pencekikan akses internet di Papua pada 2019 dengan dalih stabilitas keamanan (kemudian diputus PTUN sebagai perbuatan melanggar hukum); pemblokiran situs karena UU ITE atau aturan turunannya; pemblokiran domain layanan otentikasi Wikimedia oleh pemerintah; gangguan akses di sekitar lokasi aksi/protes; penangguhan akun ormas/organisasi oleh platform media sosial; penghapusan (takedown) konten oleh platform berdasarkan standar komunitasnya sendiri maupun atas permintaan pemerintah; pembatasan fitur tertentu oleh platform (mis. penangguhan sementara fitur siaran langsung) selama periode aksi/unjuk rasa.
- **Layanan:** biaya paket data/internet yang tidak terjangkau bagi warga berpenghasilan rendah; kualitas jaringan yang timpang antarwilayah (kota besar vs 3T); aplikasi atau situs layanan publik yang tidak ramah pengguna disabilitas (tanpa dukungan pembaca layar, kontras rendah, dsb.); operator/customer service yang lamban merespons keluhan atau sulit dihubungi saat terjadi gangguan; masyarakat adat/kelompok rentan yang tersingkir dari layanan digital karena digitalisasi yang intrusif tapi tidak inklusif.

3. Jenis-Jenis Gangguan Akses

Rentang gangguan akses sangat luas — dari yang menyasar satu konten saja hingga yang mematikan seluruh jaringan suatu wilayah. Berikut elaborasi tiap jenisnya, disusun dari yang paling spesifik ke yang paling luas dampaknya.

Konten dihapus / akun dikunci	Blokir situs & aplikasi	Throttling (pelambatan)	Shutdown lokal / mobile	Shutdown total
-------------------------------	-------------------------	-------------------------	-------------------------	----------------

Spektrum gangguan akses — dampak & skala pelanggaran makin besar ke kanan

3.1 Sensor & Pemblokiran Konten Spesifik (Takedown)

Bentuk paling sempit: satu unggahan, video, atau utas dihapus, atau satu akun dikunci/ditangguhkan oleh platform — baik atas inisiatif platform sendiri maupun memenuhi permintaan pemerintah. SAFEnet mencatat adanya permintaan penghapusan konten dari otoritas yang sebagian besar menyasar kritik warganet biasa terhadap kebijakan pemerintah, bukan konten disinformasi atau ujaran kebencian sebagaimana dalih yang biasa dipakai.

3.2 Pemblokiran Situs dan Aplikasi

Satu atau beberapa situs/aplikasi tertentu tidak bisa diakses — lewat manipulasi DNS, pemblokiran alamat IP, atau filtering URL. Biasanya dieksekusi ISP atas perintah otoritas (di Indonesia oleh Komdigi lewat sistem pemantauan otomatis). Pemblokiran bisa tepat sasaran (situs judi/pornografi ilegal) maupun salah sasaran (situs sah ikut terblokir karena filter otomatis yang terlalu luas).

3.3 Pembatasan Akses Platform

Satu platform secara keseluruhan (media sosial, aplikasi pesan) dibatasi atau diblokir sementara — dampaknya mirip shutdown parsial karena banyak orang bergantung pada satu platform untuk berkomunikasi maupun mengakses berita. Contoh internasional: pemblokiran seluruh media sosial di Chad selama 16 bulan.

3.4 Throttling (Pencekikan Jaringan)

Koneksi sengaja diperlambat sehingga layanan — biasanya media sosial atau berbagi video — praktis tak terpakai, tanpa mematikannya sepenuhnya. Paling sulit dibuktikan karena mirip gangguan teknis biasa; beberapa negara secara terbuka memerintahkan operator melakukan ini untuk mencegah penyebaran gambar/video tertentu.

3.5 Internet Shutdown Lokal / Mobile

Jaringan seluler dan/atau data internet dimatikan di wilayah tertentu — sering di sekitar lokasi aksi, konflik, atau daerah spesifik — sementara wilayah lain tetap normal. Telepon dan SMS biasa kadang masih berfungsi karena berjalan di jaringan berbeda.

3.6 Internet Shutdown Total

Seluruh konektivitas suatu wilayah atau negara padam — bentuk paling ekstrem dan paling mudah dikenali, namun juga paling merugikan karena memutus seluruh layanan publik, ekonomi, dan komunikasi darurat sekaligus.

4. Jenis-Jenis Internet Shutdown & Siapa Bertanggung Jawab

SAFEnet, mengutip riset Freedom House, membedakan tiga istilah pembatasan internet yang sering dipertukarkan padahal berbeda mekanismenya:

- **Pemutusan/Pemadaman (Shutdown/Blackout):** konektivitas nyaris nol — semua platform, aplikasi pesan, dan situs tak bisa diakses sama sekali. Bisa berskala nasional (seluruh negara) atau menyasar wilayah tertentu saja.
- **Pencekikan (Throttling):** jaringan diperlambat, bukan dimatikan — bisa menyasar seluruh koneksi atau hanya aplikasi/situs tertentu.
- **Pemblokiran (Blocking):** menyasar materi atau platform tertentu, bukan seluruh konektivitas — namun jika yang diblokir adalah platform utama komunikasi warga, dampaknya bisa menyerupai shutdown.

4.1 Siapa yang melakukan?

- **Perintah kepada ISP:** pemerintah meminta penyedia layanan internet mematuhi keputusan/pemblokiran; ISP umumnya patuh karena khawatir kehilangan izin operasi meski rugi secara finansial.
- **Perintah kepada platform:** pemerintah meminta penyelenggara sistem elektronik (PSE) untuk melakukan keputusan konten, penurunan konten, penangguhan akun, dan konten, baik langsung maupun tidak langsung melalui algoritma (shadowban); PSE umumnya patuh karena khawatir akan denda dan sanksi yang akan merugikan secara finansial.
- **Infrastruktur yang dikontrol negara:** di negara dengan penyedia telekomunikasi milik pemerintah, pembatasan bisa dilakukan langsung tanpa perantara swasta.

4.2 Kapan biasanya terjadi?

Aksi massa / protes	Pemilu & pengumuman hasil	Kerusuhan / operasi keamanan	Sidang / putusan sensitif	Kunjungan pejabat
---------------------	---------------------------	------------------------------	---------------------------	-------------------

Jendela risiko — lakukan mitigasi SEBELUM momen-momen ini

Pemicu paling umum: protes/aksi massa, pemilu dan pengumuman hasilnya, konflik dan operasi keamanan, ujian nasional, hingga kunjungan pejabat. Pemerintah biasanya beralih menjaga stabilitas atau mencegah penyebaran hoaks — meski Pernyataan Bersama PBB 2015 menegaskan bahwa pemadaman jaringan tidak bisa dibenarkan dalam hukum HAM internasional, apa pun alasannya.

5. Sebelum Beraktivitas: Persiapan dan Mitigasi

Ketika shutdown sudah terjadi, biasanya sudah terlambat untuk bersiap. Mitigasi dilakukan SEBELUM momen berisiko.

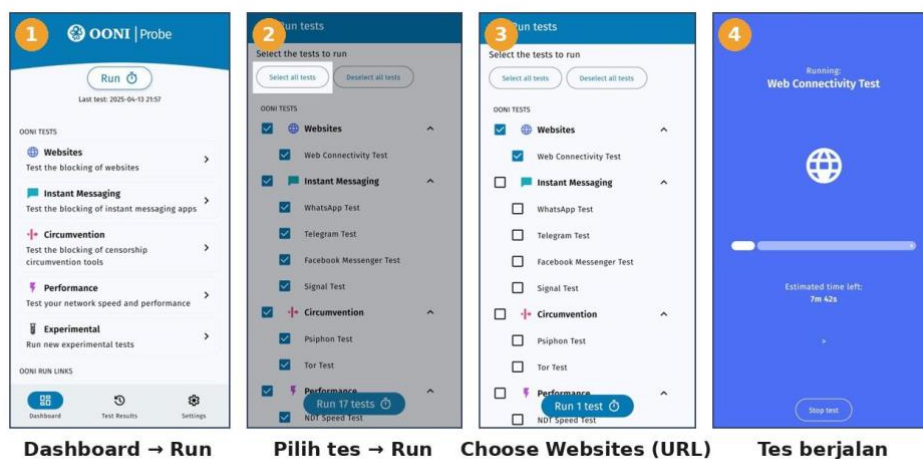
Checklist Siap-Siaga	Keterangan
☒ 2 VPN terpercaya	Psiphon, TunnelBear, RiseupVPN, Tor Browser — pasang minimal dua
☒ OONI Probe	terpasang untuk deteksi & bukti pemblokiran
☒ Aplikasi mesh	mis. Briar, untuk komunikasi tanpa internet
☒ Rencana komunikasi cadangan	pohon kontak & titik kumpul fisik
☒ 2FA aktif	kode cadangan disimpan luring
☒ Backup data	cadangkan data penting sebelum berangkat

- **VPN terpercaya:** pasang minimal dua (Psiphon, TunnelBear, RiseupVPN, Tor Browser) sebelum berangkat.
- **Rencana komunikasi cadangan:** pohon kontak (phone tree), titik kumpul fisik, satu penghubung di luar lokasi, aplikasi mesh seperti Briar.
- **Amankan akun:** aktifkan 2FA, simpan kode cadangan secara luring, perbarui kontak pemulihan.

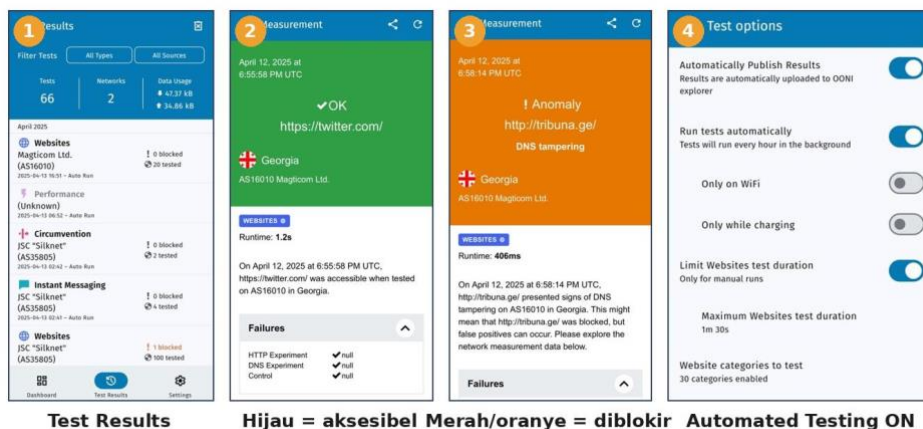
6. Alat Deteksi: OONI Probe

OONI Probe (gratis, open source) menguji apakah situs, aplikasi pesan instan, atau VPN diblokir di jaringan Anda. Hasilnya otomatis dipublikasikan di OONI Explorer — basis data sensor internet terbuka terbesar di dunia — sehingga bisa dipakai sebagai bukti dalam advokasi maupun litigasi.

No	Langkah	Detail
1	Unduh	ooni.org/install — tersedia untuk Android, iOS, dan Desktop (Windows/macOS/Linux)
2	Matikan VPN	Matikan VPN & iCloud Private Relay sebelum menjalankan tes agar hasil akurat
3	Jalankan tes (Run)	Pilih Websites / Choose Websites untuk menguji URL tertentu
4	Bagikan bukti	Show in OONI Explorer → tautan bukti publik yang dapat dibagikan
5	Otomatiskan	Aktifkan Automated Testing di Settings untuk pengukuran berkala



Langkah di aplikasi: Dashboard → Run → Choose Websites → tes berjalan. (Sumber: ooni.org)



Melihat hasil & mengaktifkan Automated Testing. (Sumber: ooni.org)

Warna	Status	Arti
Hijau	DAPAT DIAKSES	Situs normal, tidak ada indikasi gangguan
Oranye	ANOMALI / LIKELY BLOCKED	Kemungkinan diblokir — waspadai false positive
Merah	TERKONFIRMASI DIBLOKIR	Halaman blokir / DNS sensor terdeteksi

PENTING SEBELUM TES

- Matikan VPN dan iCloud Private Relay — kalau tidak, hasil tidak akurat.
- ISP/pemerintah/kantor dapat melihat Anda menjalankan OONI dan situs yang diuji — timbang risiko keamanan Anda.
- Uji dari beberapa ISP; perhatikan kuota. Alat pendukung: IODA (ioda.live) & Cloudflare Radar untuk memantau pemadaman infrastruktur.

7. SOP: Mendapati Internet Shutdown

No	Langkah	Tindakan
1	Verifikasi	Cek perangkat lain, ISP lain, tanya sekitar; bandingkan dengan IODA/Cloudflare Radar.
2	Dokumentasikan	Catat jam, lokasi, operator, jenis gangguan; screenshot galat & hasil OONI/speedtest. Simpan luring.
3	Tetap terhubung	VPN (untuk blokir platform), SIM operator lain, tethering, Briar (mesh), SMS/telepon biasa.
4	Laporkan	Begitu ada jalur komunikasi, laporkan ke kanal Bab 10.
5	Advokasi	Setelah terverifikasi, sebarkan bukti dan desak transparansi.

KASUS: Shutdown Papua 2019 — dan kemenangannya di pengadilan

Agustus–September 2019: pemerintah melakukan pencekikan lalu memutus layanan data internet di Papua & Papua Barat di tengah gelombang protes, dengan dalih stabilitas keamanan. SAFEnet bersama AJI menggugat ke PTUN Jakarta — dan Juni 2020 pengadilan memutus tindakan itu sebagai perbuatan melanggar hukum. Dokumentasi teknis dan laporan warga menjadi bahan baku kemenangan ini.

8. SOP: Mendapati Sensor & Pemblokiran

Mendapati gangguan pada situs, akun, atau konten? Ikuti alur berikut sesuai jenis yang dialami:

Situs Diblokir (halaman blokir/DNS)	Postingan Dihapus / Akun Dikunci Platform	Akun Diduga Diretas
• Uji OONI Probe pada URL tersebut • Simpan screenshot & tautan OONI Explorer • Ajukan normalisasi ke aduankonten.id • Laporkan ke aduan.safenet.or.id	• Ajukan banding (appeal) resmi ke platform • Simpan nomor tiket pengaduan • Eskalasi via SAFEnet jika menyangkut ekspresi sah	• Amankan email, ganti kata sandi • Cabut semua sesi aktif • Gunakan formulir pemulihan resmi platform • Hubungi helpline keamanan digital

- **Uji & buktikan:** jalankan tes Websites OONI pada URL tersebut; simpan tautan OONI Explorer + screenshot (tanggal, jam, ISP).
- **Banding ke platform:** jika konten dihapus/akun dikunci, gunakan mekanisme banding resmi; simpan nomor tiket. Eskalasi via SAFEnet bila menyangkut ekspresi sah.

- **Ajukan keberatan ke otoritas:** jika situs diblokir negara, ajukan normalisasi lewat Komdigi (aduankonten.id); minta dasar hukum dan transparansi.
- **Bagikan & advokasi:** publikasikan temuan terbukti di medsos, ajak orang menguji lewat tautan OONI Run, desak koreksi cepat.

KASUS DI INDONESIA

- **Magdalene.co:** media berperspektif gender tersaring filter pemblokiran otomatis di sejumlah ISP — akses pulih setelah protes publik.
- **Aliansi Mahasiswa Papua:** situsnya diblokir tanpa transparansi dasar hukum; pengukuran OONI mendokumentasikannya lintas ISP.
- **False positive mesin AIS:** sistem otomatis Komdigi pernah keliru memblokir layanan sah, termasuk domain Google. Laporan warga mempercepat koreksi.

9. Skenario Nyata: Bukan Hanya Peserta Aksi

Gangguan akses tidak hanya dialami peserta aksi. Warga biasa yang sedang bekerja, belajar, atau sekadar berselancar juga bisa mengalaminya. Berikut empat skenario dan langkah konkretnya.

	Situasi	Contoh	Langkah
A	Sedang di lokasi aksi/protes	Internet seluler tiba-tiba mati di sekitar lokasi aksi, sementara di luar area itu normal.	Ikuti SOP Bab 7: verifikasi → dokumentasi → jalur alternatif → lapor → sebarkan bukti.
B	Mendengar kabar ada situs/domain diblokir	Kasus 2026: domain otentikasi Wikimedia sempat diblokir; atau pemblokiran massal situs judi turut menyeret layanan sah.	Uji sendiri lewat OONI Probe; jika benar & situs sah, laporkan ke aduankonten.id untuk normalisasi dan ke SAFEnet sebagai data advokasi.
C	Internet lambat/mati sehari-hari di daerah	Warga di Papua/wilayah 3T mengalami internet mati sehari-hari akibat kabel laut putus/BTS rusak — kategori infrastruktur/layanan, bukan sensor.	Catat tanggal, operator, dampaknya; laporkan ke SAFEnet; cek dashboard IODA untuk mendesak percepatan perbaikan.
D	Konten dihapus/akun dibatasi setelah mengkritik kebijakan	Warganet mengunggah kritik kebijakan, lalu kontennya dihapus atau akunnya dibatasi — pola yang menurut SAFEnet kerap menysar kritik warga biasa.	Simpan bukti (screenshot, isi asli, waktu); ajukan banding resmi; laporkan ke SAFEnet dan LBH Pers untuk pendampingan.

10. Kanal Pelaporan dan Bantuan

Tabel berikut dapat Anda perbarui sendiri — tambahkan, ubah, atau hapus baris sesuai kebutuhan.

Lembaga	Fokus	Kontak
SAFEnet	Pelanggaran hak-hak digital	aduan.safenet.or.id
BSSN	Insiden siber	bsn.go.id/aduan-siber tel. 021 78833610 bantuan70@bsn.go.id
Komdigi	Konten negatif & normalisasi pemblokiran	aduankonten.id

Lembaga	Fokus	Kontak
Komnas Perempuan	Kekerasan berbasis gender online (KBGO)	komnasperempuan.go.id tel. 021-3903963
LBH Pers	Kekerasan terhadap jurnalis/pers	lapor.lbhpers.org
LBH APIK	Kekerasan berbasis gender & bantuan hukum	lbhapik.or.id/pengaduan
Komnas HAM	Pelanggaran HAM	pengaduan.komnasham.go.id
Access Now Helpline	Keamanan digital (24/7)	help@accessnow.org
#KeepItOn	Alert internet shutdown	shutdownalert@accessnow.org

Simpan panduan ini dan sebarkan ke komunitas Anda.

*Disusun oleh Divisi Akses Internet SAFEnet • boleh disebarluaskan nonkomersial dengan atribusi (CC BY-SA 4.0).
 Sumber acuan definisi kategori gangguan akses & pelanggaran hak akses: SAFEnet. Sumber acuan istilah pembatasan internet: SAFEnet, alih bahasa dari riset Freedom House (2019); AccessNow #KeepItOn.*