SMALL MEDIA

IRANIAN INTERNET INFRASTRUCTURE AND POLICY REPORT

// March - April 2013
// www.smallmedia.org.uk

INTRODUCTION

// Prior to the public demonstrations of the Green Movement four years ago, the common narrative of Iran's political environment was that elections meant the loosening of control over the public sphere. These theories held that by allowing room for some measure of discourse on political and social issues, the government was able to encourage participation in elections and secure public legitimacy. However, having faced the largest serious threat to the status quo in recent years, the following election, the Parliamentary election held early last year, left no question that the rules had changed, and that security now trumps participation.

In previous reports we had begun to describe the systemic pattern of the filtering of content associated with or promoting mainstream political figures who nevertheless clash with the core elites. While often not nearly as dramatic as the blocking of circumvention tools, these patterns align with the increased filtering of domestic content performed without clear cause or explanation. Moreover, these actions often appear arbitrary or sweeping, targeting personal blogs seemingly as equally as large audience advocacy sites or partisan news sources. If the trend of the Parliamentary election holds, while official sites for vetted but marginalized candidates will remain unblocked, popular sites run independently by supporters will be more frequently subject to filtering.

At the time of publication, nearly none of the tools designed to support access to censored content or protect privacy are working. The filtering apparatus has shifted the paradigm of how it handles international traffic in a dramatic fashion – connections that do not fall within a specified set of approved applications are subject to termination and throttling. These conditions defy basic assumptions and create significant obstacles for developers of accessibility. They also fly in the face of the broad adoption of blocked social networking platforms by both establishment and marginalized candidates, although these accounts are deemed 'independent fan accounts' despite being sophisticated in content and well coordinated on messaging.

More broadly, mechanisms core to the Internet and designed to ensure the integrity of communications between users and end hosts are now being universally disrupted, regardless of the purpose. Iran's Internet is further defining the label given to it by Iranian social media users and bloggers, the "Filternet." As the vetting process is finalized and the first round of voting quickly approaches, the fundamental ability to communicate online is more at-risk by the actions of the censorship regime and less bolstered by software developers than ever.

POLICY DEVELOPMENTS

CONTENT FILTERING AND BLOCKED SITES

- **MARCH - MAY:** Campaign sites and personal blogs supportive of President Ahmadinejad, former President Seyed Mohammad Khatami and Presidential candidate Esfandiar Rahim Mashaei hosted on Iranian-owned platforms, such as khataminews.blogfa.com, are increasingly subject to blocking or removal.

- **APRIL 4:** SMS messages containing the word 'Mashaei (مشایی),' a reference to the candidate, were reportedly blocked by telecommunication providers. Attempts to send messages containing the keyword were shown as delivered but the recipients would not receive the text. After a few hours, the blocking ended without any explanation from the authorities. This follows previous instances where bulk messages containing slogans associated with Mashaei and Ahmadinejad were blocked. (Source)

- **APRIL 10:** Qazvin Cyber Police announced the arrest of an individual for the sale of circumvention tools. (Source)

- **APRIL 10:** IRINN notes that the Wikipedia page for Ahmadinejad was blocked, apparently due to 'insults' against the president. Abdolsamad Khoramabadi, head of the Commission to Determine the Instances of Criminal Content (CDICC), stated that page was blocked 16 months ago. Independent tests on May 15 2013 show the Persian-language version is filtered, but the English page is not, and that the blocking has been in place since at least December 2012. (Source)

- **APRIL 11:** The newspaper Haft Sobh published a report on the blocking of Viber, ooVoo, Skype and Yahoo Messenger across Iran's largest ISPs. It appears that while most providers currently block all four communication services, the Telecommunication Company of Iran's (TCI) consumer-facing ISP continues to allow them. (Source)

ISP	VIBER	OOVOO	YAHOO!MESSENGER
Shatel	B	B	B
ParsOnline	B	B	U
Datak	B	B	U
AsianTech	B	B	U
TCI	U	U	U
Irancell	B	B	B
Mobinnet	U	B	U

(B = BLOCKED/U=UNBLOCKED)

- **APRIL 12:** Moj11.ir, an online campaign to support Khatami in the election became unavailable shortly after launch (Source). While the domain still exists and is pointed to the Canadian-hosted, Iranian-owned provider Mizban Market, no records exist for the domain. This subject that the site was removed by Mizban.

- **APRIL 19:** SalamKhatami.com, a reformist site launched to petition Khatami to participate in the elections, is launched and then blocked after 8 days and more than 20,000 signatures (Source: 1, 2). Additionally, SalamKhatami.org, the complementary news blog, was blocked 4 days after launch. (Source)

- **APRIL 21:** Reforms.ir, a reformist news site covering the election, is blocked on several ISPs (Source). Attempts to reach reforms.ir from outside of the country sporadically return the filtered site page. We have noted in previous reports that this ingress filtering is rare.

- **MAY 1:** The CDICC publishes an addon for Firefox to allow users to report criminal websites, and promotes its use on Internet.ir. The plugin appears to be a simple link to a simplified version of the normal reporting page, and is labeled "meisam_zahedi." After news caught onto social media, Iranians inside and outside began to report it to Mozilla. Within days the name was changed from "Filter_Internet_Ir" to "Anti Spam-internet.ir," then removed shortly thereafter. (Source)

POLICIES

- **MARCH 31**: The Cyber Police (FATA) published new regulations on the operations of Internet cafés, which includes articles such as: (Source)
  - Businesses must purchase upstream bandwidth from authorized ISPs - buying connectivity from satellite-based ISPs is illegal;
  - The owners of Internet cafés must be at least 25 years old and married;
  - Internet cafés must request ID from each user, and record personal information such as:
    i First and last name,
    ii Father's name,
    iii Number of national ID card,
    iv Postcode,
    v Phone number.
  - Internet cafés must store the date, time, IP addresses and log files of each user for at least six months;
  - Use of any circumvention tool or VPN is illegal, and the business must not install them;
  - CCTV must be installed and all data must be kept for six months;
  - Internet cafés must check their computers after working hours for keyloggers and malware.

STATEMENTS FROM MINISTRIES

- **APRIL 10:** Mohammad Hassan Nami, head of the Ministry of Information and Communications Technology, announced that Iran will launch 'Basir,' the 'Islamic Google Earth,' in the next fours months. According the interview published by Tafahom News, the main difference between the two services is that "Basir will help people to find the truth and Irwn does not to make profit for it." Nami also stated that the Internet will not be cut in 1392 (2013/14). (Source)

- **APRIL 17:** Seyyed Mohammad Reza Aghamiri, member of the CDICC, announced that around 1,500 "anti-religious websites," such as pro-Wahhabi or Baha'i content, are blocked per month. (Source)

STATEMENTS FROM MINISTRIES

- **APRIL 10:** Mohammad Hassan Nami, head of the Ministry of Information and Communications Technology, announced that Iran will launch 'Basir,' the 'Islamic Google Earth,' in the next fours months. According to an interview published by Tafahom News, the main difference between the two services is that "Basir will help people to find the truth and Irwn does not to make profit for it." Nami also stated that the Internet will not be disconnected in 1392 (2013/14). (Source)

- **APRIL 17:** Seyyed Mohammad Reza Aghamiri, member of the CDICC, announced that around 1,500 "anti-religious websites," such as pro-Wahhabi or Baha'i content, are blocked per month. (Source)

- **APRIL 5:** In an interview with Young Journalists Club, MP Mousa Ghazanfarabadi said that use of circumvention tools to bypass the filtering system is a crime, but using social networks is not illegal until the users act against Islam and the Islamic Revolution. (Source)

- **APRIL 7:** The National Internet Development Center (NID) published new stats about the number of Internet users in Iran. According to the numbers, Iran has passed 45 million users with an Internet penetration of 60%. There remain doubts about these numbers, due to the definition of connectivity used. For example, use of Internet cafés is counted. According to the NID statistics:
  - 28 millions users have connected to the Internet via GPRS;
  - 7 millions have connected via dial up;
  - 6 millions have connected via fiber optic, such as through a university or office place;
  - 3.5 millions have connected via ADSL;
  - 900,000 users have connected via WIMAX. (Source)

- **APRIL 13:** In an interview with Borna, MP Allahyar Malekshahi stated that distributing circumvention tools and teaching about bypassing the filtering system is a crime, but using social networks is not illegal, and the user should not be worried about using Facebook or Twitter. (Source)

- **APRIL 18:** Ayyob Haghighi, the deputy head of committee in charge of organizing the upcoming election, said that 170 websites are run by the opposition and opponents of the regime to affect the elections. (Source)

- **APRIL 20:** Mahmood Khosravi, director of the Telecommunication Infrastructure Company (TIC) bandwidth monopoly, confirmed the TIC has previously limited Gmail, but is not currently restricted in any manner. (Source)

CIVIL SOCIETY, PROFESSIONAL ORGANIZATION STATEMENTS

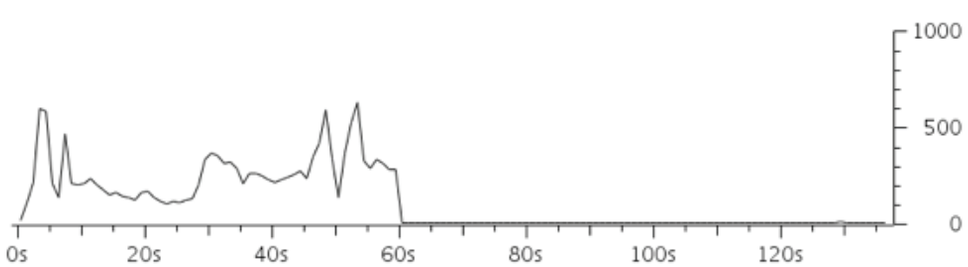
- **APRIL 4:** The Psychological Association of Qom hawza (PAQH) sent a letter to the Cultural Commission of the Parliament to request the 3G service of RighTel be stopped for Islamic and shariah reasons. According to the letter, the PAQH believes the video call feature will 'destroy Iranian families and increase immorality amongst the Iranian youth, because they can have a video call without any problems with others, especially opposite gender.' (Source)

TECHNICAL DEVELOPMENTS

NEW FILTERING RULES

After the March 8 blocking of most VPN protocols, the public quickly shifted into a different set of well-known tools, such as Psiphon, Freegate and Kerio VPN. Almost exactly two months later, on May 5, users began to report on social media and blogs that access to these and other anti-filtering services was severely limited.

TCP and UDP connections that traverse the international gateway are now blocked from exchanging traffic after exactly 60 seconds, and further attempts to connect on the same destination port is prevented for an undetermined amount of time (Source). The disruptions of services seem to be implemented through deep packet inspection (DPI) of network traffic, rather than shallow properties such as the destination port or IP address. DPI is often deployed out of band, so that the overhead of resource utilization or failure does not disrupt all outbound traffic, instead relying on terminating the connection through sending a TCP RST packet. Instead, the disruption appears to be imposed in line by the routers processing traffic. Interestly, it appears that end points continue to receive roughly a packet per second after exceeding the time window. Connections may simply be set to throttle down to nearly zero throughput after reaching the time threshold.



Throughput of Random Traffic from Iran to Europe

The new filtering rule has fundamentally broken the strategy that circumvention tools have thus far implemented to avoid filtering through DPI, wherein they sought to avoid creating a detectable traffic pattern. At the time of publication there appears to be a number of holes in the new regime, indicating that short term fixes appear possible.

Iran now effectively runs a "white list" of permissible applications with a three tier structure for the handing of Internet traffic that traverses the international gateway.

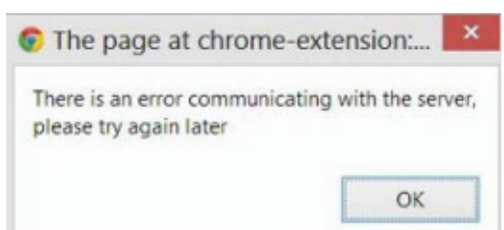
UNENCRYPTED WEB TRAFFIC: While subject to content-filtering and surveillance, unencrypted web traffic appears to be comparatively unthrottled and less subject to other forms of disruption.

ENCRYPTED, STANDARD WEB TRAFFIC: Subject to extreme throttling and intermittent disruption. (See Below: "Secure Traffic Throttling")

UNCLASSIFIED OR ABNORMAL TRAFFIC: Connections are throttled and terminated after a short period of time.

Initially, the filtering regime appeared to retain a quota on traffic across different connections, however, on subsequent tests days later, this phenomenon could not be reproduced. It is also worth noting that, while the VPN blocking appeared to have been implemented on an ISP-level, the current rules are likely enforced at the international gateway by the Telecommunications Company of Iran. Domestic traffic is unaffected by these rules.

While the most common circumvention tools are impaired or no longer working, users have partially settled into a new collection of testing versions of tools, previous generation web proxies, and miscellaneous offering, such as "VPN Gate" SSL VPN service, "Stealthy" and "anonymoX." However, several of these services became blocked within days of being publicized on social media.



SECURE TRAFFIC THROTTLING

10 MEGABIT FILE	TIME
HTTP	24s
SSH	32m 7s
LATEST FIREFOX BUILD	
HTTP	2m 54s
HTTPS	71m 14s

The throttling of secure web service has been the subject of discussion in previous editions of the Internet Infrastructure and Policy Report series. After the implementation of more aggressive filtering rules, throughput measurements were performed against international connectivity of secure services over SSL (HTTPS) and SSH, compared to normal HTTP. From the points where measurements were taken, secure traffic was consistently throttled down to between 1% and 5% of the plaintext baseline (Source: SSL, SSH). These observations reflect complaints commonly heard on social media and blogs that basic activities such as sending attachments in Gmail takes "hours" and that the Internet is "slower than 1994". (Source)

DOMESTIC SSL CERTIFICATE AUTHORITY

In early May, reports surfaced that public sector employees were being forced to install additional, unknown software on their machines, in order to register for an employee portal, karmandiran.ir (Source). The Karmandiran site is currently pointed to a host owned by a "Cube Commentators Group" on Iran's private NAT network, at 10.8.12.36, making it inaccessible from outside the country or those on circumvention tools. When a user runs the "certificate.exe" file offered, an SSL root certificate is retrieved from karmandiran.ir and installed locally (Source). This new root certificate would allow the creater, presumably the Iranian government, to issue security credentials that appear valid in the name of any website, and then potentially pose as or intercept communications between the user and other sites. It is unclear at this time how many have installed the certificate or how it has been used thus far. Furthermore, no host on the same network appears to be running an SSL service, making it uncertain whether the certificate is even used in a legitimate manner.

ICMP FILTERING

Certain types of ICMP traffic appear to be filtered on consumer ISPs. Attempts to traceroute begin to return unresponsive results after transversing the domestic firewalls.

RIGHTEL VIDEO CALLING DISRUPTION

The video calling service offered by RighTel has been intermittently unavailable for users. Support staff from RighTel have attributed the problem to “technical issues” in the network, however, the timing coincides with the controversy of being accused of inspiring immoral behavior. (Source)

NEEDS AND EDUCATION

// In the previous edition of the report, we note an unaddressed demand for circumvention tools and a lack of clarity over the security of the available services. After the major, and often foreign-funded, tools became blocked, the public appears to have moved into an even more scattered and less reputable field of anti-filtering services. Our concerns are further heightened by the authors of this series receiving additional malware posing as circumvention tools and credentials for VPN services that appear to be sent by malicious parties. As users adopt tools out of desperation, they need to be vigilant of what they are installing and aware of the ways they hand over their data to the owners of circumvention networks. Additionally, should complete network outages be associated with the election, it will be necessary to ensure that backup connectivity is available to critical sources of information, through means such as foreign dial-up numbers. Here too is is necessary to maintain a stern cautionary note on the dangers of dial-up and satellite connectivity.

NETWORK ANALYSIS

UPDATES

While ICMP requests are blocked, test observations could be completed using traceroutes through TCP requests on port 80. This approach has often been more useful as well in analyzing the internal paths for Iran’s private network. From these results, it appears that no major changes occured in the visible parts of the infrastructure, despite the noted increases of blocking. In this report, we have also added observations from the ADSL provider Shatel for the first time.

RESULTS

TCI DSL SERVICE	PISHGAMAN TOSEH ERTEBAT
Basic UDP access is available. The client was able to send fragmented UDP traffic. The client was unable to receive fragmented UDP traffic. The most likely cause is an error in your network's firewall configuration or NAT. The maximum packet successfully received was 1452 bytes of payload. UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X. A DNS proxy or firewall generated a new request rather than passing the client's request unmodified. Changes to headers or contents sent between the client and our HTTP server show the presence of an otherwise unadvertised HTTP proxy. The following headers had their capitalization modified by the proxy: Content-Type: text/html Content-Length: 770 Last-Modified: Wed 08 May 2013 07:55:09 GMT Set-Cookie: netAlizEd=BaR; path=/; domain=netalyzr.icsi.berkeley.edu Connection: keep-alive The following headers were added by the proxy to HTTP responses: Proxy-Connection: keep-alive The detected HTTP proxy changed images that were sent from our server. The detected HTTP proxy changed either the headers the client sent or the HTTP response from the server. We have captured the changes for further analysis.	UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X. A DNS proxy or firewall generated a new request rather than passing the client's request unmodified. An in-path DNS proxy modifies NXDOMAIN errors. Instead of forwarding the error, the device replaces it with a response redirecting you to IP address X.X.X.X.

HTTP proxy detection via malformed requests (?): OK We detected the presence of an in-network transparent HTTP cache that caches data which was directly requested by the client. EDNS-enabled requests for small responses remain unanswered. This suggests that a proxy or firewall is unable to handle extended DNS requests. EDNS-enabled requests for medium-sized responses remain unanswered. This suggests that a proxy or firewall is unable to handle extended DNS requests or DNS requests larger than 512 bytes. EDNS-enabled requests for large responses remain unanswered. This suggests that a proxy or firewall is unable to handle large extended DNS requests or fragmented UDP traffic. A detected in-network HTTP cache incorrectly caches information Weakly uncacheable data was cached between you and our server, even when the data was requested directly and explicitly. This suggests that there is an HTTP cache in the network which examines and caches web traffic. Since this content was not supposed to be cached, the HTTP cache is probably operating incorrectly.	

TRACEROUTE 4.2.2.2	
6 * * * **7** 10.31.41.98 184.971 ms **8** 10.41.43.98 180.559 ms **9** 10.43.43.85 179.850 ms **10** * * *	**5** 10.152.14.201 44.414 ms **6** * * * **7** 10.152.32.249 56.268 ms **8** * * * **9** * * * **10** 10.10.53.61 67.248 ms **11** * * * **12** * * *
TRACEROUTE 8.8.8.8	
6 * * * **7** 10.31.41.98 175.080 ms **8** 10.41.43.98 180.580 ms **9** 10.43.43.85 184.926 ms **10** * * * **11** * * *	**5** 10.152.14.201 45.509 ms **6** * * * **7** 10.152.32.249 50.709 ms **8** * * * **9** * * * **10** 10.10.53.69 65.306 ms **11** * * *

MOBINNET	SHATEL
UDP access to remote DNS servers (port 53) appears to pass through a firewall or proxy. The client was unable to transmit a non-DNS traffic on this UDP port, but was able to transmit a legitimate DNS request, suggesting that a proxy, NAT, or firewall intercepted and blocked the deliberately invalid request. A DNS proxy or firewall caused the client's direct DNS request to arrive from another IP address. Instead of your IP address, the request came from X.X.X.X. A DNS proxy or firewall generated a new request rather than passing the client's request unmodified. A DNS proxy or firewall blocked non-recursive DNS requests. Non-recursive requests receive an error code of -1. Direct UDP access to remote SIP servers (port 5060) is blocked.	Direct TCP access to remote SMTP servers (port 25) is prohibited. This means you cannot send email via SMTP to arbitrary mail servers. Such blocking is a common countermeasure against malware abusing infected machines for generating spam. Your ISP likely provides a specific mail server that is permitted. Also, webmail services remain unaffected. Direct TCP access to remote RPC servers (port 135) is blocked. Direct TCP access to remote NetBIOS servers (port 139) is blocked. Direct TCP access to remote SMB servers (port 445) is blocked. Basic UDP access is available. The client was unable to send packets of 1471 bytes of payload (1499 bytes total), which suggests a problem on the path between your system and our server. Direct UDP access to remote NetBIOS NS servers (port 137) is blocked. Direct UDP access to remote NetBIOS DGM servers (port 138) is blocked. During most of Netalyzr's execution, the client continuously measures the state of the network in the background, looking for short outages. During testing, the client observed 17 such outages. The longest outage lasted for 1.2 seconds. This suggests a general problem with the network where connectivity is intermittent. This loss might also cause some of Netalyzr's other tests to produce incorrect results.

TRACEROUTE 4.2.2.2	
5 10.47.33.2 504.872 ms **6** * * * **7** 10.10.53.142 86.508 ms **8** * * *	**7** * * * **8** 10.10.53.189 71.747 ms 10.10.53.193 72.015 ms 10.10.53.197 72.357 ms **9** 10.10.53.34 77.886 ms **10** * * *
TRACEROUTE 8.8.8.8	
5 10.47.33.2 504.863 ms **6** * * * **7** 10.10.53.142 80.073 ms **8** 10.10.53.97 88.354 ms **9** * * *	**7** * * * **8** 10.10.53.185 72.948 ms 10.10.53.181 72.871 ms 10.10.53.193 72.635 ms **9** * * *