A Longitudinal Study on Digital Filtering in Saudi Arabia

Fatemah Alharbi (fmhharbi@taibahu.edu.sa)
Taibah University
Michalis Faloutsos
University of California, Riverside
Nael Abu-Ghazaleh
University of California, Riverside

Research Article

Keywords:

Posted Date: March 10th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1225568/v1

Abstract

In the space of Internet filtering, we make a rare positive observation: Saudi Arabia has been opening its digital borders since 2017 in a deliberate new era towards openness. Internet filtering is routinely used by institutions to restrict access to websites and services that promote content that is deemed inappropriate with respect to governing laws, values, or policies. Here, we present a comprehensive longitudinal study of *digital filtering*, which we define to include both mobile apps and website access, in Saudi Arabia over a period of three years. Our results show that Saudi Arabia has indeed made significant progress towards opening its digital borders: (a) the use of mobile applications has been significantly permitted; and (b) web access has become more open. Specifically, we monitor access to: (a) 18 social media and communications mobile apps such as WhatsApp, Facetime, and Skype; and (b) Alexa's top 500 websites in 18 different categories. First, we find that our mobile app group was completely blocked in 2017, but access was permitted to 67% in 2018, 93% in 2019, and all, except WeChat, in 2020. Second, we conduct measurements from multiple vantage points covering the three largest telecommunications companies in Saudi Arabia: Saudi Telecom Company (STC), Mobily (owned by Etisalat of the United Arab Emirates), and Zain (from Kuwait), and *four* major cities in Saudi Arabia: Riyadh, Jeddah, Makkah, and Al-Khobar. Our results show that Internet filtering decreased by 3.4% and 2.2% in *Adult* and *Shopping* respectively, which are the most two blocked categories. Finally, we find that changes in the filtering policy reflect the wider geopolitical dynamics of the region. For instance, we find that filtering rules emerge for: (a) ISIS-friendly sites in 2020, and (b) news sites from Qatar in 2017, Iran in 2018, and Turkey in 2020, in response to diplomatic tensions. Finally, we investigate and characterize the technical mechanisms and the network topology used in the implementation of the filtering.

1 Introduction

Several countries restrict the access to information on the Internet, which they deem inappropriate or harmful for their citizens. The rationale and justification can be usually attributed to: (a) laws and morals of the country, and (b) security threats for citizens or the country. We refer to this type of restriction as *digital filtering*. Here, we use this term to include both: (a) limiting access to websites; and (b) preventing the use of mobile applications. The reason is that the emergence of smartphones provides ways to access information and communicate privately beyond the traditional use of websites. Our study focuses on the Kingdom of Saudi Arabia, which is considered to be among the most conservative countries. The government manages the access to the Internet with a filtering system to protect the values of the Saudi society (which center around Islam, its official religion), in addition to implementing national security and public safety policies [1]. Unsurprisingly, this practice is a controversial and polarizing topic. On the one hand, many organizations criticize the level of digital filtering in Saudi Arabia. For instance, Freedom House characterizes Saudi Arabia as "not free" [2], and it is ranked 170 out of 180 countries by Reporters Without Borders as one of the top violators of press freedom [3]. The same organization also published a report in January 2016 which ranks Saudi Arabia as one of the "15 enemies of the Internet" since 2005 [4]. On the other hand, we see many domestic organizations that do support digital filtering. For instance, the Ministry of Media provides regulations for digital publishing activity [5] which strictly prohibit any content that violates the provisions of Islamic law, breaches the national security, incites violence among citizens, or violates copyrights law. The

Ministry of Interior (MOI) launched an electronic service [6] to help citizens report any type of cybercrimes including production of websites violates public moral (such as pornographic and gambling sites) or impinges on public order and religious values as stated in the Anti-Cyber Crime Law [7]. Many individuals and non-government-linked organizations support the filtering service [8–10]. Internationally, the Safer Internet Day (SID) [11] is an organization that provides an education and awareness-raising effort spanning more than 100 countries including Saudi Arabia [12].

In the last few years, Saudi Arabia has undergone significant sociopolitical changes which seem to have brought forward a more progressive approach regarding access to information. We provide some highlights of significant events between 2018 and 2020, which can provide useful context for our study. This period coincides with the start of the execution of Saudi Arabia's national Vision 2030 and National Transformation 2020 programs [13] that were announced in April 2016. The two vision documents were nationally adopted as a roadmap for economic and developmental investments and projects across all fields of endeavor in the country, with the stated aim of creating a more tolerant and moderate country. Interestingly, the two vision documents introduced a series of sweeping social reforms. For example, in September of 2017, a royal decree lifted the ban on women driving that was enacted in 1957 [14]. Additionally, according to the Kingdom's General Authority for Entertainment (GAE) [15], in 2018, Saudi Arabia has allowed the operation of movie theaters for the first time in decades. In addition, during the same year, the Saudi government allowed international artists to perform musical concerts and allowed the participation of women, which are significant moves towards a more open society. At the same time, there has been a number of geopolitical events, such as rising tensions with Qatar, Iran, and Turkey, including briefly an embargo on Qatar.

Given these significant social changes, and geopolitical events, a natural question is whether the digital filtering policies have changed in response. There are a few studies (that are older, and less comprehensive than our work) focusing on Saudi Arabia, while there are several studies of Internet filtering in other countries, which are reviewed in Section 7. To the best of our knowledge, our work represents the first systematic, longitudinal study of digital filtering in Saudi Arabia. The study spans the period from March 2018 to April 2020, with three separate measurements, one in each calendar year. We focus on answering four questions: (a) "what content is filtered?", (b) "how is filtering implemented?", (c) "how does filtering evolve over time in response to geopolitical conditions?", and (d) "what are the technical mechanisms and the network topology used in the implementation of the filtering?".

A key novelty of our approach is a comprehensive and systematic treatment of these questions. We pursue a multi-pronged strategy summarized in Fig. 1: **(a) Quantification**: we measure website network accessibility as well as mobile application accessibility (specifically, those used for voice/video communication); **(b) Understanding**: we seek to reverse engineer the filtering infrastructure and understand the different filtering mechanisms employed; and **(c) Interpreting**: we explore whether societal shifts in response to the moderation visions, as well as geopolitical events influence the filtering policy over time. We discuss each of these directions in more detail below.

In addition, we developed an extensive measurement infrastructure using multiple vantage points inside Saudi Arabia including: (a) *four* major cities spread across the country (Riyadh, Jeddah, Makkah, and Al-Khobar) and (b) *three* major Internet Service Providers (ISPs) in the country. We argue that our study provides reliable observations by contrast to prior studies which overwhelmingly rely on VPNs or PlanetLab nodes [16–18].

A. Quantification: What is filtered? We provide a fairly extensive study on the accessibility of both mobile apps and websites and mobile apps from within Saudi Arabia and its evolution over time. Our results show significant progress towards the opening of the country's digital borders:

- Mobile applications accessibility: we conduct systematic measurements on 18 of the most popular mobile social network applications worldwide and in the Middle East including Facetime, Tango, Viber, Line, SOMA, and WeChat. As shown in Fig. 2, all of the selected apps were blocked over the period 2013–2017, while 67% and 93% of them were accessible in 2018 and 2019, respectively. In 2020, all these apps are accessible, except WeChat. These results point to a significant relaxing of the filtering rules for mobile apps.
- Network accessibility: We assess web access filtering by considering the top 500 most popular websites in 18 different categories according to Alexa [19] for a total of 9000 websites. In Fig. 2, we plot the evolution for the three most blocked categories: *Adult*, *Shopping*, and *Games*. We observe a moderate trend across the categories towards more openness. For example, the number of accessible websites in the *Shopping* category increased from 90.4% in 2018 to 93% in 2020.

B. Understanding: How is filtering implemented? We identify the mechanisms in the communication interaction, where the filtering takes place. Inspired by earlier efforts [20], we develop a significantly more detailed tool for assessing digital filtering. The key capability is that we detect the specific techniques used for filtering. In more detail, we identify four types of filtering: (a) DNS level filtering, (b) IP address filtering, (c) HTTP filtering, and (d) TLS filtering, all of which we will detail in the full paper. Our results show that Internet filtering in Saudi Arabia is based on HTTP filtering augmented with TLS filtering for connections using HTTPS:

- HTTP filtering: By comparing the filtering results between 2018 and 2020, we see that HTTP filtering decreased by 3.4%, 2.2%, and 1.2% in *Adult*, *Shopping*, and *Games* categories, respectively.
- TLS filtering: We also see the reflection of digital border openness in the TLS filtering results. For instance, we observe that the number of websites from the Shopping category that are filtered by TLS-level filtering decreased from 9.6–6.6% during the time of the study.

Additionally, we go below the application layer and develop a measurement-driven method to reverse-engineer the topology of the filtering infrastructure, whose accuracy is corroborated by official documents.

C. Interpreting: How does filtering evolve over time in response to geopolitical conditions? We finally go at the political and policy level and examine the manifestation of real-world events on filtering. We find that ISIS-friendly sites are blocked due to the fact that ISIS supports terrorism and destabilization to the region.

We also find that more news sites got blocked. For instance, some Qatari, Iranian, and Turkish news sites got blocked in 2017, 2018 and 2020, respectively, amid continued political tensions with these countries.

An earlier version of this paper appeared in the Proceedings of the 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI) in 2020 [21]. This paper extends substantially this previous work: we add substantial new details and experiments. Specifically, we clarify the contribution and the description of the technical details in more depth. We also add new experiments to provide an understanding of the Internet filtering infrastructure in Saudi Arabia. We highlight our contributions as follows:

- We conduct additional experiments to comprehensively understand Internet filtering in Saudi Arabia. More precisely, we reverse-engineer the filtering infrastructure including confirming the general topology of the internet filtering as discussed in some of the official documents from the Ministry of Information. We conduct experiments to independently reconstruct the network topology of the filtering system; see Section 6.
- Many studies have been conducted to examine the filtering practices and mechanics in different countries around the world. Due to the 6-pages limit requirement by the USENIX FOCI workshop, we could not explain the related work; thus, we add a dedicated section for this purpose; see Section 7. In this section, we briefly survey a number of these studies and explain their relationship to our work where appropriate. • We add detailed results for our WeChat experiments, where we found a uniquely interesting behavior. WeChat is one of the most popular messaging applications owned by the Chinese company Tencent; see Section 5.5.
- We substantially expand the writing and add more technical details to help readers understand our work more clearly. Specifically, we review some of the most commonly deployed Internet filtering mechanisms, which can enable filtering at different levels of granularity; see Section 3. We also explain our results in more depth; see Section 5.
- Now that the times have changed and the use of technology has changed, we need to understand the evolution in Internet filtering, specifically in Saudi Arabia: a traditionally conservative country that has embarked on economic and societal changes in many aspects of its daily operations and public policies with the stated objectives of modernization and openness. We present a brief history of Internet filtering in Saudi Arabia; see Section 2.

The remainder of the paper is organized as follows. We present a brief history of Internet filtering in Saudi Arabia in Section 2. We present some background on Internet filtering mechanics in Section 3. We present the methodology we employ in the measurement study in Section 4. We present the results of the study in Section 5, including some analysis of the impact of local and regional geopolitical events on the evolution of the filtering policies. We present our analysis of the filtering infrastructure in Section 6, and we discuss related work in Section 7. Finally, we present some concluding remarks in Section 8.

2 History And Background

The history of the Internet in the Kingdom begins when King Fahd University of Petroleum and Minerals (KFUPM) connected to the Internet in 1993. This initial system used two dedicated Domain Name System

(DNS) servers for name resolution [22]. After being intensively used by the academic sector, the Internet was brought to the public in 1999 after the Council of Minsters officially issued Resolution No. 163 [23]. It gave King Abdulaziz City for Science and Technology (KACST), located in Riyadh, the authority to create the Internet Services Unit (ISU) and to carry out oversight over the licensing, deployment and management of the Internet in the country. Since then, the unit, in cooperation with the Communications and Information Technology Commission (CITC), is responsible for providing Internet service in Saudi Arabia. Despite this late adoption, especially in terms of connectivity, the number of Internet subscribers increased rapidly: CITC estimates that the number of Internet users has grown from nearly 1 million in 2001 to 3 million in 2005 [24]. At the end of 2018, the number of users is more than 27 million which represents 83.4% of the population in Saudi Arabia [25]. In addition, in April 2016, the Crown Prince Mohammad bin Salman Al-Saud announced the Vision 2030 and National Transformation 2020 programs [26] that gave high priority to the Communication Information and Technology (CIT) sector, which has a goal of ultimately providing 90% broadband coverage across the different regions of the country. Internet filtering in Saudi Arabia is managed by a central and standardized system located in KACST. All ISPs direct their web traffic to an ISU proxy server which keeps a log of user activities. If there is an ISP-level firewall or other network security functionality, it is legally required not to bypass this proxy. Although there are always ways to circumvent Internet filtering [17, 27–29], this type of practice is considered a cybercrime in Saudi Arabia. Violators are prosecuted and may be punished with up to five years in prison [7].

Website filtering uses two sources of information [30]:

1. Commercial list: The CITC has contracted with an unnamed international company specialized in website ranking to obtain their own list of websites categorized into more than 90 categories. Those which related to pornography, gambling and drugs are summarily blocked; an effort to provide a family safe Internet. The list is updated by the company on a daily basis, and there is a continuous line of communication with the company to correct errors related to websites classification.

2. Saudi-Arabia-specific list: It is an internal list prepared by CITC. The websites are blocked based on requests by regular users and specialized authorities [31] after reviewing them and ensuring that they contain materials inappropriate to the Saudi society. The CITC reported that 92.80% of these websites are related to pornography while 2.77% are related to gambling, sorcery, drugs, etc. Unlike other countries who covertly block web pages without informing users (e.g., Bangladesh, Russia, India, China, Turkey and Malaysia) [17], Saudi Arabia makes blocking explicit. While the list of prohibited websites is not publicly available, any request to a blocked website causes the user to be redirected to a web page owned by ISU. For instance, Fig. 3 shows a warning page in response to visiting www.betonline.ag (a gambling website). Figure 4 shows a different warning page in response to visiting www.aljazeera.com (a news website) which has been blocked due to political tensions with Qatar where Aljazeera is headquartered. CITC also receives requests to block or unblock websites from customers. For instance, more than 8 thousand unblock requests were received in 2016 [32], with 7% of these ultimately accepted. On the other hand, more than 900 thousand requests to block websites were received with 56% of the requests resulting in a block. This number increased to more than 1 million by the end of 2017 [33]. Overall, the CITC has handled over 6 millions blocking requests since 2008.

There are many other countries where Internet filtering is present due to historic and domestic issues (e.g., Nazi websites in Germany [34], pedophilia in the European Union [35], violation of copyright law in France [36]). In Saudi Arabia, national security and cultural beliefs are the origin of the government's concerns in regards to Internet access [1]. The government has been practicing Internet filtering since 2001 when the Council of Minsters issued a resolution outlining the basis for content filtering [37]. Accordingly, the ISU published a "black-list" of prohibited websites [38]. Here are some examples of blocked content:

- Two episodes of the "American Dad!" TV series were blocked for having a scene showing a negative portrayal of Saudis [39].
- The Ministry of Media blocked "Pirate Bay" and "Torrentz.eu" websites for distributing copyrighted materials [40].
- To promote Islam being a peaceful religion [41], any websites that promotes the so-called "Islamic State" of Iraq and Sham (ISIS) are called to be banned [42].
- Some social network applications, such as WhatsApp and Skype, were banned in 2013 for violating regulatory requirements [43].

3 Overview Of Internet Filtering Mechanisms

In this section, we review some of the most commonly deployed Internet filtering mechanisms, which operate at different levels of granularity. Internet filtering refers to a multitude of technical policies that can be employed to prevent users from accessing specific content or Internet-connected machines. The policies can vary from blocking all connections towards a particular country to micro-focused strategies blocking specific websites, servers, and even words. These policies rely on a number of mechanisms that interfere with the user's ability to access these resources. Specifically, there are many steps in establishing a connection to a website from a browser, filtering techniques can interfere at any of these steps (e.g., TCP connection establishment). Naturally, one can use combinations of these mechanisms to implement an overall filtering policy.

3.1 DNS-level Blocking

Accessing a website starts with a Fully Qualified Domain Name (FQDN) address, specified as part of a Universal Record Locator (URL) in a browser address bar (e.g., http://www.example.com). The FQDN is the portion of the URL that fully identifies the domain name of the target server (e.g., www.example.com without the http:// prefix). The Domain Naming Service (DNS) protocol provides a resolution service to map FQDNs to their corresponding Internet Protocol (IP) addresses [44]. DNS is supported by a hierarchical infrastructure which contains a set of distributed name servers (an example is shown in Fig. 5 above). At the top of the hierarchy, there are 13 root servers that are geographically distributed at a global level. At the next level, there are a set of Top-Level Domain (TLD) servers which service queries for top level domains (e.g., .edu, .com, and .org), and at the bottom there is an embedded hierarchy of authoritative name servers that hold the translation from the FQDN for the part of the address space they manage to the corresponding IP addresses.

DNS queries from clients are processed by resolvers that can walk the hierarchy until they reach the authoritative name servers responsible for the FQDN being resolved. In countries where authorities have control over DNS resolvers, they interject in the resolution process to manipulate translations and redirect users from accessing a filtered site (see Fig. 6-a and Fig. 6-b). In other words, they can prevent the translation of FQDNs to their corresponding IP addresses, and instead they direct users to another server under their control, for example, to display a message indicating that the target server is blocked. For instance, in Iran, when a client sends a DNS query to access a banned site, instead of receiving the legitimate IP address, the client is directed to a private IP address (10.10.34.34) that is controlled by the filtering module [45]. Similarly, extensive work show evidence that China's Great Firewall (GFW) uses this type of filtering [46–49].

3.2 IP Address Based Blocking

After DNS resolution, the next potential intervention point available for filtering is at the level of TCP (or UDP) connection establishment, which uses IP addresses to identify the destination of the connection. Governments (or enterprise) maintain a pre-defined list of IP addresses belongs to banned sites. This blacklist is usually handed to Internet Service Providers (ISPs) to execute the filtering [18]. Basically, when a client requests access to a forbidden site, the ISP will prevent connection establishment (by dropping the SYN or SYN/ACK packet). For instance, in China, requests to banned sites are intercepted by GFW servers and then responded to by spoofed TCP-RST packets (see Fig. 7), forcing clients to terminate the TCP connection [17].

Filtering based on IP addresses can also be used to block access to entire subnets. For instance, the Syrian authorities filter IP addresses belong to specific geographical regions (e.g., Israel) [50]. Blocking using IP addresses has the advantage of working even when the connection is encrypted, or when the users bypass the use of DNS.

3.3 HTTP Filtering

One could evade the two filtering techniques we just presented: DNS-level and IP addresses. One could change IP addresses and DNS records of the blocked servers to evade filtering, at least until the filtering lists are updated again.

As a result, another filtering intervention uses HTTP-level filtering. This mechanism typically uses one of two approaches: (a) Fully Qualified Domain Name (FQDN) filtering, and (b) general keyword filtering. The FQDN filtering checks the URL string (typically in HTTP GET requests) after the http:// prefix. The general keyword filtering checks the URL string against a list of forbidden keywords. When a "match" is found, the connection is blocked. Note that beyond checking the FQDN, keyword filtering can provide a fine-granularity filtering. It can filter based on the occurrence of the keyword in the URL (e.g., blocking a specific page on a website, such as a specific user in Facebook). For example, using keyword FakeUserabc123 that corresponds to the name of a Facebook user, we can block access to all URLs that contain FakeUserabc123 which will block access to https://www.facebook.com/public/FakeUserabc123.

This intervention is typically applied to HTTP, either during the initial GET request or when responses are received. When the requests are filtered, the filtering system can force the connection to reset or timeout, which displays an error to the client. In this scenario, requests never reach the destination web server.

Similarly, when the responses are filtered, HTTP filtering is applied forcing the connection to terminate (see Fig. 8). Previous work has shown that Pakistan [20] and China [17] use this type of filtering. Interestingly, Verkamp and Gupta [17] show evidence that the filtering node in Saudi Arabia responds back with a warning page upon filtering an HTTP request. As we will see later, our results seem to contradict their findings.

3.4 TLS Filtering

Since HTTP filtering requires deep packet inspection to identify the keywords inside the payload of the packet, if encryption is used (i.e., HTTPS rather than HTTP), the keyword is not available and HTTP filtering fails. This gives users and websites a simple way to bypass filtering. To prevent this, additional filtering can be implemented at the TLS handshake level. After the TCP 3-way handshake succeeds, when a client tries to establish a TLS connection with a blocked website, the filtering node sends TCP-RST packets after the Client Hello message forcing the TLS connection to be terminated as shown in Fig. 9 below. If TLS filtering is implemented to complement HTTP filtering, if HTTPS is used, TLS filtering can prevent the establishment of the encrypted session. We believe that we are the first to identify this type of filtering.

3.5 Other Strategies

There are other filtering techniques. First, some techniques use deep packet inspection that can enable sophisticated and fine-level filtering based on packet characteristics and content. Second, another approach uses traffic shaping, in which traffic to non-approved websites is delayed, but not blocked. Therefore, they are not blocked, they just make the access less desirable. Third, some filtering techniques use port numbers, regulating and restricting the use of specific web services (e.g., email servers, or instant messages). We did not observe such mechanisms during our study, and for this, we do not discuss these methods further.

4 Methodology

We explain the measurement methodology, the tools, and the data collected in our experiments. We start by presenting some ethical considerations that we contemplated as we undertook this study.

4.1 Ethical Considerations

Although this is a technical study, the sensitivity of the topic of filtering created the need for societal and ethical considerations. The need was made more imperative by the nationality of one of the authors.

To avoid legal complications, we discussed the scope of our study with a Saudi high-ranking government official, who is an expert in Saudi Arabian law, and he confirmed that the study does not violate the Saudi Arabian law. Clearly, digital filtering is a sensitive topic, and we had to consider whether the experiments would violate not only ethical considerations, but also any laws or regulations in Saudi Arabia. Article 6 in the Anti-Cyber Crime Law of the country [7] states that the production of any artifacts that would undermine

public order is strictly illegal. In the context of our work, we had to verify that our measurement study does not present mechanisms to bypass the filtering which would make it illegal under article 6.

We took precautions to ensure that our study would not jeopardize any individual within or outside Saudi Arabia. We never disclosed the personal information of our anonymous volunteers, nor did we re-distribute or otherwise share the detailed experimental logs data (now or in the future). We only analyze aggregated information that neither exposes details of the network or any identifiable information with respect to our measurement points. Additionally, since digital filtering in Saudi Arabia is evident and explicit (as shown in Fig. 3 and Fig. 4), the act of probing blocked sites is legal.

4.2 Our Measurement Configuration Setup

To assess filtering inside Saudi Arabia, we tested the reachability of the most popular websites worldwide according to the Top Sites lists overall and by category published by Alexa [51]. We collected the top 500 websites in 18 different categories [19]: *Adult*, *Arts*, *Business*, *Computers*, *Games*, *Shopping*, *Society*, *News*, *Regional*, *Reference*, *Sports*, *Global*, *Saudi Arabia*, *Home*, *Health*, *Recreation*, *Kids & Teens*, and *Science*. The measurements were repeated three times, roughly one year apart, between March 2018 and April 2020. For each iteration of the measurements, we got the updated lists of the top 500 websites ending up with three lists for each category corresponding to the three measurements. We found that the lists remained almost identical (less than 3% of change) across the three years and the changes were typical at the very bottom of the list. We also found that if a site is blocked in the previous year (e.g., in 2018) is either still blocked in the following years (e.g., in 2019 and 2020) or turned to be accessible. In other words, we have not encountered a case where a website is blocked in the previous year and no longer on the list in the following years.

In addition, we tested the availability of 18 mobile applications, including Line, Skype, and Facetime, as we discuss later.

4.3 Our measurement approach

To conduct our measurements, we developed a tool, which was inspired by Samizdat [20], which was used in a study of Internet filtering in Pakistan in 2013, as we discuss in Section 7. Our tool introduces significantly new functionality in order to allow us to study filtering at a deeper level. For each website in our lists, we deploy the following measurement methodology in order to capture a detailed view of any potential filtering:

a. DNS Filtering. First, the tool performs a DNS lookup using UDP and records the IP address in the response packet; otherwise, the retrieved error code (e.g., Timeout, SERVFAIL, REFUSED, NXDOMAIN, etc) is recorded. It then performs the same test using TCP and records the results.

b. IP Address Filtering. If the website is successfully resolved in the first test, the tool initiates a TCP connection using a stream socket to the IP address and port 80. If the connection is established, the test is recorded as successful; otherwise, it is recorded as a failure.

c. HTTP Filtering. This experiment is divided into two phases. In the first phase, we check if there is direct HTTP filtering of the FQDN in the GET request. Specifically, the tool tries to establish an HTTP connection

and sends a GET request to the website. Both the response and returned code are recorded. In the second phase, using a non-blocked website (e.g., www.google.com.sa), the tool appends the URL of the website we want to test (e.g., www.aljazeera.com) to Google's URL (e.g., http://www.google.com.sa/www.aljazeera.com). The normal behavior is to see the well-known Page Not Found HTTP 404 error code. If a different error code (e.g., 403) is returned, this means HTTP-URL-Keyword filtering is enabled.

d. TLS Filtering. Separately, we extended the tool to try to establish a TLS connection with the web server of the site we want to test to check if there is filtering on the HTTPS protocol.

To increase the confidence in our results, we took the following steps to increase the reliability and consistency of our measurements:

First, we wanted to ensure that network issues (e.g., temporary unreachability, packet losses and other networking pathologies) do not affect the measured results. For this reason, we randomly selected and re-probed 10% of sites per category 100 times each and discovered no errors in the initial measurement for these websites. We also modified the set of open DNS servers used by Samizdat.

Second, in addition to the default DNS servers used by our vantage points (which belong to the respective ISP DNS service), we measured the Internet filtering on the following public servers: Google (8.8.8.8), Quad9 (9.9.9.9), OpenDNS (208.67.222.222), Norton (199.85.126.10), Comodo (8.26.56.26), and Level3 (209.244.0.3).

Third, to get more precise results, we performed DNS lookups using both UDP and TCP protocols. We tested site accessibility over both HTTP and HTTPS protocols since HTTPS is not amenable to keyword-based filtering.

Finally, we also conducted a number of Wireshark measurements to capture and analyze the detailed network behaviors and to verify the subtleties of the filtering mechanisms.

4.4 Filtering at the Mobile App Level

In what is arguably, a relatively novel dimension in filtering, we want to assess if mobile applications are affected by filtering. We conduct a systematic measurement study with two smartphones one in the USA and one in Saudi Arabia and we compare the differences in terms of downloading and using apps. We discuss the results from this study in Section 5.5.

4.5 Measurement Vantage Points

We conducted measurements from six different vantage points distributed across four major cities in Saudi Arabia using the three major ISPs in the country. The four cities whose geographical location is shown in Fig. 10 below) are: (1) Riyadh, which is the capital and the largest city of Saudi Arabia (population 6.5 million) and is centrally located; (2) Jeddah, which is located on the west coast and is the second largest city in the country (population 4 million); (3) Makkah, which is the birthplace of Islam and the spiritual center of the kingdom (population 2 million); and (4) Al-Khobar, which is one of the major cities in the eastern region of the country (population 1 million). We selected these cities because of their different nature and

roles in the Kingdom, as well as for their geographical distribution. Table 1 below shows the details of each network. We chose vantage points connecting to different Internet Service Providers (ISPs) to understand whether there is ISP level filtering, or other variation in the experienced filtering based on the ISP. The machines in N1, N2, and N3 are connected to the Internet through the same ISP which is the Saudi Telecommunication Company (STC). We conducted our measurements in one city, Makkah, through 3 different vantage points connecting the same machine to all three major ISPs: STC, Zain, and Mobily. All machines are connected to their default gateways, or routers, with a 1GB Ethernet cable. All machines run Windows 10 Professional Edition.

Enhancing the trustworthiness of our results. We wanted to make sure that failures to accessing resources were not due to: (a) transient outages, and (b) reasons other than filtering policies. To reduce the effect of such phenomena, we used the following two mechanisms. First, we conducted the measurements multiple times to eliminate the effect of transient phenomena, such as short-lived outages. Second, to establish a baseline external reference point, we also executed the same measurements outside Saudi Arabia. Specifically, we used machine from our university in the USA, which also run Windows 10 Professional Edition. We used these measurements as a reference point. For example, to confirm that an unreachable website is indeed blocked inside Saudi Arabia, we checked its accessibility from the USA. If the website returned the same error code (e.g., HTTP codes 503 or 301 indicating that the server is unavailable or moved permanently, respectively) in both countries, we consider that the lack of accessibility is not due to filtering.

5 Results

Overall, we observe that the filtering rules are significantly relaxed over the time for both websites and mobile apps. This provides substantial evidence that Saudi Arabia is cautiously opening its digital borders. We summarize the results of our study in Fig. 11, Table 2, and Table 3. We highlight the observations as follows:

Observation 1: Filtering has relaxed in each website category. We analyzed the accessibility for various websites categories as we discussed earlier. We present some observations per category. The overall conclusion is that for each category the filtering has decreased.

a. Adult websites. Unsurprisingly, we see that the most blocked category is *Adult* where 85.4%, 82.2%, and 82% of the websites are blocked in 2018, 2019, and 2020, respectively. The content of the sites in this list is usually related to pornography, gambling, drugs, violence, and similar content inappropriate for young audience. We spot-checked the content of some of the *Adult* sites that were not blocked and found that most are related to art work including comics and caricatures (we did not find any that are pornographic, gambling, or drug-related for example). We note that the increase is minimal on the other categories that are least blocked; however, we observe the opposite on the sites from the most blocked categories (e.g., *Adult* and *Shopping*). We see that the largest additive difference in blocking is in the most blocked categories. The observed drop was due to websites that used to be blocked and later turned to be accessible. In addition, if we consider the top 200 sites sampled from the three lists for the *Adult* category corresponding to the three

measurements (since they are almost identical), we find that 98.5% and 94% were blocked in 2018 and 2020, respectively.

b. Shopping websites. The second most blocked category is *Shopping*. We believe the main reason behind blocking is that these sites sell products that are considered illegal (e.g., alcohol and guns).
c. Gaming websites. The third most blocked category is *Games*, in which all blocked sites related to gambling. Saudi Arabia considers gambling illegal since it is strictly prohibited under Islamic Shari'a law. There are no state-licensed casinos, bookmakers or poker rooms. In fact, all forms of gambling are illegal in the Saudi Arabia.
d. Globally popular websites. The *Global* category represents the most popular websites worldwide. In this category, we see that more than 7% of the these websites are blocked across the three-year measurements. We found that nearly 60% of these blocked sites also belong to the *Adult* category. The remaining 40% of the blocked sites belonged to social network applications such as WeChat and VK, as well as a few websites from China. Interestingly, in January 2019, students and faculty at the University of California (UC) have been warned not to use WeChat while visiting China; apparently, this warning is issued to protect their communications since that application raises security and privacy concerns [52].
Observation 2: Resolving a filtering mystery: most visited and yet blocked. Surprisingly, we see that 24, 23, and 19 of the most visited websites from Saudi Arabia per Alexa are blocked in 2018, 2019, and 2020, respectively. One might wonder how a popular site in the country is visited, while it is blocked. Alexa determines the popularity of a site based on two metrics: (1) Unique Visitors, which is the number of unique visitors of a web page; and (2) Pageviews, which corresponds to the number of URL requests (i.e., HTTP GET request) for a website [53]. Our multi-layer analysis of filtering was able to resolve the mystery. Our results show that all blocked sites from this category passed the DNS filtering test. This suggests that users received the requested DNS resolution, but were never able to view the web page, since it is blocked by other mechanisms as we discuss later in the section. However, its interesting that these sites are popular even as users fail to access them.

Observation 3: Finding a filtering loophole. We found a filtering weakness: content from a blocked website could be accessed indirectly through another website. This is best illustrated with this example: aljazeera.com is a blocked news site, while Twitter.com is not. A user could access contents on Aljazeera using its Twitter account as a "loophole": a link on Twitter points to an Aljazeera article. Since Twitter uses HTTPS, and hence, HTTP-URL-keyword filtering is not applied, we found that Aljazeera contents can be accessed and viewed from inside the country. This is surprising since we found evidence that filtering is performed at the TLS level (see Section 5.4); however, it is not applied in this scenario. Technically, the request through twitter.com/AlJazeera is missed by the filtering.

Observation 4: Server-side filtering. We also observe server-side filtering [54], where some websites reject requests from devices within Saudi Arabia. In other words, the website refuses to provide content to users in Saudi Arabia. An example of such a website is www.sce.com which belongs to Southern California Edison (SCE), a US company that provides energy and electricity to the Southern California region. While the site is accessible in US, HTTP code 502 is returned when trying to access it in Saudi Arabia indicating that the server blocked the connection. Our rational is that an energy company may want to protect its infrastructure.

The US power-infrastructure has already been the targets of cyber attacks, with the most recent being the Colonial pipeline.

Observation 5: Filtering seems to be consistent across ISPs. With respect to the operation of the filtering mechanism, we found that Internet filtering rules applied uniformly across the different vantage points and ISPs we tested: thus, we suspect that there is no additional ISP-level filtering. After verifying this observation, we show results only from one of the vantage points in the remainder of the paper (N6).

Observation 6: The kingdom is moving towards more moderate regulations on digital filtering. With regards to mobile apps measurements, our results show that all apps were blocked in 2017, but access was permitted to 67% in 2018 and 93% in 2019. We repeated the experiment in 2020 and found that all apps, except WeChat, were accessible; see Section 5.5.

Observation 7: Geopolitical events reflects on filtering. We found evidence of the impact of real-world events on filtering. See Section 5.6 for more details.

In the remaining of the section, we provide a more in-depth technical analysis of filtering and the mechanisms.

5.1 DNS Filtering

We conducted experiments to measure filtering at the DNS level. As shown in Table 2, we did not encounter a significant presence of DNS filtering, meaning that the majority of DNS lookups are successful. The numbers shown in the DNS-UDP and DNS-TCP columns correspond to transient connectivity issues such as TIMEOUT and SERVFAIL. A very small portion of DNS lookups, consistently returned REFUSED, NoAnswer, or NXDOMAIN DNS error codes, but the number is negligible. To ensure that these websites are actually not blocked, we checked their status using our machines in the US and verified that these websites return the same errors indicating that they have likely gone offline.

We wanted to further investigate if the transport protocol (UDP or TCP) of request has any effect on the outcome of filtering. Our results suggest that it does not. We found that there was no difference between DNS lookups performed using UDP and TCP. This indicates there are no constraints in DNS over TCP deployment in the country, i.e., there is no filtering of DNS over TCP requests. We also repeated the same DNS lookups on 6 open DNS servers. We found that the final results confirm our findings. There were minor variations between the behavior of the open DNS resolvers. For example, Comodo had the lowest success rate in DNS lookups (especially in UDP) in all categories.

5.2 IP Address Filtering

We conducted experiments to see if there is evidence of IP address filtering. Our measurements show a number of websites in which the IP address filtering failed as shown in Table 2. The data suggests that the main cause of this issue is not the Internet filtering system, but DNS lookup failures since no IP address is retrieved. For all other websites, the tool was able to connect to their IPs on port 80. This indicates there is no filtering at the level of TCP (or UDP) connection establishment.

5.3 HTTP Filtering

We find that the majority of the filtering happens at the HTTP filtering level. In fact, the filtering here is roughly two orders of magnitude compared to filtering at earlier stages of the connection. In Table 2, we see that column "HTTP" dominates. A large number of websites were filtered based on the HTTP URL string, (either FQDNs or special keywords): 82.2%, 7.6%, and 6.2% of the Adult, Shopping, and Games websites were blocked in 2019, respectively. These connections were blocked at the HTTP level. In fact, we examined the logs, and we verified that the TCP 3-way handshake process between our Saudi machines and the forbidden site's web server establishes successfully.

To fully explore this filtering stage, we want to identify if the filtering happens by examining the name of the domain (i.e., FQDN-based filtering), or via the use of keywords (i.e., URL-keyword filtering), as we discussed earlier.

a. FQDN-based filtering. We send the GET request directly to the website server of the FQDN we want to test. The filtering system allows the client to send the GET request (i.e., the request is forwarded to the forbidden server); however, instead of receiving a legitimate HTTP response, the system replies back with an HTTP response with the status code 403 for accessing forbidden content. This observation contradicts the findings by Verkamp et al. [17] where the authors report that a spoofed HTTP response with a status code 200 is returned, perhaps indicating that the filtering implementation has changed. The filtering mechanism then directs the user to one of the warning pages shown in Fig. 3 and Fig. 4, based on the site's category. The warning page is an HTML < iframe > presenting a warning message both in Arabic and English. Figure 12 shows a Wireshark trace for blocked website www.betonline.ag (a gambling website). What happens after the prohibited request is received? By analyzing the traces, we found that after receiving the 403 HTTP error code, the client receives TCP-RST packets forcing a termination of the HTTP connection. The error message displayed when a blocked website is accessed explicitly indicates that this filtering is maintained by a company called Wire Filter [55] (see the HTML < iframe > in Fig. 13). Our investigation shows that WireFilter provides web security solutions and services (such as filtering) in Saudi Arabia [56].

b. URL-keyword filtering. As we explained earlier, this filtering mechanism searches the URL string against a forbidden list of strings. We find that overall URL-keyword matching plays a significant role in the filtering process.
In more detail, our results show identical behavior of filtering as in the case of FQDN-based HTTP filtering, confirming that the filtering uses URL-keyword filtering. The difference in these two cases occurs when using HTTPS. When we repeat the keyword-filtering experiments using HTTPS, the filtering does not work and the client receives the 404 Page Not Found code indicating that URL-keyword filtering works only at the HTTP-level connection. In this case, the connection (including the TLS handshake) is being established to the unblocked website (a.com), which returns that the specific page (the one we created with the blocked domain) is not found – no filtering occurred. A breakdown of HTTP filtering results is shown in Fig. 14.

5.4 TLS Filtering

We wanted to test whether how filtering handles requests using the HTTPS protocol. Recall that HTTPS encrypts the payload, which many filtering agencies can consider undesirable. We found that if the website being contacted is blocked, it remains blocked under HTTPS. When examining the traces, we discovered that this is due to TLS level filtering. As shown in Fig. 15, when trying to access the blocked website www.betonline.ag, the filtering system allows the TCP 3-way handshake but sends a TCP-RST packet when the client tries to establish a TLS connection. On Windows, when we sent the GET request, the Windows socket error code 10054 was returned, indicating that the HTTPS connection was forcibly closed by the server. In this case, the browser displays a page (as shown in Fig. 16) indicating that the HTTPS/TLS connection could not be established.

5.5 Mobile Application Filtering

In this section, we report our results in regards to mobile application filtering, and we start by providing some context regarding the policies of Saudi Arabia.

Historical context regarding mobile app usage. In 2013, CITC blocked the Voice over Internet Protocol (VoIP) call services on Viber, a popular mobile application that offers free video/voice calls [57]. VoIP calls on similar applications were slowly being blocked including FaceTime, Skype, Line, Tango, Facebook Messenger, WhatsApp and Snapchat. We believe that the main reason behind this ban was economic, since these applications provide free alternatives to services that otherwise generate revenue to cellular carriers and ISPs. CITC received requests from service providers such as Mobily and STC to block the free or low-cost VoIP calls on these applications to protect their competitiveness and rights [58, 59]. However, in 2017, CITC responded to citizens demands and announced its intent to lift the ban on all applications that provide voice and video communications over the Internet, as long as they meet the regulatory requirements of the country [60]. We conjecture that this decision was also driven by the Vision 2030 and National Transformation 2020 programs published with the aim of modernizing society. One of the stated goals is to provide transparency and clarity with respect to policies, especially in the telecommunications and information technology sectors.

We conduct our measurements for mobile apps over three years and show the results in Table 3. We consider 16 communication mobile apps including FaceTime, Tango, Line, Viber, SOMA, YeeCall, Facebook Messenger, WhatsApp, Snapchat, and imo. We attempt to install and use them on two iPhones, one in Saudi Arabia and the other in USA. We tested the text, audio, and video communication services. All of these apps support text, audio and video communication.

In March 2018, five applications failed to establish at least one of the text, audio, and video communication services, as shown in Table 3. WhatsApp and Viber established an active connection for 1–2 seconds, but then the calls got disconnected suddenly. We believe that this experiment indicates that these two applications were indeed blocked in Saudi Arabia [61]. We also found that VoIP calls on imo are blocked in Saudi Arabia.

In October 2019, we repeated the experiment and added two more applications: Houseparty and WeChat. We found that both audio and video calls are blocked on WhatsApp, which was corroborated by a CITC

statement [62].

The application WeChat exhibits a uniquely interesting behavior. WeChat is one of the most popular messaging applications owned by the Chinese company Tencent [52, 63, 64]. In Saudi Arabia, the installation of the application comes with a pre-condition: the user has to show that s/he has a friend on WeChat, who needs to meet additional requirements as shown in Fig. 17 above! These requirements for the friend are that s/he: (a) has been a WeChat user for at least one month if s/he an international user or for 6 months if s/he is a China Mainland user; (b) has not completed "Help Friend Register" check for other new user in the past month; (c) has not been blocked from using WeChat in the past month; and (d) if s/he is a China Mainland user, s/he has activated WeChat Pay. By contrast, WeChat can be installed in the US without any such requirements. Intrigued, we repeated the experiment with three more iPhones in Saudi Arabia. The installation failed on all of them for the same reason. Although the vice president of Tencent announced back in 2013 that WeChat is available in Saudi Arabia [65], this is not fully accurate. Currently, we are not sure if the installation failure is caused by Tencent or the Internet filtering system.

All other tested messaging applications are open and supported including Viber and imo.

Finally, in April 2020, we repeated the experiment and found that nearly all previously-blocked messaging applications were accessible, including WhatsApp, with the only exception being WeChat.

5.6 The Effect of Geopolitical Events on Internet Filtering

Over the past years, the Middle East experienced several major political events that caused world-wide ramifications. We quantify the effect of these events on Saudi Arabian policies regarding access to information, as we discuss below.

A prominent event was the rise of the so-called “Islamic State” in Iraq and Syria (known as ISIS) in the last decade with global impact. We tested the accessibility of a number of ISIS-friendly websites and found that all of them were blocked. Note that we obtained these sites by searching prominent ISIS-friendly websites on the web and following links from authoritative sources: following previous practices, we do not publicly disclose these sites due to ethical considerations. ISIS and its affiliates have exploited social media websites, such as Twitter, to spread their propaganda and to recruit new members [66]. This type of activity has in turn been countered by efforts from the Saudi Arabian government by regulating information access for Saudi citizens. For instance, at the Shura Council, the chairman of the Islamic and judicial affairs committee called for the blocking of all ISIS websites as they were considered sources of terrorism and destabilization for the region [42]. Restricting access to these sites was also implemented by many other countries and institutions [67–71]. In addition, many Saudi citizens launched an online campaign on Twitter aiming to lock down user accounts belonging to or supporting ISIS [72].

Another prominent event is the increased political tension between Qatar and Saudi Arabia, which was also captured in our measurements. Because of these tensions, the Saudi authorities blocked some Qatari news web sites [73] in 2017. For instance, as shown in Fig. 4, a warning page by the Ministry of Culture and Information was displayed when we tried to visit www.aljazeera.com; one of the most popular news

websites in Qatar. In addition, in April 2020, we obtained a list of Qatari news sites [73] and found that all of them were blocked.

Another notable geopolitical event in our study period is the ongoing conflict between Saudi Arabia and Iran. Following an attack on the Saudi embassy in Tehran in January 2016 [74], Saudi Arabia cut all diplomatic relations with Iran. Our measurements show evidence of this event through its impact on the Internet filtering. In particular, our measurements in 2018 show that many of the top Iranian sites (mostly from the News category) got blocked.

Finally, in April 2020, we observed a change in the access for some Turkish sites compared to the earlier measurements. Upon investigation, we found that Saudi authorities blocked two prominent Turkish news websites, Anadolu and TRT Arabic platforms, amid what the Ministry of Media communicated as continued violations of their regulations. We conjecture that the move was partly driven by a campaign on Twitter by Saudi citizens calling for the Turkish news platforms to be blocked [75].

6 Internet Filtering Infrastructure

In the past, all network traffic in Saudi Arabia was directed to a central network at the Internet Service Unit (ISU). In 2016, the volume of international Internet traffic rose by 114% relative to the traffic in 2015 (to 3.185 TB/s [32]). With the increasing market penetration of Internet connectivity and the accompanying growth in Internet traffic, the Internet filtering infrastructure has also evolved. All outbound Internet connectivity is routed through two main Data Service Providers (DSPs): (1) the Integrated Telecom Company (by Mobily) and (2) Bayanat al-Oula for Network Services (by Mawarid Holding Group), to provide national and international Internet communications services [76].

To explore the filtering infrastructure, we used the tracert utility to identify the network paths between machines inside and outside the country. We conducted our measurements by randomly selecting 10 public IP addresses of machines outside Saudi Arabia, which were verified using the tool [77]. We also confirmed that these machines are accessible and responsive to tracert from our US vantage points.

When an end-user in Saudi Arabia sends a request to an international website, the request first goes through her ISP's proxy before it reaches the DSPs' proxy servers. Then, we observed that before connecting to hops outside the country, the packets has to go through a node with a private address (10.188.x.x) as shown in Fig. 18, which we assume is the IP address of the system used for Internet filtering. CITC clearly states that the Internet filtering servers are located in a centralized access point at KACST, which is located in Riyadh [1, 30]. The filtering infrastructure is illustrated with in Fig. 19.

To further validate that 10.188.x.x is the filtering center, we conducted a two-directional measurement as follows. We conducted the same measurement to tracert from one of our machines in Saudi Arabia, say A, to our lab machine in the US, say B. We then compared the path of the routers visited A → B and B → A using tracert. The two measured paths were similar in terms of router prefixes with the exception of the filtering node (10.188.x.x), which was not present on the traceroute originating from USA host to Saudi Arabia.

As a final step to increase our confidence, we repeated the above measurement from 10 hosts within Saudi Arabia and from two cities: Jeddah and Makkah. The tracert outputs reveal a large amount of nodes that share the same address space as the filtering node, confirming that all network traffic within the country passes through centralized servers as well.

7 Related Work

As the Internet has grown to be an essential service for accessing information, sharing opinions, coordinating activist organization, many countries have sought to regulate this open access through Internet filtering. As a result, many studies have been conducted to examine the filtering practices and mechanics in different countries around the world. In this section, we briefly survey a number of these studies and explain their relationship to our work where appropriate.

a. Country-Specific Internet Filtering studies. For some countries, the underlying motivation to effect filtering believed to be political. For instance, Nabi [20] used a publicly available dataset of websites to check their accessibility in Pakistan. He found that the government performs filtering at DNS and HTTP levels. Aryan et al. [45] showed evidence that all Internet traffic in Iran is directed to a centralized equipment which is apparently controlled by the government. In 2011, during the political events in Libya and Egypt, Dainotti et al. [78] analyzed country-wide government-ordered Internet outages using a variety of publicly available datasets. Furthermore, Chaabane et al. [50] presented results of measurements analysis of a sophisticated Internet filtering system enforced by the Syrian government. They discovered that Instant Messaging is heavily censored. Many studies have explored the Internet filtering infrastructure of the Great Firewall of China (GFW) over the years [18, 28, 47]. In the UK [79] a system filters pedophile advocacy websites that promote sexual exploitation of children. In Germany, all Nazi promoting websites are blocked by the government [80]. Internet filtering can also be imposed by Internet users on themselves. For instance, Gebhart et al. [81] presented an adequate and a comprehensive study on Internet filtering in Thailand. They distributed a survey on 160 respondents and found that nearly 70% of them enable filtering settings on their connections. At the economic level there is evidence of some companies or organizations using Internet filtering to force customers to use specific products [82]. We expect such economically driven filtering to increase if net neutrality repeal efforts go into law in the USA.

b. Studies on Internet Filtering in Saudi Arabia. Most related to our study, Zittrain and Edelman conducted the first study on Internet filtering in Saudi Arabia [38]. In 2002, they used proxy servers to prop a list of random distinct websites (approximately 64,557) from 6 different categories. They performed a lightweight measurement study and concluded that nearly 3.15% of the websites were blocked based on different categories. Likewise, in 2004, the OpenNet Initiative (ONI) organization published a similar report [83] and confirmed the findings in [38]. Most recently, in 2012, Verkamp and Gupta [17] studied the filtering mechanics used in 11 countries, including Saudi Arabia. They claimed that Internet filtering in Saudi Arabia is based on destination IP address filtering and directs users to an HTTP response with a status code of 200. Our study is similar in spirit, but substantially larger in scale, covering systematically classes of websites and mobile applications. Our study is also repeated over multiple years at a time where Saudi Arabia is experiencing a shift to modernize. We also explore the technical mechanisms underlying the

observed behavior in detail. In fact, our results show substantial differences from these earlier studies; for example, we found that filtering is applied at the HTTP and TLS levels instead of IP. We also repeat our analysis multiple times and observe trends in filtering over time.

c. Filtering Measurement Tools. Several research efforts developed tools to measure and study Internet filtering. For instance, CensMon [27] was developed as a tool to monitor and detect filtering characteristics globally. UBICA [84] was designed to aggressively collect filtering-related data from different vantage points by running the tool on home gateways and personal computers. OONI [85] and ICLab [86] are two other platforms that are designed to detect filtering using embedded devices such as Raspberry Pis [87]. Iris [88] is also developed as a scalable, accurate, and ethical method focusing on the problem of measuring manipulations on the DNS protocol. In addition, Nabi used a test script, dubbed Samizdat [20], that inspired our filtering tool. Samizdat first downloads a list of websites and prepares it for testing. For each website, the tool performs a DNS lookup to check for DNS level filtering. It then tries to establish a TCP connection. Next, the tool checks for HTTP-URL-keyword filtering. In the last step, the tool checks for HTTP-FQDN filtering. For each test, the results are recorded in a log file locally consistent with recommended ethical practices (i.e., not in a remote server as in [27]). Our tool provides significant new functionality. For example, some of our modifications include a different website input and preparation process: the websites are distinct per category since they are crawled directly from Alexa and do not need cleaning to remove redundancy.

d. Data Resources. The are also some efforts that provide network accessible data. For instance, ONI [89] makes global Internet filtering data more accessible to researchers and journalists. However, their data is outdated with the last release being in September 2013 while for Saudi Arabia the latest release was in 2009. The University of Michigan, on the other hand, established a project called Censored Planet [90] to frequently update the filtering data. The project contains a publicly accessible database with global footprint.

8 Conclusion

In this paper, we study Internet filtering in the Kingdom of Saudi Arabia: a traditionally conservative country, which seems to have made significant steps towards modernization in the last five years. This move towards openness is amply supported by our work. Our contributions are twofold.

First, we develop a comprehensive methodology and tools to measure, collect and analyze Internet filtering behavior at a refined level of granularity. In addition, we expand the concept of filtering to consider access to mobile applications. We also develop techniques to distinguish between four types of filtering: (a) DNS level filtering, (b) IP address filtering, (c) HTTP filtering, and (d) TLS filtering. This in depth examination can provide significant information on the strengths and limitations of a filtering approach.

Second, we present a comprehensive longitudinal study of Internet filtering in Saudi Arabia over the period of three years. The overall conclusion is that Saudi Arabia has become more moderate in its digital filtering policy. We evaluate filtering behavior by probing Alexa's top 500 websites in 18 different categories from vantage points covering the three largest telecommunications companies in Saudi Arabia and five cities. We find that mobile application accessibility has become significantly more moderate. We find that among 17

of the most popular mobile social network applications such as WhatsApp, Facetime, and Skype, are now accessibly, and only WeChat is still not freely available in Saudi Arabia. We also find that geopolitical events such as the rise of ISIS or intra-country tensions have a direct effect on digital filtering.

We see our work as a fundamental step towards developing a deep understanding of the various techniques that are used to support filtering. To further facilitate research in this area, we intend to provide open access to our tool and data to the research community.

Declarations

Acknowledgements

This material is based on work partially supported by Taibah University (TU) and the Saudi Ministry of Education (MOE). The work is also partially supported by the University of California Office of the President UC Lab Fees grant number LFR-18-548554. Any opinions, findings, and conclusions or recommendations expressed in this work are those of the authors and do not necessarily reflect the views of the funding agencies.

Data Availability

The datasets generated and analyzed during this study are not publicly available due ethical considerations as discussed in Section 4.1.

References

1. Communications and Information Technology Commission (CITC). General Information on Filtering Service. https://filter.sa/en/general-information-on-filtering-service/. Online; accessed 26 December 2021.
2. Freedom in the world 2021: Saudi arabia. Free. House (2021)., available at https://freedomhouse.org/country/saudi-arabia/freedom-world/2020.
3. The 2021 world press freedom ranking (2021)., available at https://rsf.org/en/ranking.
4. The 15 enemies of the internet and other countries to watch (2016)., available at https://rsf.org/en/news/15-enemies-internet-and-other-countries-watch.
5. Ministry of Media. Regulations. https://www.media.gov.sa/en/document-library. Online; accessed 29 December 2021.
6. Ministry of Interior. Reporting Cyber Crimes, available at: https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/6166.
7. Communications and Information Technology Commission (CITC). Anti-Cyber Crime Law. https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/2 (2007).
8. Cybersecurity for Children Association. https://www.cyberkids.org.sa/.

9. Hemaya Group. Saudi Group for Information Assurance. http://hemayagroup.org/home/.
10. Alkadhi, Meshal. Al-Burhan. http://www.el-burhan.com/blog/.
11. Safer Internet Day. https://www.saferinternetday.org/.
12. Communications and Information Technology Commission (CITC). Blocking protects Internet users from the damage caused by some inappropriate sites: https:// (2010).
13. Saudi Vision 2030. Vision 2030. http://vision2030.gov.sa/en. Online; accessed 29 December 2021.
14. The ban on saudi women driving is ending: Here's what you need to know (2018)., available at https://www.cnn.com/2018/06/22/middleeast/saudi-women-driving-ban-end-intl/index.html.
15. General Entertainment Authority. https://www.gea.gov.sa/en/.
16. Mathrani, A. & Alipour, M. Website blocking across ten countries: A snapshot. In PACIS, 152 (2010).
17. Verkamp, J.-P. & Gupta, M. Inferring mechanics of web censorship around the world. In FOCI (2012).
18. Xu, X., Mao, Z. M. & Halderman, J. A. Internet censorship in china: Where does the filtering occur? In International Conference on Passive and Active Network Measurement, 133–142 (Springer, 2011).
19. Alexa Top Sites. The top 500 sites on the web (2018)., available at https://www.alexa.com/topsites.
20. Nabi, Z. The anatomy of web censorship in pakistan. In FOCI (2013).
21. Alharbi, F., Faloutsos, M. & Abu-Ghazaleh, N. Opening digital borders cautiously yet decisively: Digital filtering in Saudi arabia. In 10th {USENIX} Workshop on Free and Open Communications on the Internet ({FOCI} 20) (2020).
22. Al-Tawil, K. M. The internet in saudi arabia. Telecommun. Policy 25, 625–632 (2001).
23. King Abdulaziz City for Science and Technology: Maeen Network. Internet Service Unit. https://www.maeen.sa/en/about/isu/ (Online; accessed 29 December 2021).
24. Communications and Information Technology Commission (CITC). Annual Report 2005. http://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR_REP_001E.pdf. Online; accessed 29 December 2021.
25. General Authority for Statistics (GASTAT). Annual Yearbook 2018. https://www.stats.gov.sa/en/46. Online; accessed December 2021.
26. CSaudi Gazette. Full text of Saudi Arabia's Vision 2030. https://english.alarabiya.net/en/perspective/features/2016/04/26/Full-text-of-Saudi-Arabia-s-Vision-2030.html (2016). Al-Arabiya News.
27. Sfakianakis, A., Athanasopoulos, E. & Ioannidis, S. Censmon: A web censorship monitor. In USENIX Workshop on Free and Open Communication on the Internet (FOCI) (2011).
28. Clayton, R., Murdoch, S. J. & Watson, R. N. Ignoring the great firewall of china. In International Workshop on Privacy Enhancing Technologies, 20–35 (Springer, 2006).
29. Freedman, M. J. Experiences with coralcdn: A five-year operational view. In NSDI, 95–110 (2010).
30. Communications and Information Technology Commission (CITC). General Information on Filtering Service. https://filter.sa/en/general-information-on-filtering-service/. Online; accessed 29 December 2021.

31. Communications and Information Technology Commission (CITC). Block Website Request. www.filter.sa. Online; accessed 14 April 2020.
32. Communications and Information Technology Commission (CITC). Annual Report 2016. (2016)., available at http://www.citc.gov.sa/en/mediacenter/annualreport/Documents/PR_REP_012Eng.pdf.
33. Communications and Information Technology Commission (CITC). CITC receives more than one million applications for blocking links by the end of 2017. http://. Online; accessed 29 December 2021.
34. Evans, P. Will germany's new law kill free speech online? BBC News (2017)., available at http://www.bbc.com/news/blogs-trending-41042266.
35. COUNCIL OF THE EUROPEAN UNION. Joint meeting of the Law Enforcement Working Party and the Customs Cooperation Working Party. http://register.consilium.europa.eu/doc/srv?l=EN&f=ST20718120201120COR201 (2011).
36. Gunn, A. French assembly passes 'three strikes' hadopi law. Beta News (2009)., available at https://betanews.com/2009/05/12/french-assembly-passes-three-strikes-hadopi-law/.
37. King Saud University. Saudi internet rules, 2001. http://fac.ksu.edu.sa/hidaithy/page/20215 (Online; accessed 29 December 2021).
38. Zittrain, J. & Edelman, B. Documentation of internet filtering in Saudi Arabia (Harvard Law School, 2002).
39. Saba, M. Will 'american dad' define the saudis for us? Arab. News (2005)., available at http://www.arabnews.com/node/277392.
40. Sar, E. V. Saudi arabia government blocks the pirate bay (and more). TorrentFreak (2014)., available at https://torrentfreak.com/saudi-arabia-government-blocks-pirate-bay-140402/.
41. writer, S. 'isis is enemy no. 1 of islam,' says saudi grand mufti. Al-Arabiya News (2014)., available at https://english.alarabiya.net/en/News/middle-east/2014/08/19/Saudi-mufti-ISIS-is-enemy-No-1-of-Islam-.html.
42. Alarabiya. Saudi arabia.. al-shura demands to ban all isis web sites. Alarabiya (2016)., available at http://ara.tv/gqz88.
43. Saudi orders telcos to ensure skype, whatsapp meet local laws. Reuters Newsl., available at https://www.reuters.com/article/saudi-telecoms-ban/saudi-orders-telcos-to-ensure-skype-whatsapp-meet-local-laws-idUSL5N0CN0DH20130331 (2013).
44. Arends, R., Austein, R., Larson, M., Massey, D. & Rose, S. RFC 4035 - Threat Analysis of the Domain Name System (DNS) (2005).
45. Aryan, S., Aryan, H. & Halderman, J. A. Internet censorship in iran: A first look. In FOCI (2013).
46. Lowe, G., Winters, P. & Marcus, M. L. The great dns wall of china. MS, New York Univ. 21, 1 (2007).
47. Levis, P. The collateral damage of internet censorship by dns injection. ACM SIGCOMM CCR 42 (2012).
48. Towards a comprehensive picture of the great firewall's DNS censorship. In 4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14) (USENIX Association, San Diego, CA, 2014)., available at https://www.usenix.org/conference/foci14/workshop-program/presentation/anonymous.

49. Ensafı, R., Winter, P., Mueen, A. & Crandall, J. R. Analyzing the great firewall of china over space and time. Proc. On privacy enhancing technologies 2015, 61–76 (2015).
50. Chaabane, A. et al. Censorship in the wild: Analyzing internet filtering in syria. In Proceedings of the 2014 Conference on Internet Measurement Conference, 285–298 (ACM, 2014).
51. Alexa Top Sites. The alexa top sites web service., available at https://aws.amazon.com/alexa-top-sites/.
52. Griffiths, J. University of california tells students not to use wechat, whatsapp in china. CNN (2019)., available at https://www.cnn.com/2019/01/11/asia/university-california-china-wechat-intl/index.html .
53. Alexa. How are Alexa's traffic rankings determined? Available at https://support.alexa.com/hc/en-us/articles/200449744-How-are-Alexa-s-traffic-rankings-determined-.
54. Tschantz, M. C. et al. A bestiary of blocking: The motivations and modes behind website unavailability. In 8th {USENIX}Workshop on Free and Open Communications on the Internet ({FOCI} 18) (2018).
55. Wire Filter. http://www.wirefilter.com/. Online; accessed 29 December 2021.
56. Wire Filter. https://wirefilter.com/solutions/web-security-solutions/. Online; 29 December 2021.
57. Ushe, S. Saudi arabia blocks viber messaging service. BBC News (2013)., available at https://www.bbc.com/news/world-middle-east-22806848.
58. Gaskell, H. Whatsapp's new call service to be blocked in ksa. ITP.net (2015)., available at https://www.itp.net/security/602475-whatsapps-new-call-service-to-be-blocked-in-ksa.
59. Griffin, A. Facebook messenger blocked in saudi arabia: Chat apps have voice and video call functions banned over regulations. Independent (2016)., available at https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-messenger-blocked-in-saudi-arabia-chat-apps-have-voice-and-video-call-functions-banned-over-a7027301.html.
60. Communications and Information Technology Commission (CITC). In line with the needs of the user and in line with global trends, CITC announces the launch of Internet communications applications. http://www.citc.gov.sa/ar/mediacenter/pressreleases/Pages/2017092001.aspx (2017).
61. Arab News. Saudi Communications Commission activates Internet calls, WhatsApp still blocked. https://www.arabnews.com/node/1164956/saudi-arabia (2017).
62. Whatsapp calls are blocked in saudi arabia. the reasons are organizational. Sabq (2019)., available at https://sabq.org/wY2Vmk.
63. McDonell, S. https://www.bbc.com/news/blogs-china-blog-48552907.(2019).
64. China's WeChat, Weibo and Baidu under investigation. BBC News (2017)., available at https://www.bbc.com/news/world-asia-china-40896235.
65. Wechat arrives in saudi arabia. Saudi Gazette (2013)., available at http://saudigazette.com.sa/article/47305.
66. Osborne, C. Anonymous targets isis social media, recruitment drives in #opisis campaign. ZDNet (2015)., available at https://www.zdnet.com/article/anonymous-targets-isis-social-media-recruitment-drives-in-opisis-campaign/ .

67. Facebook. Hard questions: How we counter terrorism. Facebbok (2017)., available at https://about.fb.com/news/2017/06/how-we-counter-terrorism/.
68. Reisinger, D. Twitter has suspended 1.2 million terrorist accounts since 2015. Fortune (2018)., available at https://p.dw.com/p/1FyTF.
69. DW. Turkey blocks websites loyal to isis. DW (2015)., available at https://p.dw.com/p/1FyTF.
70. Noon. Iraq: Minister of communications: Blocking isis websites tops our ministerial program. Noon (2014)., available at http://www.non14.net/public/56224.
71. Lomas, N. Uk outs extremism blocking tool and could force tech firms to use it. TechCrunch (2018)., available at https://techcrunch.com/2018/02/13/uk-outs-extremism-blocking-tool-and-could-force-tech-firms-to-use-it/.
72. Hazaa, M. A. A popular campaign to close isis accounts on twitter. Alarabiya (2015).
73. Here is a list of all qatari web sites that are blocked in saudi arabia. Alarabiya (2017)., available at http://ara.tv/z8sek.
74. Hun condemns attack on saudi embassy in iran. BBC News (2016)., available at https://www.bbc.com/news/world-middle-east-35229385.
75. The New Arab. Saudi Arabia blocks Turkish news sites Anadolu, TRT amid continued Ankara-Riyadh tensions (2020). Available at https://english.alaraby.co.uk/news/saudi-arabia-blocks-turkish-news-sites-anadolu-trt.
76. Saudi arabia country report - freedom on the net 2018. Free. House (2018)., available at https://freedomhouse.org/report/freedom-net/2018/saudi-arabia.
77. IPInfoDB. IP Address Information. https://ipinfodb.com/. Online; accessed 29 December 2021.
78. Dainotti, A. et al. Analysis of country-wide internet outages caused by censorship. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference, 1–18 (ACM, 2011).
79. Clayton, R. Failures in a hybrid content blocking system. In International Workshop on Privacy Enhancing Technologies, 78–92 (Springer, 2005).
80. Dornseif, M. Government mandated blocking of foreign web content. arXiv preprint cs/0404005 (2004).
81. Gebhart, G. & Kohno, T. Internet censorship in thailand: User practices and potential threats. In 2017 IEEE European symposium on security and privacy (EuroS&P), 417–432 (IEEE, 2017).
82. Comcast Corporation. Before the federal communications commission in the matter of broadband industry practices. https://docs.fcc.gov/public/attachments/FCC-08-183A1.pdf (2008). Online; accessed 29 December 2021.
83. Initiative, O. et al. Internet filtering in saudi arabia in 2004. Berkman Cent. for Internet Soc. (2004).
84. Aceto, G. et al. Monitoring internet censorship with ubica. In International Workshop on Traffic Monitoring and Analysis, 143–157 (Springer, 2015).
85. Filasto, A. & Appelbaum, J. Ooni: Open observatory of network interference. In FOCI (2012).
86. ICLab. Uk outs extremism blocking tool and could force tech firms to use it., available at https://iclab.org/.
87. Pi, R., available at https://www.raspberrypi.org/.

88. Pearce, P. et al. Global measurement of {DNS} manipulation. In 26th {USENIX} Security Symposium ({USENIX} Security 17), 307–323 (2017).
89. OpenNet Initiative. Opennet initiative., available at https://opennet.net/research/data.
90. Censored Planet. Censored Planet. https://censoredplanet.org/about. Online; accessed 2 January 2022.

Tables

Table1. Measurement Vantage Points

ID	City	ISP
N1	Riyadh	STC
N2	Jeddah	STC
N3	Al-Khobar	STC
N4	Makkah	STC
N5	Makkah	Zain
N6	Makkah	Mobily

Table 2. Breakdown of Internet filtering results against Alexa top 500 websites in 18 categories. Numbers in blue, green, and red denote results in 2018, 2019, and 2020, respectively. The HTTP and TLS/HTTPS results are for status code 403. Note that these are the absolute numbers of filtered/failed requests at each stage of the communication: DNS filtering, IP address filtering, HTTP filtering and TLS/HTTPS filtering

Category	Filtering Method														
	DNS						IP			HTTP			TLS/HTTPS		
	UDP			TCP											
Adult	5	7	3	7	9	5	2	8	8	427	411	410	4	1	1
Arts	2	5	6	5	6	4	9	11	10	12	10	8	10	7	7
Business	3	10	11	3	8	5	6	13	14	30	26	20	38	29	15
Computers	0	0	0	0	0	0	1	0	0	10	9	8	8	6	3
Games	0	0	1	0	0	0	0	0	0	36	31	30	13	11	11
Global	6	7	7	6	7	7	12	12	12	35	31	28	9	8	6
Health	4	3	5	4	3	2	7	6	5	13	9	7	17	8	2
Home	1	2	0	1	2	1	4	5	4	9	8	8	16	10	7
Kids & Teens	2	1	1	2	1	1	3	1	0	7	6	5	12	6	5
News	0	0	0	0	0	1	1	0	0	21	19	19	20	17	13
Recreation	0	0	0	0	0	0	6	2	1	20	18	16	18	15	11
References	0	1	1	0	0	0	0	2	1	5	4	4	6	6	6
Regional	1	1	0	1	1	1	1	3	2	26	25	22	21	20	20
Saudi Arabia	12	12	12	11	12	13	18	18	18	24	23	19	15	15	14
Science	3	0	1	3	0	0	3	1	1	5	3	1	6	5	5
Shopping	1	1	0	1	1	1	1	1	1	46	38	35	48	36	33
Society	0	0	0	0	0	0	4	1	2	20	20	19	18	17	17
Sports	0	0	0	0	0	0	1	0	0	8	4	1	11	9	8

Table 3. The evolution of access to popular messaging mobile applications, including text, audio and video communications. Symbols show if a communication service is supported (√), blocked (☒), not applicable (NA) (e.g., service not available at the time), or not tested (NT). Note that the results displayed for the period 2013-2017 are based on personal experience and not extensive measurements. Also note that the release date of all apps except HouseParty (released in 2019) is either before or within this period. For instance, Line, Telegram, and Google Duo were initially released in 2011, 2013, and 2016, respectively.

Application	2013-2017			2018			2019			2020		
	Text	Audio	Video	Text	Audio	Video	Text	Audio	Video	Text	Audio	Video
Viber	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
Tango	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
FaceTime	✓*	✗	✗	✓*	✓	✓	✓*	✓	✓	✓*	✓	✓
YeeCall	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Skype	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
WhatsApp	✓	✗	✗	✓	✗	✗	✓	✗	✗	✓	✓	✓
Line	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
Telegram	✗	✗	NA	✗	✗	NA	✓	✓	NA	✓	✓	NA
AllApp	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Google Duo	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Houseparty	NA	NA	NA	NA	NA	NA	✓	✓	✓	✓	✓	✓
WeChat	NT	NT	NT	NT	NT	NT	✗	✗	✗	✗	✗	✗
SOMA	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Snapchat	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Google Hangout	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Facebook Messenger	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
imo	✓	✗	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
JusTalk	NT	NT	NT	✓	✓	✓	✓	✓	✓	✓	✓	✓

* Text is iMessage

Figures

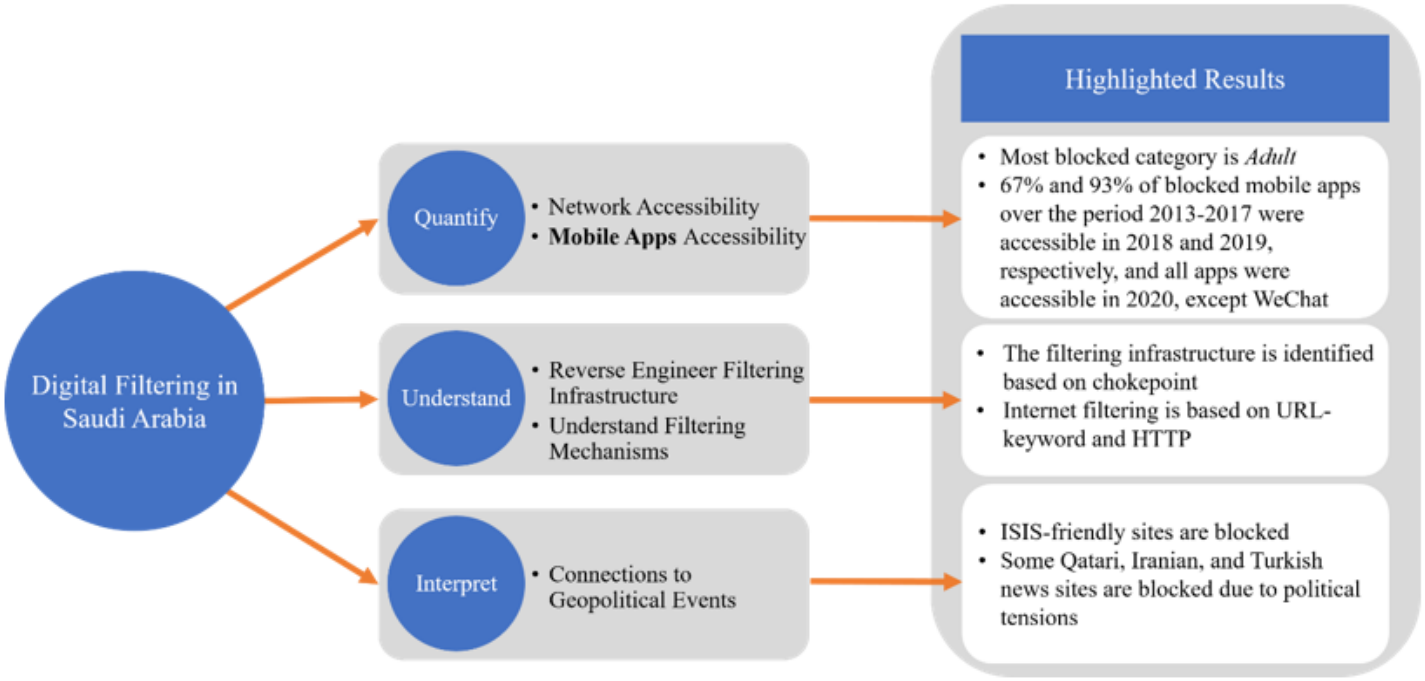


Figure 1

Overview of the key questions, contributions, and findings of our work

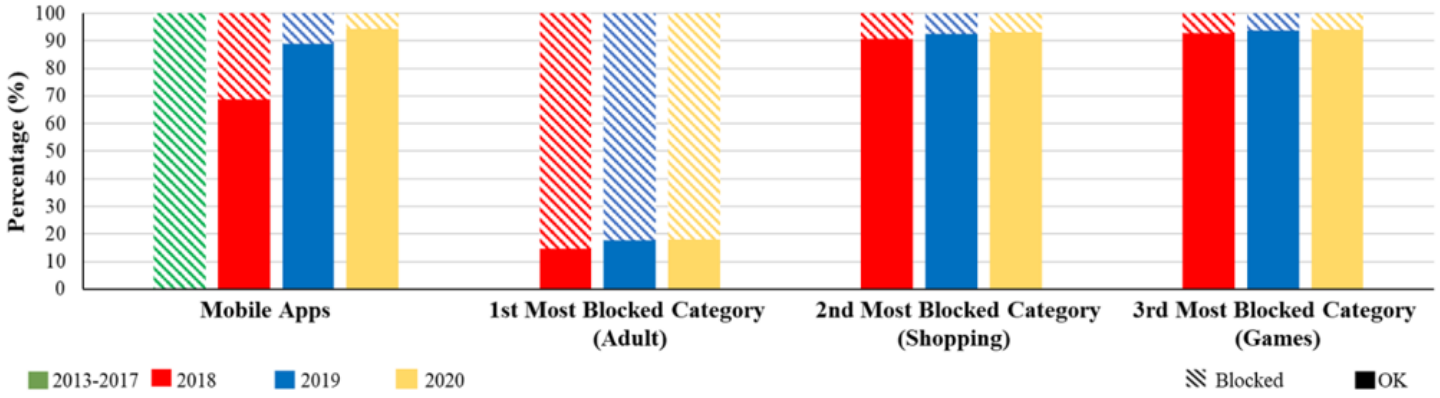


Figure 2

Overview of the extent of filtering over time per category. We observe a significant relaxing of the filtering rules for both Internet and mobile apps. Note that we did not measure the period 2013-2017 but rely instead on personal use and public sources (e.g., Twitter and Saudi news sites). The bars for mobile apps represent the percentage of the apps that were tested at that time period: we added two new apps in 2019.

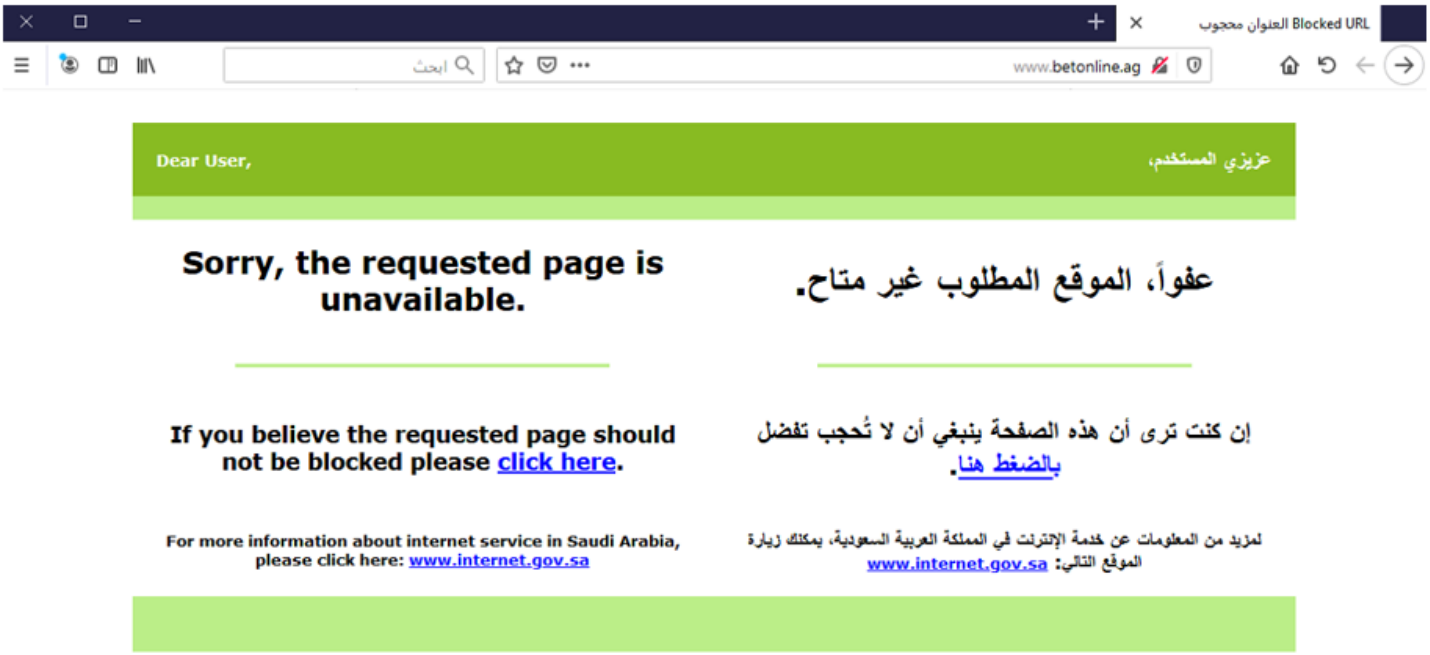


Figure 3

General filtering warning page

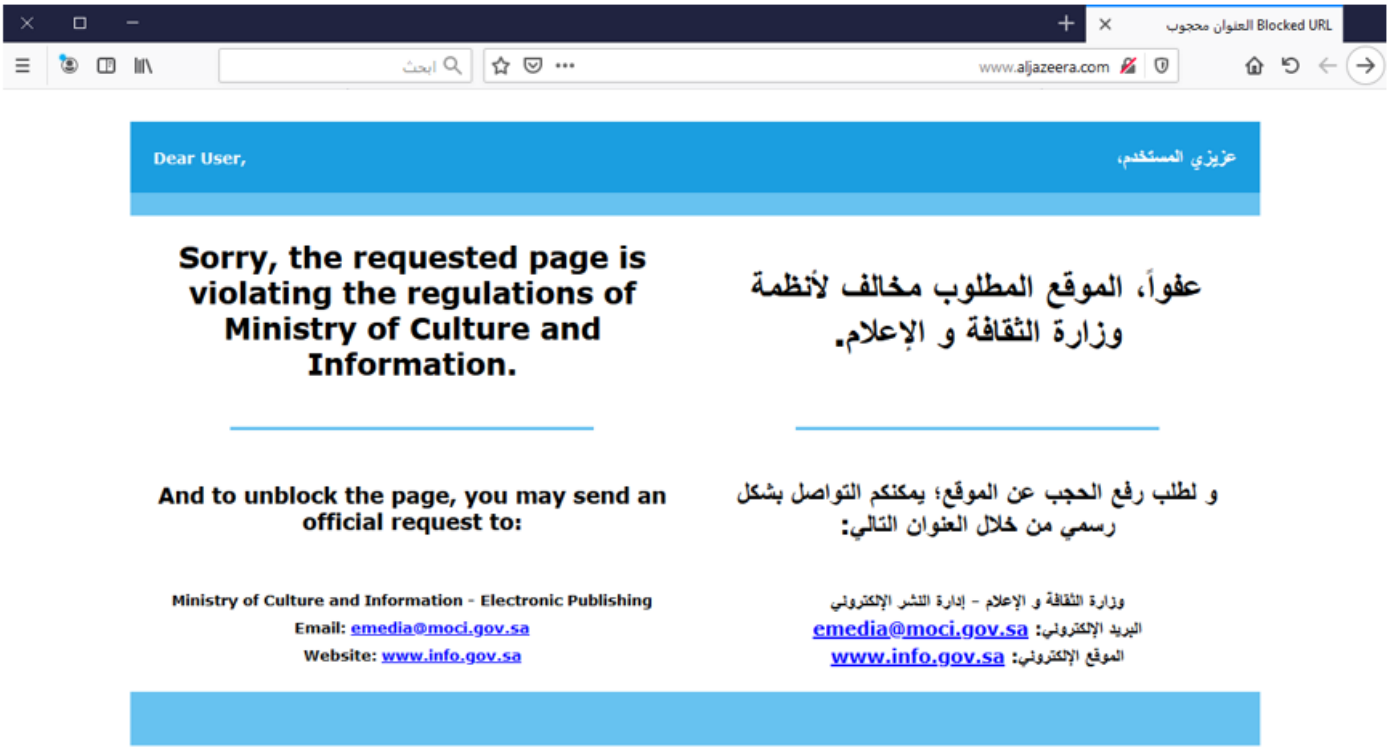


Figure 4

Filtering warning page by the Ministry of Culture and Information

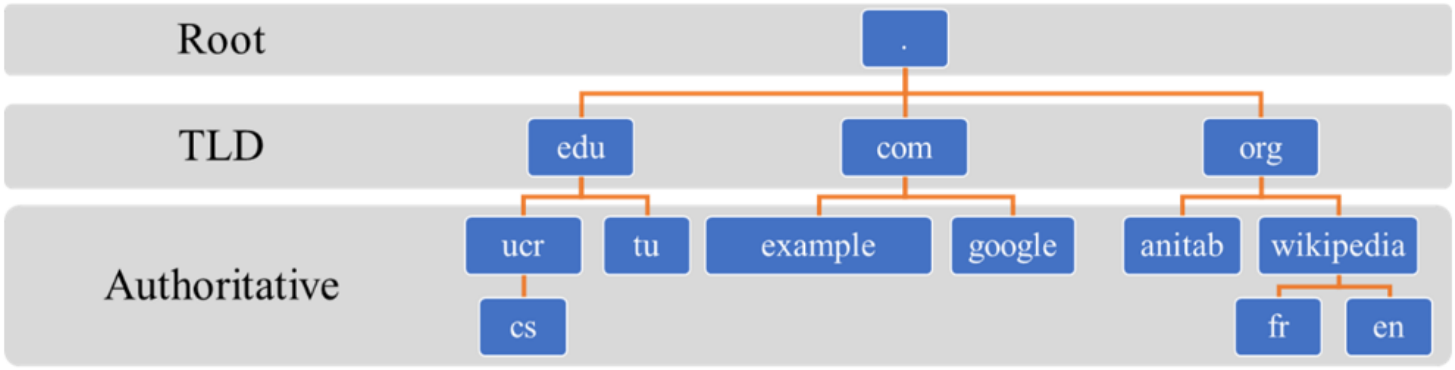
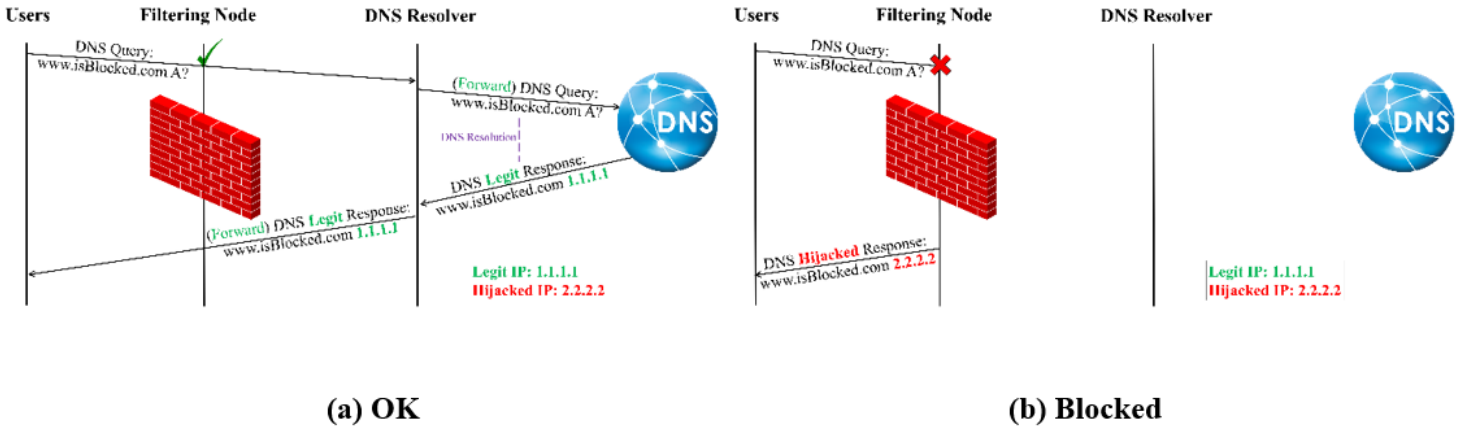


Figure 5

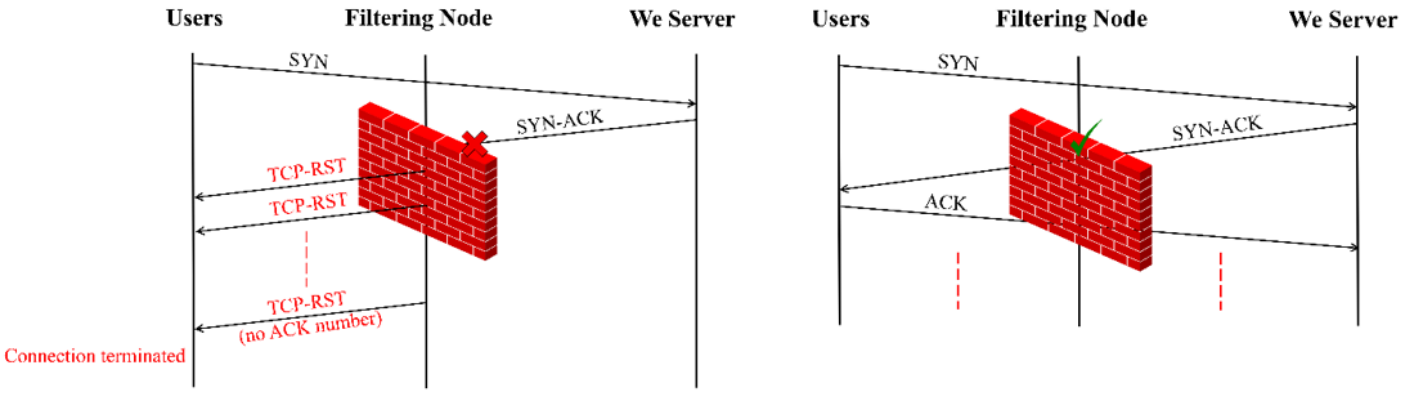
Hierarchy of DNS name servers



(a) OK (b) Blocked

Figure 6

DNS-Level Blocking



(a) OK (b) Blocked

Figure 7

IP Address Based Blocking

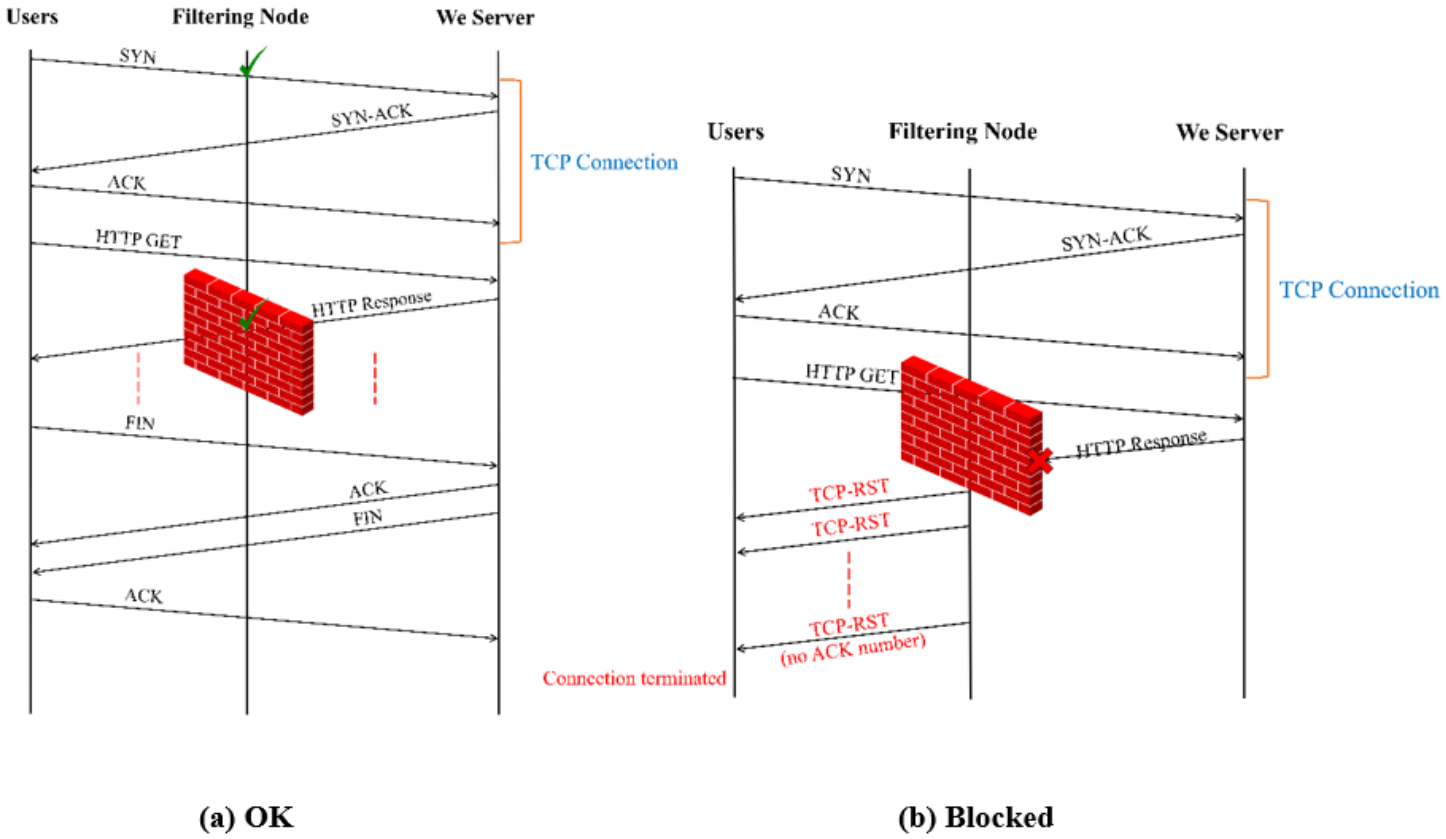


Figure 8

HTTP Filtering

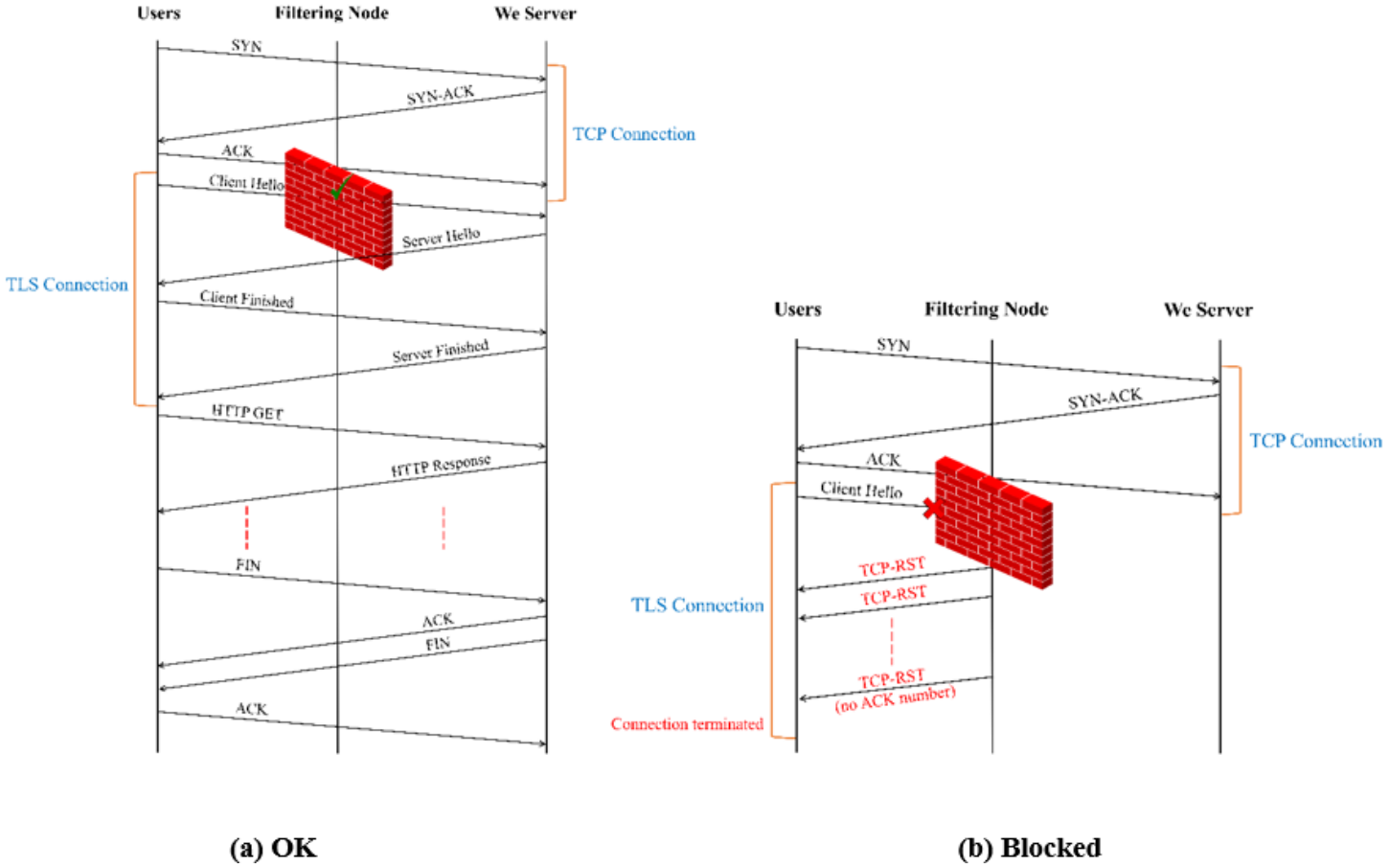


Figure 9

TLS Filtering

Figure 10

Geolocation of the Vantage Points

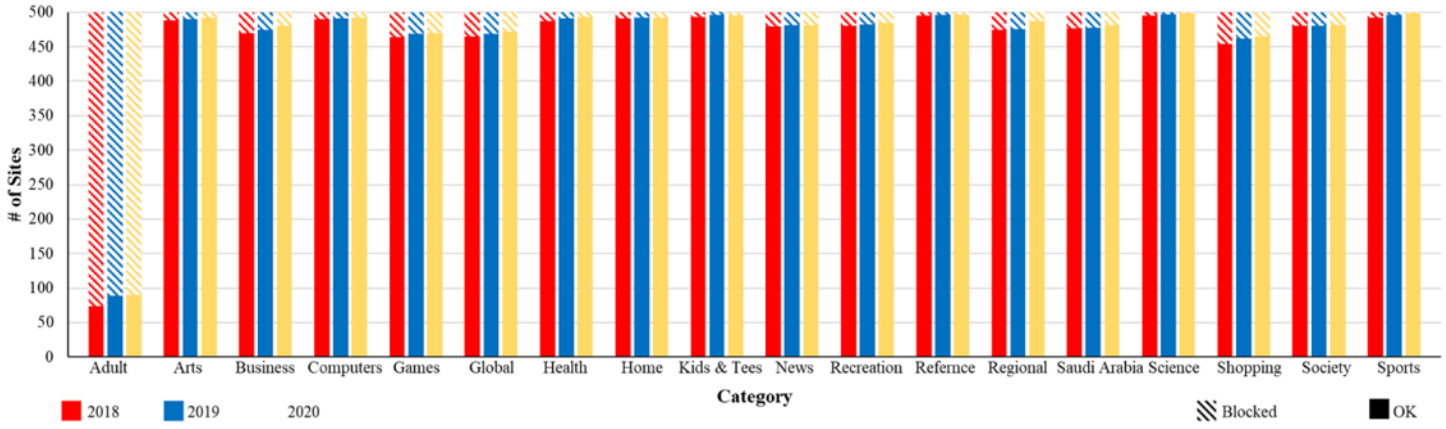
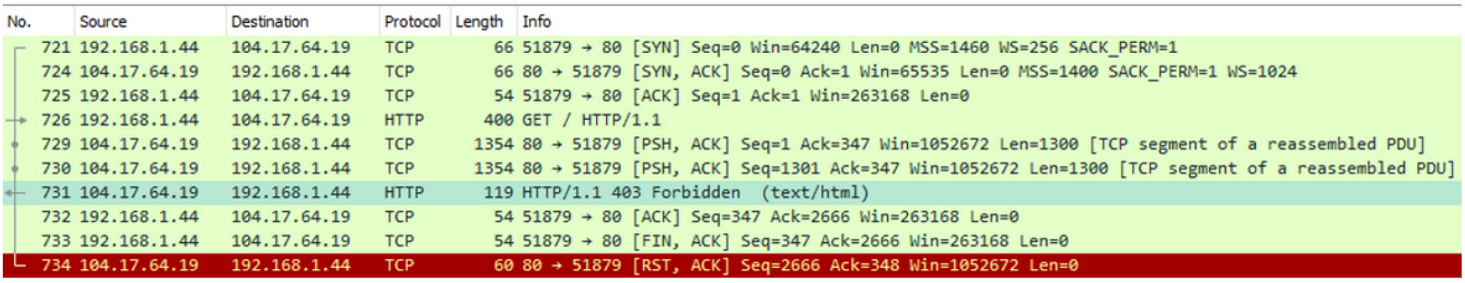


Figure 11

The scope of Internet filtering in Saudi Arabia



No.	Source	Destination	Protocol	Length	Info
721	192.168.1.44	104.17.64.19	TCP	66	51879 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
724	104.17.64.19	192.168.1.44	TCP	66	80 → 51879 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
725	192.168.1.44	104.17.64.19	TCP	54	51879 → 80 [ACK] Seq=1 Ack=1 Win=263168 Len=0
726	192.168.1.44	104.17.64.19	HTTP	400	GET / HTTP/1.1
729	104.17.64.19	192.168.1.44	TCP	1354	80 → 51879 [PSH, ACK] Seq=1 Ack=347 Win=1052672 Len=1300 [TCP segment of a reassembled PDU]
730	104.17.64.19	192.168.1.44	TCP	1354	80 → 51879 [PSH, ACK] Seq=1301 Ack=347 Win=1052672 Len=1300 [TCP segment of a reassembled PDU]
731	104.17.64.19	192.168.1.44	HTTP	119	HTTP/1.1 403 Forbidden (text/html)
732	192.168.1.44	104.17.64.19	TCP	54	51879 → 80 [ACK] Seq=347 Ack=2666 Win=263168 Len=0
733	192.168.1.44	104.17.64.19	TCP	54	51879 → 80 [FIN, ACK] Seq=347 Ack=2666 Win=263168 Len=0
734	104.17.64.19	192.168.1.44	TCP	60	80 → 51879 [RST, ACK] Seq=2666 Ack=348 Win=1052672 Len=0

Figure 12

Wireshark trace of HTTP-URL-Keyword filtering

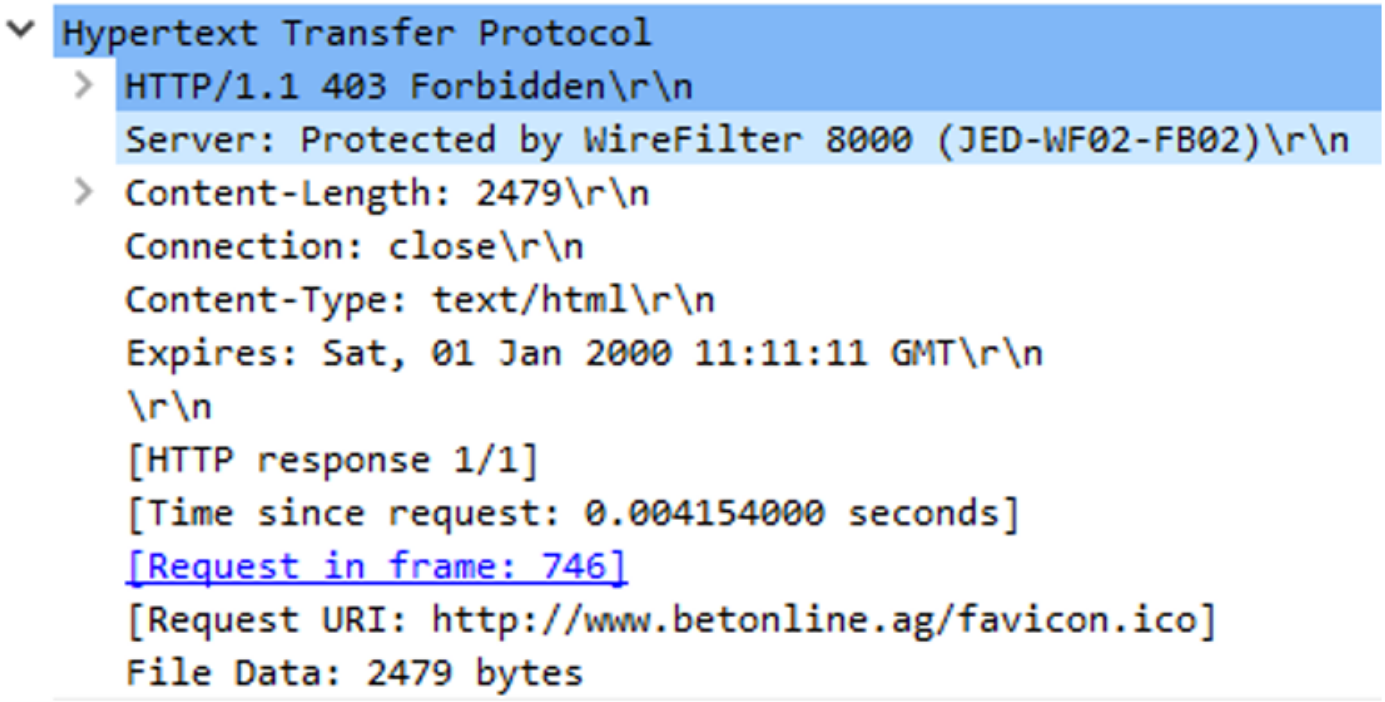
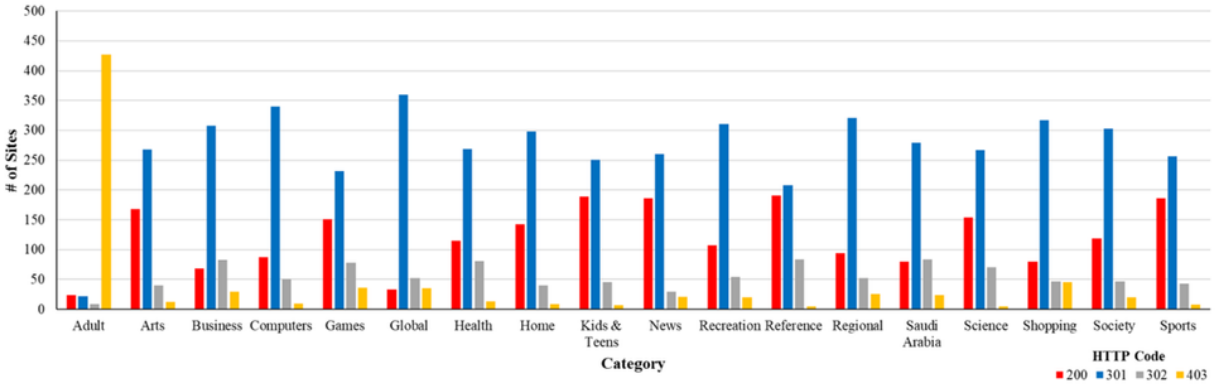
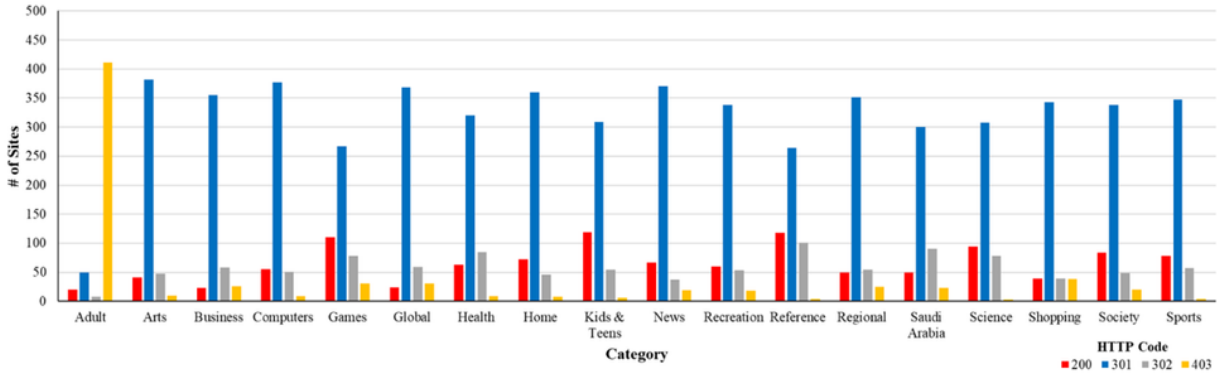


Figure 13

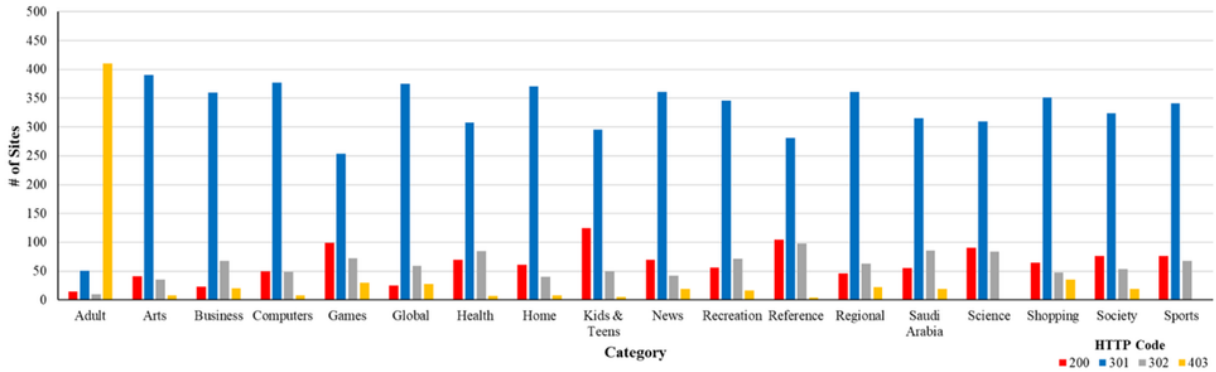
Wireshark trace showing the company in charge of filtering in Saudi Arabia: WireFilter



(a)



(b)



(c)

Figure 14

HTTP filtering results by returned status code. The HTTP 200 OK success status response code indicates that the request has succeeded. The 301 and 302 Found status codes are used to indicate that the URL has been permanently and temporally, respectively, moved/redirected to a new URL. Code 403 indicates that access to the requested URL is forbidden due to client-related issues; in our case the reason is filtering).

No.	Source	Destination	Protocol	Length	Info
275	192.168.1.44	104.17.64.19	TCP	66	51889 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
279	104.17.64.19	192.168.1.44	TCP	66	443 → 51889 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM=1 WS=1024
280	192.168.1.44	104.17.64.19	TCP	54	51889 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
281	192.168.1.44	104.17.64.19	TLSv1	571	Client Hello
282	104.17.64.19	192.168.1.44	TCP	60	443 → 51889 [RST, ACK] Seq=1 Ack=2 Win=1052672 Len=0

Figure 15

Wireshark trace of TLS filtering

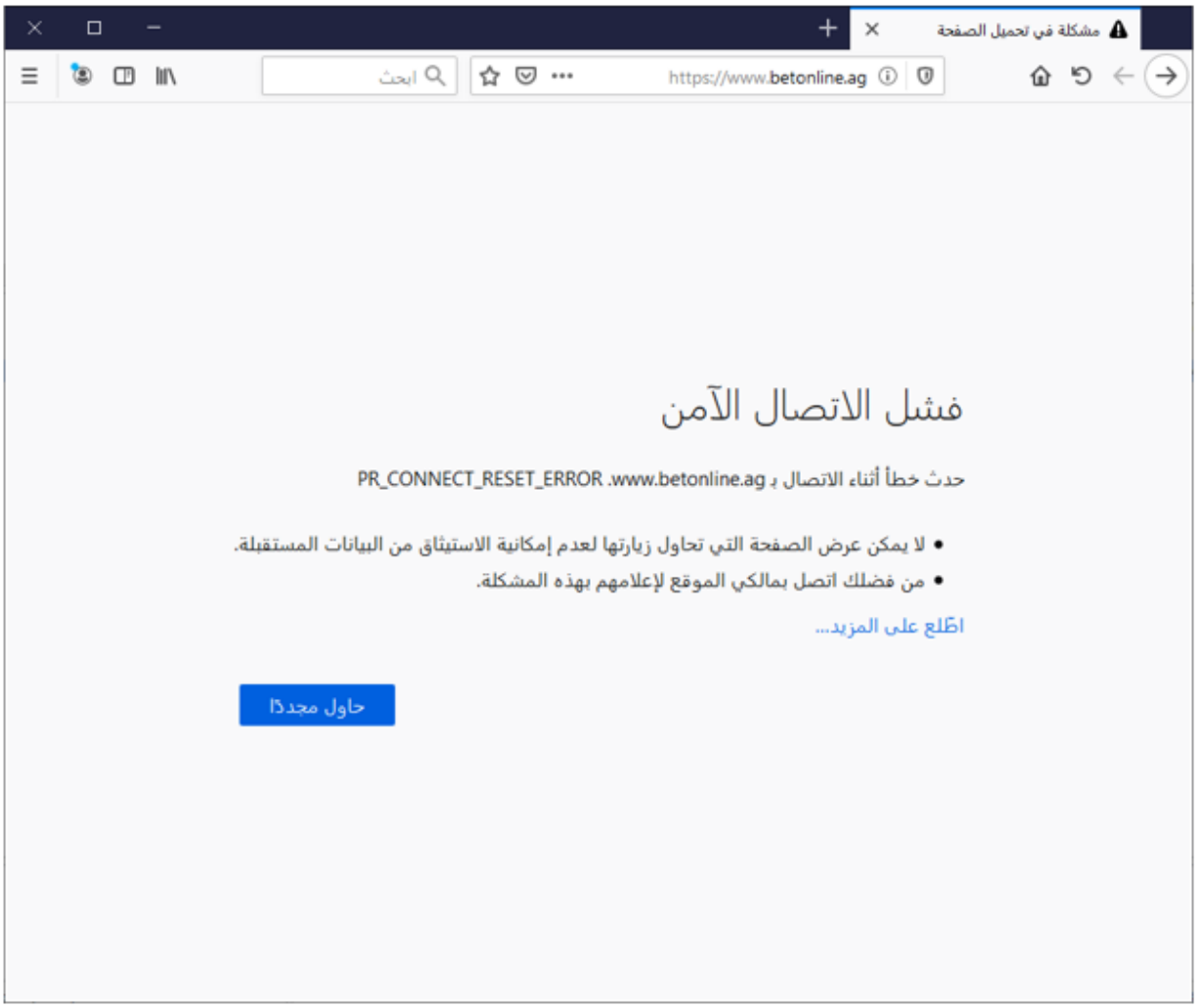


Figure 16

TLS/HTTPS connection cannot be established for a blocked site

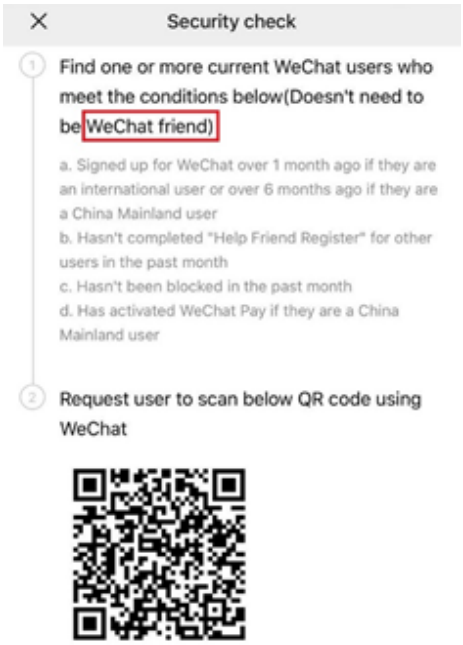


Figure 17

WeChat Security Check

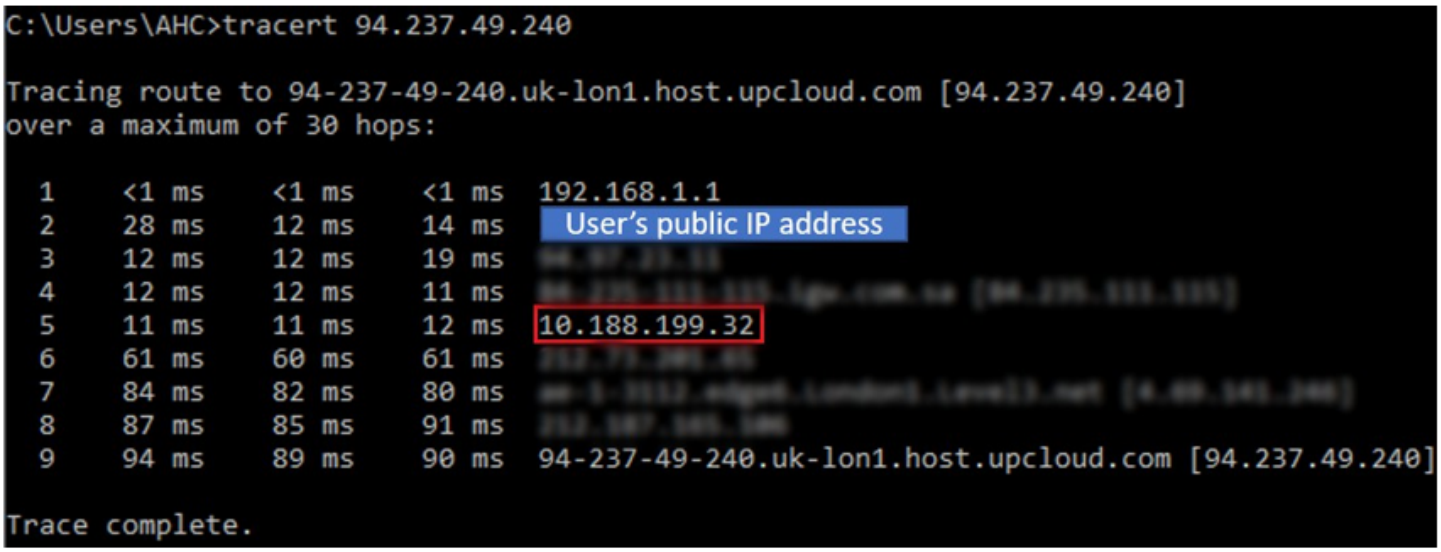


Figure 18

Output of tracert between a machine in Saudi Arabia and a machine in UK

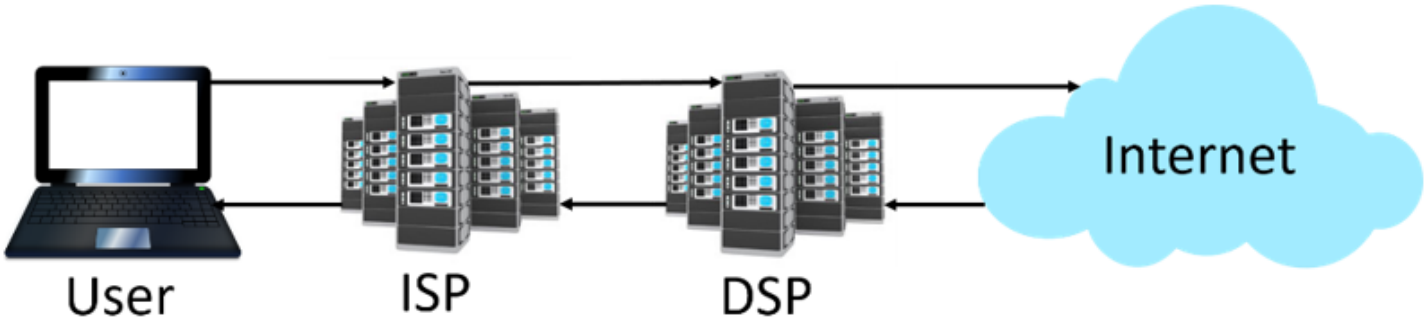


Figure 19

The infrastructure of the filtering system in Saudi Arabia