

THE STATE OF IRANIAN COMMUNICATION

Manipulation and Circumvention

MORGAN SENNHAUSER

Project Coordinator, NedaNet

JULY 13, 2009

CONTENTS

PURPOSE	2
HISTORY	3
TRAFFIC MANIPULATION	4
OVERVIEW _____	5
MONITORING _____	6
<i>Internet</i>	6
<i>SMS</i>	7
<i>Telephone</i>	7
IP BLOCKING _____	8
<i>What Gets Blocked</i>	9
BANDWIDTH THROTTLING _____	11
KEYWORD FILTRATION _____	13
TRAFFIC CLASSIFICATION _____	14
<i>QoS Services</i>	14
SHALLOW PACKET INSPECTION _____	15
<i>SSL</i>	15
FINGERPRINT PACKET INSPECTION _____	16
DEEP PACKET INSPECTION _____	17
WHAT ELSE IS POSSIBLE _____	18
<i>Automation</i>	18
<i>Expansion</i>	18
<i>Invisibility</i>	19
SUMMARY _____	20
RESPONSE	21

DETERMINING SUCCESSFUL RESPONSES	22
<i>How resilient is it to countermeasures?</i>	22
<i>How secure is it?</i>	22
<i>How expensive is it to run?</i>	22
<i>Is it traceable?</i>	23
<i>How easily can it be deployed?</i>	23
<i>Would It Operate Securely With Full Disclosure?</i>	24
<i>How easy is it to use?</i>	24
<i>Has it been tested thoroughly?</i>	24
NORMAL USAGE	25
<i>Single-Hop Proxies</i>	25
<i>Multi-Hop Circuits</i>	26
<i>Summary</i>	27
SPECIAL USAGE	28
<i>Peer-to-Peer</i>	28
SUMMARY	29
CONCLUSION	30
WORKS CITED	31

PURPOSE

This document is an overview of the current state of communications in Iran, as well as a rundown of the recommended methods for circumvention.

As this document is intended for non-technical readers, I hope to provide a clear yet thorough picture of the Iranian data manipulation system as well as suggested circumvention methods. For the more technical among us (our programmers and developers), I hope to stimulate development in the proper direction by showing what methods have already failed to work and what methods may work.

I also hope to dispel some of the rumors about the Iranian filtration system and clarify which circumvention methods are predicted to work and which may not.

Finally, some information about Iran's data manipulation may be left intentionally vague. This is to prevent the Iranian government from discovering we know more about their monitoring and manipulation than they think we do. Additionally, I do not cite many sources, as doing so would reveal how we obtained the information, and therefore make it much more difficult to continue to do so.

An additional note: This document is not intended to be a detailed analysis of the Iranian firewall, so some parts may be worded in ways which may not be technically correct, but get the point across much more clearly than a more technically correct sentence would. That said, if you find something which is simply incorrect, please inform me.

HISTORY

After the Iranian presidential election on June 12th, the Iranian government began to limit civilians' basic freedoms in strict and unjustifiable ways, due to allegations of election fraud. The government prevented protests by using teargas, batons, and eventually automatic weapons. They limited phone communications, preventing people from communicating with friends and family. They also began limiting the Internet inside Iran.

However, there were several sites that were not blocked which enabled the Iranians to share photographs, video, and thoughts about the election, and the subsequent violence against protesters. The most notable site for the torrent of information coming out of Iran was Twitter, where content tags like #iranelection and #gr88 (Green Revolution 1388, the current year on the Islamic calendar) took control of the most used tags for over two weeks. (Nolte, 2009)

This enabled millions of people to see and read about what was happening in Iran. And as they watched footage of protesters being beaten, and became far too familiar with the concept of Basij militia arresting people in the middle of the night, they wondered what they could do.

Initially, assisting was easy. One could follow simple instructions to set up a proxy and send the IP and port of the proxy server to one of several volunteers who would then spread the connection details into Iran. Unfortunately, most proxies were quickly blocked, which meant that it took a constant rush of people setting up proxies on thousands of computers to keep communication even somewhat open.

Obviously, this pace could not be continued indefinitely, and it was becoming clear that this was going to be a long struggle for the Iranian people. Worse, rumors were circulating that the Iranian government was enabling previously unused hardware, which made the majority of proxies obsolete.

Some examination proved these rumors to be true. The Iranians had moved beyond simple IP blocking to much more thorough methods of data manipulation- things that would also prove much more difficult to circumvent.

TRAFFIC MANIPULATION

Traffic manipulation, in terms of computer networking, is any tampering done to information in transit from its origin to its destination. The most well known case of traffic manipulation is the Great Firewall of China (Golden Shield Project), the complex system of measures used to filter the information that Chinese citizens can access online. (Stilgherrian, 2008) However, many other nations and entities have instituted some form of traffic manipulation. For example, many companies block the IPs¹ of servers their employees do not need to access during work hours, such as eBay.

There are many types of traffic manipulation, however, and they all pose different problems to those who wish to work around them. The next few sections summarize and show examples of the methods used to impose communication restrictions in Iran.

¹ IP address: a computer's address on the Internet, this is typically how other machines will refer to a computer online.

OVERVIEW

The Iranian firewall² is a much more complex system than is commonly observed at a national level. For example, in China, the firewall is simply IP blocking and some keyword dropping. (Stilgherrian, 2008) In Myanmar, they solved their communications issues by disconnecting the entire Internet. (Drash, 2007)

The Iranians, however, had to take a middle ground. A simple firewall wouldn't work, there was too much public attention on getting around it, and too many people inside desperate to get information out. Cutting off the Internet completely wouldn't work, as there are businesses within Iran that would fail if their lines of communication were cut off; the most prominent of these is the oil industry.

Therefore, the methods which they had to employ had to be more thorough than IP blocking and keyword filtering, without debilitating the economy. They decided on a multi-level system that used several redundant systems, and is astonishingly good at manipulating the data flow from and to Iran.

² Firewall: a system in place on a network used to block select traffic

MONITORING

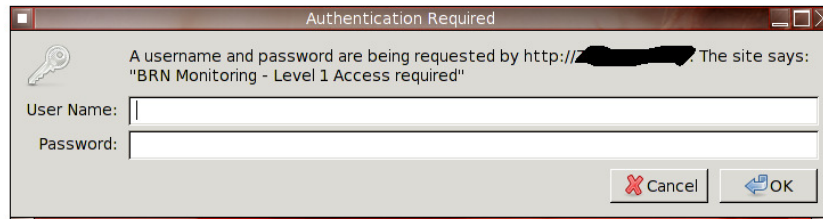


Figure 1 BRN Monitoring (NedaNet, 2009)

Before examining the types of traffic manipulation in place, I feel it is important to discuss the Iranian government's practices of information monitoring. It is not always necessary to change or block the flow of information; sometimes it is enough to gather information. This is commonly referred to as *wiretapping*, because it is essentially putting a tap in the middle of the communication, and listening to what is being transmitted.

The Iranian government had been monitoring most international communication well before the election. The most commonly acknowledged form of monitoring is that done by the Iranian post office. However, there are other examples:

INTERNET

Iranian Internet traffic is superficially scanned for certain keywords. However there is no confirmation about what is done with the information obtained, nor are we entirely sure how thorough the traffic monitors are. It requires a great deal of manpower to thoroughly monitor communications, and it is unknown if the Iranian government has invested the required effort. Note that a lot of what is commonly referred to as Internet monitoring is actually manipulation, and is therefore covered in a different section.

There are some concerns that the Iranian government may be monitoring not just traffic, but users too. They may be using hardware to find strong wireless signals, and locate people that way. This is unconfirmed, but plausible.

SMS

The monitoring of SMS³ by the Iranian government has recently gotten a lot of attention. It is believed that this monitoring, combined with location tracking, has been used to arrest people who were sharing information about protests after the election. Additionally, the entire SMS system has been shut down and brought back several times since the elections, so even if it were secure to use, it would not be very reliable. (Kanalley, 2009) (Ghulam News, 2009) (Wire News Sources, 2009)

TELEPHONE

The land line⁴ phones of Iran, like those in almost every other country, are capable of being monitored, and therefore most likely are. It is not recommended that any Iranian use their telephones for any purpose.

Cell phones are probably also monitored. There are also some unconfirmed reports of the Iranian militia tracking protesters' physical location by their cell phones. We have no evidence, but it is highly likely.

³ SMS: Simple messaging system, also known as cellular text messaging

⁴ Land line: Also known as stationary phones, these are wired into buildings, and are not mobile

IP BLOCKING

The first method of traffic manipulation which the Iranian government employed was relatively simple. They dropped (stopped transmitting) any packets that were going to or coming from a flagged IP address. For example, the domain www.bbcpersian.com (IP address: 212.58.253.68) was blocked shortly after the election results were announced. Any traffic going to or from that IP would be ignored; it would appear to both sides as if the other did not exist. This is useful in blocking entire servers, such as websites that go against the Iranian government's doctrine, or computers acting as proxies.

emsenn.com to facebook.com

```
PING www.facebook.com (69.63.184.142) 56(84) bytes of data.  
64 bytes from www-10-03-ash1.facebook.com (69.63.814.142): icmp_seq=1 time=32.9  
64 bytes from www-10-03-ash1.facebook.com (69.63.814.142): icmp_seq=2 time=39.8  
64 bytes from www-10-03-ash1.facebook.com (69.63.814.142): icmp_seq=3 time=39.0  
64 bytes from www-10-03-ash1.facebook.com (69.63.814.142): icmp_seq=4 time=34.5  
--- www.facebook.com ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
Rtt min/avg/max/mdev = 32.975/36.606/39.830/2.906
```

Iranian server to facebook.com

```
Iranian server:  
PING www.facebook.ccom (69.63.184.142) 56(84) bytes of data.  
--- www.facebook.com ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 3002ms
```

Figure 2: Ping of Facebook from Ohio and Iran (NedaNet, 2009)

The above is a pinging of the main Facebook server, www.facebook.com (IP address: 69.63.184.142), from my main server and a computer in Iran. As you can see, the ping from my server is successful and I receive a response from Facebook's server. This shows that the server is functional and able to communicate in both directions with my machine.

However, the machine in Iran sees no response from the Facebook servers. To a computer inside Iran, it would appear that the Facebook server is nonoperational.

What is odd is that when this ping was done, the domain name www.facebook.com still resolved to its IP address, 69.63.184.142. This is unusual because they could have also blocked the domain name from resolving, preventing any knowledge of the Facebook server from being obtained.

WHAT GETS BLOCKED

It's usually fairly hard to determine what will be blocked and what won't be, though there are a few broad categories that usually get blocked. In addition, servers that are blocked are sometimes unblocked a few days later, only to be promptly blocked again. Currently the reason for this sporadic unblocking is unknown. Additionally, sites that you would think would be blocked are not, while those you sites that you wouldn't think of are.

BITTORRENT

BitTorrent filesharing, while peer-to-peer, relies on centralized servers to connect the peers. At a minimum, at least one linkage of peers must be made by the tracker, although from there the peers can connect by peer exchange. (One person sharing all his peers' IPs with all other peers he is connected to). For this reason, many BitTorrent trackers have been blocked to prevent the sharing of information through this medium.

NEWS

Many foreign news agencies' websites have been blocked. The stated reason for this is to prevent the Iranian people from being influenced by the Western media - which is, in some ways, correct. However due to the lack of impartiality and truthfulness from their own (government-operated) news outlets, the Iranian people were most likely not looking to be influenced, but merely learn what was happening in their own country.

Additionally, they have been blocking Iranian news outlets that expressed moderate views, claiming that the moderate media was trying to corrupt the sanctity of the Islamic Republic.

BLOGS

Many blogs have been blocked by the Iranian firewall, mostly because they were sharing video, photographs, or opinions on the protests. This was, in the eyes of the Iranian government, not a good thing, as they were trying to prevent any knowledge of the protests from spreading, especially within their borders. The fact that many blogs were blocked also greatly diminished how much of the international support the Iranian

people were able to see. Finally, blogs were blocked because many of them were sued to mirror tools which could be used to circumvent the firewall.

POLITICAL OPPOSITION

Those in Iranian politics who take a much more moderate stance than the incumbent leaders are also liable to be blocked within Iran. Due to previous harassments, many opposition leaders' webservers are hosted outside of Iran. However that does not prevent them from being filtered.

CIRCUMVENTION TOOLS

Websites which explain how to circumvent the Iranian firewall are frequently blocked, making it much more difficult to get these tools into Iran. However, many other people have set up mirrors of the files and instructions, so blocking these tools has proved ineffective.

PROXY SERVERS

Perhaps most rapidly, proxy servers are constantly being blocked by the Iranian firewall, as they provide a direct (if usually insecure) link to the outside world. Due to the speed with which they are being blocked, among other reasons, they are not currently recommended for use in Iran.

BANDWIDTH THROTTLING

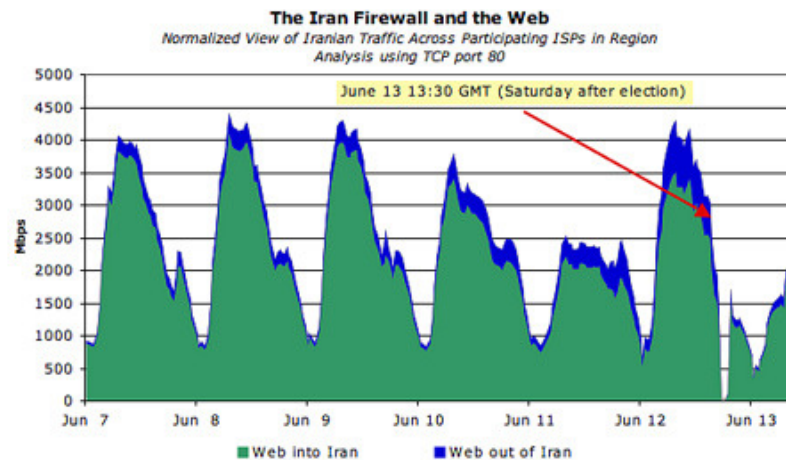


Figure 3: Iranian national bandwidth, election week (Labovitz, 2009)

In addition to monitoring, there have also been strict limits on the amount of available bandwidth in Iran since the election. This limit is most likely artificially imposed as it limits the amount of traffic that must be monitored and manipulated. With less than normal traffic, the load on the manipulation servers is much lower. This enables the Iranian government to devote much greater attention to every piece of information they receive, resulting in much more thorough analysis; this in turn increases the risk to dissidents within Iran, and means that our countermeasures must be much more thorough. Unlike the Golden Shield Project in China, where the system is well established and also much less resource intensive due to the light nature of inspection, the Iranian firewall is very thorough and would be unable to function if the Iranian Internet were at full capacity (an estimated six gigabytes a second).

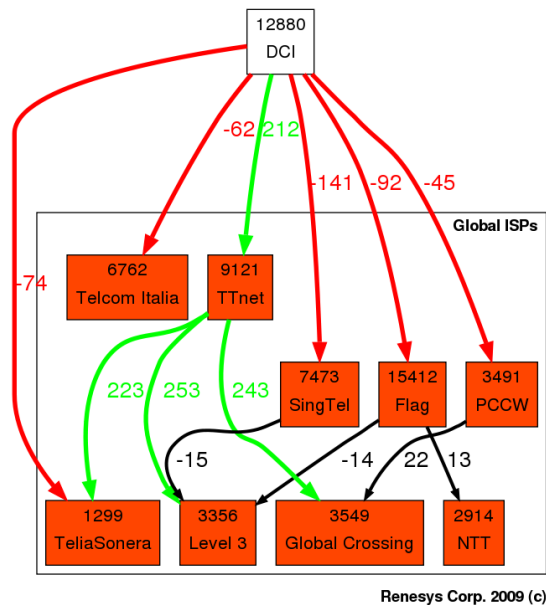


Figure 4: Traffic changes from Iran to international ISPs (Cowie, 2009)

The image above is an examination in the decrease or increase of traffic that the international Internet service providers who operate in Iran saw in the days after the election. The six providers are:

- TTNNet (Turk Telecom)
- FLAG
- SingTel (Singapore telecom)
- PCCW
- Telia Sonera
- Telecom Italia

On the chart above, the red lines represent traffic lost, while green represents traffic gained (and black represents minor changes.) What is unusual about the traffic flow is that while traffic to almost every other ISP lessened, TTNNet and its subsequent connections saw a tremendous increase in traffic. While the exact reason for this is unknown, it can be speculated that the traffic manipulation system installed on Turk Telecom’s connection is more sophisticated and most likely larger, meaning it could monitor a greater volume of traffic more successfully than the other providers.

KEYWORD FILTRATION

This is also another fairly simple type of filtration where the government drops any packets featuring certain keywords, such as *protest*, *proxy*, or *mousavi*. There are also rumors circulating that they block any information that transmits IP and ports in their standard form (such as *4.2.2.1:1338*) is also blocked.

Although Yahoo! Instant Messenger is now blocked, it was functional prior to the election, although there were keyword restrictions of the type above imposed on it. In addition, messages containing standard formed urls (such as <http://www.google.com>) were blocked, though it was easy to circumvent by manipulating the text (such as *www///google///com*). Keyword filtration is still in use to some extent, but it is mostly inactive due to the high resource intensity and low effectiveness in stopping traffic. That said, keyword *monitoring* is still in effect; this is a simple way to flag dissidents.

TRAFFIC CLASSIFICATION

Traffic classification, also referred to as Quality of Service control (QoS) is the filtration and manipulation of information based by the transfer protocol⁵ and port⁶ it is transmitted on. For example, website (HTTP) traffic is typically run over the TCP protocol, on port 80. If one wished to slow down almost all website browsing. This can be employed to manipulate the protocols that dissidents are most likely used to view and receive information the Iranian government would rather they not. It would also appear that the degree to which they throttle traffic by QoS varies based on the time and day of the week. This is most likely to prevent too heavy of restrictions on normal business operations. However, it has been shown that businesses in Iran don't rely heavily on the Internet, so there may be another, unknown reason, for why they have set up QoS scheduling.

QOSED SERVICES

The following is a list of the services we believe to have been manipulated based on port and protocol.

HTTPS

HTTPS (HTTP with encryption) is believed to have been throttled using QoS in Iran. The suspected reason for this is that many web-based email providers require HTTPS to log in. Therefore, by throttling HTTPS, Iranian access to email has been limited

SSH

SSH, or Secure Shell, is commonly used to remotely access computers. Additionally, it can be used to "tunnel" a connection through. For both of these reasons, it is heavily throttled in Iran.

⁵ Protocol: standard by which information is transmitted

⁶ Port: the defining endpoint of a connection, which is tied to a specific server and protocol

SHALLOW PACKET INSPECTION

Stateful packet inspection, also referred to as shallow packet inspection, is the lightest type of packet inspection. It is the examination of the header information of a packet; the information that identifies what type of information the packet contains. The header of a packet usually contains a few things, most importantly (for purposes of traffic manipulation) the protocol, options, and packet length. These values can be used to determine the alleged contents of a packet without much more inspection than QoS controls require, making them more efficient than heavier inspection while more thorough than QoS. This is currently the most widely used type of packet inspection in the Iran.

SSL

SSL⁷ is the most notable type of traffic to be throttled and manipulated by this level of packet inspection. It does not matter what port SSL traffic is transmitted on, it will be manipulated and shaped anyway. This has heavily hurt the ability of many individuals and organizations to access the Internet in their favorite secure methods (such as HTTPS).

⁷ An transfer protocol which provides encrypted communication.

FINGERPRINT PACKET INSPECTION

Fingerprint packet inspection is the examination of how a packet is formed. Based on the packet length, and several other identifying features of a packet (ignoring the headers, which can be intentionally misleading) it is possible to determine what type of information a packet holds, still without having to deeply examine the packet. This is a fairly resource-intensive form of packet identification, and therefore isn't widely used at this time. It is believed that this is the type of packet inspection the Iranian government wishes to nationally expand, due to its balance between resource usage and depth of examination.

DEEP PACKET INSPECTION

True deep packet inspection is the thorough examination of a packet's contents. This can be used to figure out more information about a packet than would be known by other filtering. Even if the contents are encrypted, it is possible to tell what type, generally, of information a packet contains. Combining this knowledge with the information gathered by fingerprinting and header inspection, it is possible to manipulate almost all known forms of Internet traffic.

Currently their ability to implement deep packet inspection is unknown, but is suspected to be minimal. There is simply too much burden on the chokepoints to implement widespread packet inspection. However, the situation may change which would greatly allow the Iranian firewall to expand their deep packet inspection.

WHAT ELSE IS POSSIBLE

We now have a decent grasp of the types of filtration employed in Iran at this point. In order to start working on a viable and long-term solution, we have to examine where things are going next. There are three major ways in which the Iranian firewall can be expanded beyond its current level.

AUTOMATION

The process of automating the traffic filtration and manipulation is a long one; it requires a lot of tinkering to be done properly. Automatically tagging traffic, however, reduces the human labor required to operate the firewall. The automation will not be dramatically noticeable at any single point, but will be a constantly increasing measure.

In addition to the process of automating much of the filtration, they are also working on managing the ISP level filtration at a central control center as much as possible, which will speed the development of automation.

EXPANSION

There are a few ways which the Iranian firewall is going to be expanded, listed in the predicted order that they will be focused on:

- **Migration.** The Iranian government is currently expected to move some of their filtration methods to the ISP level, from their current position at the international chokepoints. This is to reduce the burden on these chokepoints, enabling them to more thoroughly inspect the information they see. There are some concerns among the Iranian government that this filtration will put too much control in the hands of the ISPs. The fear is that intentional or accidental misconfiguration may allow some traffic through which they feel shouldn't be. This is more reason why they are pushing for a national control center, as well.
- **Labor.** The amount of employees dedicated to Iranian network control is expected to grow as the Iranian firewall becomes more a permanent feature of the Iranian general infrastructure. What level and the role of these employees is currently unknown, as is how many they will be hiring.
- **Hardware.** The amount of processing power the Iranian government has now is restrictive to the level of traffic manipulation they can implement. Additionally, the lack of control they have over the ISP

connections is detrimental to thorough traffic routing. If they are able to purchase new hardware, it would eliminate both these issues, assuming they have the operators to manage the equipment.

INVISIBILITY

Any solution which is able to be implemented without detection is an ideal solution. You cannot circumvent something if you are unaware of the circumvention taking place. However, due to the scale and aggressiveness of the Iranian firewall, any successful solution will mostly likely be visible.

SUMMARY

There is a very sophisticated traffic manipulation system in Iran currently, and its complexity is growing. It is much more thorough than any other national firewall to date, presenting many challenges which have never existed before. In order to develop a long term solution to the Iranian firewall, it is vital we understand these developments and risks. In doing so, we can thoroughly and correctly prepare our responses to ensure that the communication lines of the Iranian people remain open.

RESPONSE

With all of those varied methods of traffic inspection possible, a single solution is not the correct response. There are methods we can work toward, but none are permanent, and even the longevity of a response is greatly variable. Therefore, it is best to not only consider and develop solutions for the current situation, but to predict where things are heading, and how to counteract the predicted changes.

DETERMINING SUCCESSFUL RESPONSES

There are a few questions which I ask of all proposed suggestions for circumventing the Iranian firewall.

Usually it works to weed out bad choices rather quickly; also, it helps see where existing products can be improved.

HOW RESILIENT IS IT TO COUNTERMEASURES?

Any tool must first be determined to be secure against being throttled by the methods already in place, as well as be somewhat resistant to new measures. This is not to say that a solution must be able to withstand targeted and long-term attacks to be considered viable; it must be able to withstand the collateral damage of general manipulation increases.

HOW SECURE IS IT?

Assuming that the traffic is not easily manipulated, how secure is the information being transmitted?

Unencrypted (plain) text is completely insecure. Anyone in the transmission path, from the origin to destination, can view the full contents of what you are transmitting. Obviously, encryption is necessary. The key to successful encryption is improving on the system's weakest point. In networking, this is most often the key exchange. Prior to setting up the encrypted transmission, the two clients must agree on the specific key used to encrypt the text. This is where many encryptions fail, allowing man-in-the-middle attacks (a person in the middle of the origin-destination line, who can pretend to be the destination and decrypt the traffic, view it, re-encrypt it, and pass it on to the true destination.)

HOW EXPENSIVE IS IT TO RUN?

Servers are expensive to operate. The monetary cost involved in any planned long-term measure should be carefully considered. Depending on the level of usage, costs could range anywhere from less than a hundred dollars a month to tens of thousands of dollars a week. These costs could prove prohibitive, which is why I tend to stay away from solutions requiring dedicated servers.

IS IT TRACEABLE?

If the information being transmitted is tracked to the person using it, that is evidence against them. The activities which a solution are used for should not imply guilt. If a solution is used only to view illegal materials, than anyone using that tool can be assumed to be viewing illegal materials. Therefore, solutions which have a dedicated use of helping dissidents, and a detectable fingerprint are not suggested as long term solutions, since they may allow them to operate, yet use the fact that they are being used against the users. The examples of programs which might be treated this way are FreeGate, UltraSurf, and Haystack (among others, those are the three most well-known.)

HOW EASILY CAN IT BE DEPLOYED?

Many solutions require a lot of personal communication between the distributor and the recipient. The most ready example is the long route of communication from someone who set up a proxy server (Donor) to someone who needs it (Iranian):

1. Donor creates proxy
2. Donor gives credentials to Facilitator
3. Iranian asks Facilitator for a proxy
4. Facilitator gives Iranian a proxy

There is an unsustainable amount of cooperation between Donor and Facilitator, and Facilitator and Iranian. Additionally, if the Facilitator is unable to complete the duties they have volunteered for, the system will

fall apart. Generally the more coordination required for distribution, the less reliable the growth of a product can be.

WOULD IT OPERATE SECURELY WITH FULL DISCLOSURE?

This is not a black and white determining factor, but does help to determine a product's estimated lifetime. It can be assumed that, eventually, a product will be cracked. The variables that determine the speed it takes are many, but it is usually a fairly quick process. Then there is the delay of reorganizing traffic manipulation to catch the new circumvention tool. Of course, the tool may not be throttled if it is broken; it may be allowed to operate without manipulation in order to allow continued monitoring. It is for this reason that the transmissions not only be difficult to detect, but secure even after they have been detected.

HOW EASY IS IT TO USE?

While many of the people developing and testing tools to be employed in opening Iranian communication, the users (the Iranian people) may not be. Therefore, it is important that the burden placed on the client is relatively low.

HAS IT BEEN TESTED THOROUGHLY?

Any solution intended to last must be aggressively attacked and put through simulations based on the knowledge we have of the Iranian firewall. This helps to ensure that a product will be able to survive the current levels of filters, even if it is discovered.

NORMAL USAGE

This is a rundown of all the tools that allow a general connection to the Internet. These do not restrict the types of connections which can be used, meaning they are for all purposes.

SINGLE-HOP PROXIES

A single-hop proxy is one which has a single intermediary connection between the origin and true destination. This enables them to be faster (usually) than multiple-hop proxies, at the cost of a great deal of security.

HTTP

HTTP proxies are proven to be ineffective against the Iranian firewall at this time. Before explaining how they don't work, their operations should be explained, briefly.

1. Client connects to Proxy
2. Proxy forwards traffic between Client and Destination

The problem is that all parts of this are blatantly marked as being proxy traffic. The initial connection is broadcast in plain text, and easily identifiable. From then on, all traffic between the proxy and client is also plaintext, meaning that it can be intercepted and manipulated in all ways that are possible if no proxy were used. Note that in the beginning, when only IP blocking was employed, this was not the case, so with the extent of the firewall at that time, HTTP proxies were good enough.

FREEGATE

FreeGate works by allowing a client to connect to the DynaWeb service, which is a closed system of proxies created by Dynamic Internet Technologies (DIT). (Dynamic Internet Technology) Currently, not too much is known about the inner workings of FreeGate, although there are some beliefs that as the Iranian firewall expands, FreeGate may not be able to remain operational.

PSIPHON

Psiphon works as a sort of HTTPS proxy, although instead of being publicly accessible, it requires the Donor getting the account credentials to Iranian. This increases the resource intensity of the product for mass distribution. Additionally, all Psiphon servers log the clients' activities, reducing the security of the communication. Furthermore, due to the fact that SSL is highly throttled in Iran currently, that means that there is a high chance that Psiphon traffic is also manipulated. For this reason, it is believed that Psiphon is not a viable solution for mass distribution. However, if you have friends and family in Iran who want something a bit more useful than HTTP proxies, but have complaints about other solutions, it may work to temporarily keep them connected.

MULTI-HOP CIRCUITS

These are connections with two or more intermediate connections between the origin and the destination.

TOR

Tor is a multiple-node proxy which focuses not only on keeping the information secure, but the users' identities as well. It has a bit longer circuit than other multiple-node proxies, though they are special in the fact that they don't require dedicated servers. Any home user, business, or other organization can run a Tor relay, helping to speed up the Tor network.

While Tor is secure, it does have a few downsides. Most noticeably is the speed of the Tor network. It is very slow, which discourages Iranians from using it. There have also been complaints of Tor being difficult to install; however there is a Tor browser and IM bundle, which comes with an Internet browser and instant messaging client.

If you are willing to make the sacrifice of speed for the security granted by Tor, it is one of the recommended tools to get around the Iranian firewall.

HAYSTACK

Haystack is a circuit proxy developed by Austin Heap and Daniel Colascione, specifically to operate from within Iran. Due to concerns that information leaks may cause preemptive responses to the product, information is fairly scarce. However, there are some things that have been revealed. Haystack will be available to clients who run Windows, Mac, and Unix systems, and will work in a way similar to FreeGate (in what sense it is similar is not certain). (Heap, 2009)

While the Haystack developers are maintaining a great deal of secrecy around the specific workings of the product, there are some things we have confirmed from the developers about how it will work. It will be a multiple-node circuit type of proxy; additionally, it is an obfuscating proxy, though what that specifically means is unclear. (Colascione, 2009).

SUMMARY

While there are a great number of tools currently in place to allow Iranians to communicate on the Internet, there are concerns of security with all solutions, and all solutions are temporary. As the Iranian firewall evolves, so will our usage of these tools, to enable us to keep Iranians online and communicating openly.

SPECIAL USAGE

There are some tools that may be developed which are not intended to allow access to the entire Internet, but still allow people to communicate.

PEER-TO-PEER

Peer-to-peer connections are a type of connection in which two users communicate without the need of a centralized server. Almost everything on the Internet relies on client-server connections, though peer-to-peer is increasingly being used. It is a viable way for communication because it is incredibly hard to completely block and does not require a single server to stay in service for the duration of the conflict. Unfortunately, almost all peer-to-peer solutions require a network that is separate from the general Internet, meaning that they would not allow dissidents to access their favorite websites. Peer-to-peer connections are being emphasized due to the fact that Iranian to Iranian connections are not manipulated in any way.

FREENET

FreeNet allows the users to view (either in open or darknet methods) a completely peer-to-peer web. It has the benefit of being able to be a *darknet*, meaning no one who isn't trusted to get on is even able to connect. However, this also greatly limits the content available on the darknet. Furthermore, adding content is a fairly complicated process.

While FreeNet is a great system and currently in very active development, it is not quite ready for use in a situation like Iran.

GNUNET

GNUnet is an anonymizing filesharing network that is entirely peer-to-peer. By treating all peers as relays for data transfer, information being accessed by a client is indistinguishable from information simply being routed through the peer. While fairly simple to use, GNUnet has a fairly small user-base, meaning that the content available, and the speed of downloading it, may not be too great.

SUMMARY

In handling the Iranian firewall's current measures and expansion, there are a wide variety of options. However, at this time, none are ideal and all are able to be theoretically filtered without cutting all Internet. We do have several ways to keep the Iranian people communicating with the world and each other and are developing new and expanded communication methods.

CONCLUSION

The Iranian firewall is a much more thorough method of communication filtration than has previously been seen on a national scale. It will be difficult to defeat, even temporarily, but not impossible. It will require a great deal of work, however, and developing and improving on existing tools, or even creating new tools. With a dedicated effort to circumvent it, the Iranian firewall will be routed around.

“The Internet interprets censorship as damage and routes around it.”

- *John Gilmore, cofounder of the Electronic Freedom Foundation*

WORKS CITED

- Colascione, D. (2009, July 10). Questions About Haystack. (Multiple, Interviewer)
- Cowie, J. (2009, June 14). *Strange Changes in Iranian Transit*. Retrieved July 10, 2009, from renesys|blog:
<http://asert.arbornetworks.com/2009/06/a-deeper-look-at-the-iranian-firewall/>
- Drash, W. (2007, September 28). *Internet cut in Myanmar*. Retrieved July 10, 2009, from CNN.com:
<http://www.cnn.com/2007/WORLD/asiapcf/09/28/myanmar.dissidents/>
- Gharam News. (2009, June 11). Retrieved July 10, 2009, from Gharam News: <http://www.gharamnews.ir/news-20704.aspx>
- Heap, A. (2009, July 4). *Haystack: Good Luck Finding That Needle*. Retrieved July 11, 2009, from Austin Heap:
<http://blog.austinheap.com/2009/07/04/haystack-good-luck-finding-that-needle/>
- Kanalley, C. (2009, June 11). *SMS system down in Iran just hours before election*. Retrieved July 10, 2009, from breaking tweets: <http://www.breakingtweets.com/2009/06/11/sms-system-down-in-iran-just-hours-before-election/>
- Labovitz, C. (2009, June 18). *A Deeper Look at The Iranian Firewall*. Retrieved July 9, 2009, from Arbor Networks:
<http://asert.arbornetworks.com/2009/06/a-deeper-look-at-the-iranian-firewall/>
- NedaNet. (2009, June 19). *BRN Monitoring*. Retrieved July 9, 2009, from
http://emsenn.com/iran/brn_monitoring.png
- NedaNet. (2009, June 15). *NedaNet Research*. Retrieved July 9, 2009, from Ping Comparison:
http://emsenn.com/iran/ping_comp.txt
- Nolte, H. (2009, July 3). *#iranelection - Twitter topics & historic events*. Retrieved July 10, 2009, from examiner.com: <http://www.examiner.com/x-6207-Using-Computers-Examiner~y2009m7d3-iranelection--amazing-Twitter-trending-topic-stats-and-historic-events-cited>
- Stilgherrian. (2008, August 1). *The Great Firewall of China*. Retrieved July 10, 2009, from Stilgherrian:
<http://stilgherrian.com/politics/the-great-firewall-of-china-how-it-works-how-to-bypass-it/>

Wire News Sources. (2009, July 2). *Iran 'lifts block on SMS texting'*. Retrieved July 10, 2009, from Herald de Paris:
<http://www.heralddeparis.com/iran-lifts-block-on-sms-texting/42694>