**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačního inženýrství**


**Bakalářská práce**

# Internetové služby v prostředí cenzurovaných sítí

**Ali Saremi**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ali Saremi

Informatika

Název práce

**Internetové služby v prostředí cenzurovaných sítí**

Název anglicky

**Internet services in censored networks**

---

**Cíle práce**

Tato bakalářská práce se zabývá prostředky blokování a cenzury na internetu. Jejím cílem je popsat nástroje, které jsou využívány k cenzurování a omezení přístupu na internet v Íránu.

**Metodika**

První část práce se bude zabývat definicí cenzury, důvody jejího zavedení a zhodnocení dopadů cenzury v Íránu. Druhá část se bude zabývat typům internetové cenzury a možnostem technického obcházení cenzury. Závěrečná část bude zaměřena na experiment filtrování a následné ověření funkčnosti internetových služeb. Pro technická měření a experimenty bude použita platforma FortiGate. Dokumentační část práce bude dodržovat standardy softwarového inženýrství, především modelovací jazyk UML a vnější metriky určené pro měření jakosti softwaru.

**Doporučený rozsah práce**

40-60 stran

**Klíčová slova**

Internet, Cenzura, Internetové služby, Obcházení internetové cenzury

---

**Doporučené zdroje informací**

DEIBERT, Ronald. Access denied: the practice and policy of global Internet filtering. Cambridge, Mass.: MIT Press, c2008. ISBN 978-0262541961

DUTTON, William H. Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet. Paris: UNESCO Pub., c2011, 103 p. ISBN 978-923-1041-884

MATHIESEN, Kay. Censorship and Access to Expression. HIMMA, Kenneth Einar a Herman T. TAVANI. The handbook of information and computer ethics. Hoboken, N.J.: Wiley, 2008, s. 573-587. ISBN 978-0-471-79959-7

---

**Předběžný termín obhajoby**

2019/20 ZS – PEF (únor 2020)

**Vedoucí práce**

doc. Ing. Vojtěch Merunka, Ph.D.

**Garantující pracoviště**

Katedra informačního inženýrství

Elektronicky schváleno dne 25. 11. 2019

**Ing. Martin Pelikán, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 25. 11. 2019

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 30. 11. 2019

**Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Internetové služby v prostředí cenzurovaných sítí" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2019 _____

**Poděkování**

Rád bych touto cestou poděkoval svému vedoucímu bakalářské práce doc. Ing. Vojtěchu Merunkovi, Ph.D. za odborné vedení, který byl vždy trpělivý a od kterého jsem rád přijímal rady a připomínky, které mi poskytoval při psaní této práce.

**Internetové služby v prostředí cenzurovaných sítí**


## Abstrakt

Tato bakalářská práce se zabývá tématem filtrování neboli cenzurovaní internetu a popisuje metodiky, které se využívají k omezení přístupu na internet a cenzurování. Teoretická část práce popisuje podstatu filtrování, jakým způsobem to funguje a jaká je situace cenzury v Íránu. Čtenář je zde také seznámen se sadu protokolů, které jsou použité k filtrování a také s možností obcházení cenzury. Praktická část je zaměřena na způsob fungování cenzury pomocí filtračních programu a následně ověření funkčnosti filtru.



**Klíčová slova:** Internet, Cenzura, Internetové služby, Obcházení internetové cenzury

**Internet services in censored networks**


## Abstract

This bachelor thesis deals with the topic of filtering or the Internet censorship and describes methodologies that are used to censoring and internet access restrictions. The theoretical part describes the substance of filtering, how it works and how is the situation of censorship in Iran. The reader is also acquainted with a set of protocols that are used for filtering and the possibility of circumventing censorship. The practical part is focused on the way censorship works by filtering programs and then verification of filter functionality.



**Keywords**: Internet, Censorship, Internet services, Internet censorship circumvention

**Obsah**

**Seznam obrázků**

**Seznam tabulek**

# 1. Úvod

Obvykle tam, kde platí určitá omezení, je větší pravděpodobnost, že se ji lidé budou snažit obejít. To samé platí pro internetové cenzury v zemích jako je Írán.
Od té doby, kdy se cenzura internetu v Íránu stala vážným tématem, tak se téměř okamžitě našel také způsob, jak ji obcházet. V dnešním světě je téměř nemožné zabránit lidem v přístupu k informacím. Nehledě na to, jak silné a pokročilé jsou filtrační systémy, tak oproti lidské inteligenci jsou bezmocné.

# 2. Cíl práce a metodika

## 2.1. Cíl práce

Tato bakalářská práce se zabývá prostředky blokování a cenzury na internetu a cílem je popsat metodiky, které jsou využívány k cenzurování a omezení přístupu na internet.
První část definuje cenzuru, důvody jejího zavedení a vyhodnocuje situaci cenzury v Íránu.
Druhá část se zabývá typy internetové cenzury a možnostmi obcházení cenzury.
Závěrečná část je zaměřena na provádění filtrování a následné ověření funkčnosti.

## 2.2. Metodika práce

První část práce se bude zabývat definicí cenzury, důvody jejího zavedení a zhodnocení dopadů cenzury v Íránu. Druhá část se bude zabývat typům internetové cenzury a možnostem technického obcházení cenzury. Závěrečná část bude zaměřena na experiment filtrování a následné ověření funkčnosti internetových služeb. Pro technická měření a experimenty bude použita platforma FortiGate. Dokumentační část práce bude dodržovat standardy softwarového inženýrství, především modelovací jazyk UML a vnější metriky určené pro měření jakosti softwaru.

# 3. Teoretická východiska

## 3.1. Úvod do filtrování

### 3.1.1. Příčiny filtrování

Rozšíření internetu vytvořilo zázemí, kde je možné, aby široká škála informací se po celém světě šířila bez omezení. Na druhé straně bylo spektrum internetových uživatelů stejně široké a rozmanité jako jeho obsah. Neomezený přístup k informacím a skutečnost, že kdokoli by měl přístup k jakékoli informaci, mnoho vyděsilo a vyvolalo kritiku. Existovala skupina kritiků, kteří protestovali proti neetickému obsahu internetu a považovali to za zvláště škodlivé a perverzní pro děti a dospívajících. Druhou skupinou kritiků byly vlády, které nesnesly odpor. Tyto vlády se po léta snažily prosadit své myšlení a ideologii svým národům, omezovaly jejich společnost a cenzurovaly média, jako jsou tisk a noviny, a tak tvrdě zasahovali proti jakékoli modernosti a nesouhlasu, které odporovaly jejich touhám. Není divu, že takové vlády považují internet a šíření informací, které nejsou pod jejich kontrolou, za vážnou hrozbu pro jejich samotnou existenci. Protože se většina těchto vlád, navzdory své přirozené povaze, snažila prezentovat jako demokratické a hledající svobodu, nemohla uvést hlavní důvod své opozice vůči svobodné výměně informací. Proto se také připojili k předchozí skupině a prosazovali boj proti korupci a nemorálnímu materiálu.

Obě skupiny však neměli možnost úniku od internetového prostředí. Vědecké a kulturní úspěchy internetu byly ve skutečnosti tak velké, že je nebylo snadné ignorovat. Vzhledem k tomu, že internet byl globální sítí a na základě své struktury nemohla mít žádná skupina ani vláda úplnou kontrolu nad tím, co bylo zveřejňováno, postupně vznikala myšlenka kontrolovat spíše přístup a dosah uživatelů internetu než kontrolovat publikace.

Zde se do internetové kultury dostal pojem „filtrování“. Filtrování znamená odstranění nečistot, ale v internetové kultuře je to blokování přístupu uživatelů na stránky, které obsahují nevhodný obsah.

Na rozdíl od toho, co se původně myslelo, nebylo filtrování úspěšné v boji proti korupci a nevhodnému obsahu, nejenže nebránilo jeho rozsáhlému zveřejňování na internetu, ale také s sebou přineslo neočekávané problémy, které vyvolaly kritiku, a dokonce prudkou opozici.

Hlavní nevýhodou filtračních systémů bylo to, že bylo implementováno pomocí počítačového softwaru. Není divu, že tyto systémy kvůli své strojové povaze nerozumí lidským spisům

a materiálům a jednají slepě. Například na některých webových stránkách, zejména na těch, které nabízejí služby blogů, mohou existovat stovky nebo možná tisíce článků, které obsahují pouze malé procento neetického obsahu. Jelikož filtrační systémy nejsou schopny tyto obsahy odlišit, blokují přístup k celému webu, a tak činí obrovské množství cenných informací a materiálu nepoužitelným.

Dalším problémem s filtrováním bylo to, že uživatelé internetu tvořili širokou škálu lidí, od pětiletého dítěte po padesátiletého člověka, od negramotné osoby po zkušeného univerzitního profesora, stejně jako od lidí různého pohlaví, různých náboženství a různých úrovní myšlení. Je zřejmé, že různí lidé mají různé potřeby, a co je považováno za škodlivé a zavádějící, může být pro někoho užitečné, dokonce nezbytné. Filtrační systémy však tyto rozdíly nedokázaly odhalit, a tak cenzurovaly všechno stejně.

Obvykle za nemorální jsou považovány stránky, které obsahují sexuální problémy a vulgárnost. Tyto stránky nelze zcela filtrovat, jelikož jejich obsah je víceméně podobný, neboť se stovky těchto webů vytvářejí každý den a prakticky nejsou k dispozici žádné filtry, které by je všechny detekovaly a blokovaly. V nejnáročnějších filtračních systémech může i jeden nezkušený uživatel pomocí vyhledávače získat přístup k jednomu z těchto webů za méně než deset minut. Většina obětí filtrování jsou uživatelé, kteří chtějí správně používat internet.

Podle výše uvedených informací vypadá, že místo vyčišťování internetu se stalo filtrování nástrojem despotických vlád. To lze lépe pochopit s ohledem na geografické rozšíření filtrování. Je zřejmé, že filtrování bylo prováděno v zaostalých zemích, které mají černou historii v oblasti lidských práv, a prakticky neexistují žádné vyspělé země, které by zbavily svobodu jejich občanů od volného přístupu k informacím. Je třeba podotknout, že v západních zemích je filtrování také poněkud dohodnuto, ale jeho rozsah je přísně omezen na weby, které distribuují pornografické obrázky a nemorální obsah. V těchto zemích vláda nepoužívá filtrační systém, nýbrž tuto práci provádí pouze některé poskytovatelé internetových služeb (ISP). Rodiče, kteří se obávají o zdraví svých dětí a dospívajících, používají takové ISP k přístupu na internet.

V zemích, kde je filtrování prováděno, se dříve či později každý uživatel internetu setká s problémem, že stránku, kterou potřebuje, je neprávem filtrována. Vzhledem k tomu, že ve většině těchto zemí neexistuje oprávnění pro protesty, existují pro uživatele dva způsoby. Buď se vzdají a dovolí nadřízeným, aby se rozhodli o jejich osudu, nebo pokračují ve své vůli a pokusí se osvobodit od diktatury a cenzury.

Lidská přirozenost je taková, že nemůže souhlasit s jakoukoliv nadvládou nebo omezením, přestože je to uvaleno z laskavosti. Proto mnoho uživatelů přistoupilo k cenzuře tváří v tvář a pokusilo se znovu získat ztracenou svobodu. Jakmile se filtrování začalo rozšiřovat, rovněž se vyvinula i kultura anti-filtrování.

Naštěstí počáteční rozvoj internetu proběhl v zemích, kde reaktivní myšlení a přístup k péči nemají místo. V těchto zemích je člověk považován za stvoření mající rozum a moudrost, které dokáže rozpoznat jeho dobro a zlo. V důsledku toho je struktura internetu založena na základě svobodné a neomezené výměny informací a ve skutečnosti jsou filtrační systémy komponenty uložené na internetu, které zcela nevyhovují jeho ostatním strukturám. Tato nekompatibilita vytvořila četné únikové cesty, které mohou uživatelé použít k překonání bariéry filtrování.

Je však třeba poznamenat, že filtrování a boj proti němu je nekončící. Na jedné straně pole jsou vládci a vlastníci filtračního průmyslu, kteří se snaží minimalizovat únikové cesty uživatelům a zpřísnit smyčku dominance nad svými vlastními lidmi, a na druhé straně se uživatelé snaží identifikovat, využívají slabých stránek systému a získávají zpět svou ztracenou svobodu.

Jisté je, že ani jedna strana nevyjde jako absolutní vítěz a na každou akci bude reagovat druhá strana, a proto je lepší použít frázi „odpor proti filtrování“ místo „boj proti filtrování“, neboť se jedná o virtuální válku ve virtuálním světě a ti, kteří skutečně chtějí bojovat proti filtrování a cenzuře, musí bojovat s kořeny pramenícími z krátkozrakosti a despotismu ve reálném světě. [1]

### 3.1.2. Cenzura internetu v Íránu

Od vstupu internetu do Íránu uplynulo více než dvacet pět let. Íránští uživatelé měli hezké vzpomínky na první roky příchodu technologie do své země, jelikož v prvních letech zažili tuto technologii bez cenzury. Ale neuplynulo dlouho a země se stala jedním z největších internetových cenzorů. Dnes je Írán spolu s Čínou jedním z největších internetových cenzorů, i přestože růst internetu v Íránu je velmi významný. V roce 2001 bylo v Íránu milion uživatelů a v roce 2017 tento počet vzrostl o dalších 51 milionů. Momentálně v Íránu internet používá šedesát devět procent populace. V současné době existuje v Íránu více než 660 poskytovatelů internetových služeb (ISP) a zhruba 19 ICP firem.

Firma Shatel, přidružený k íránské telekomunikační společnosti, je největším poskytovatelem internetových služeb v zemi.

Podle „Pravidel a předpisů pro počítačové informační sítě“ jsou všichni poskytovatelé aplikačních služeb, včetně telekomunikační společnosti, povinni zavést filtrační systém, který zabrání uživatelům přístup k neautorizovaným webům.

Podmínky filtrování jsou schválené v nejvyšší radě. V současné době existuje tříčlenný výbor složený ze zástupců telekomunikace, ministerstva kultury a ministerstva informací a bezpečnosti, které jsou pod vedením nejvyšší rady kulturní revoluce a dohlíží na internetové aktivity. Tato skupina je oficiálním orgánem a má na starosti seznam blokovaných webů. Přesto bylo opakovaně zjištěno, že i soudní moc přímo vydala příkazy k blokování některých webových stránek.

Internetová cenzura v Íránu probíhá různými způsoby a na různých úrovních. Pro stránky, kde se server a jeho provozovatelé nacházejí v Íránu, se to řeší formou donucení, ale u takových stránek, které nemají server v Íránu, se to řeší formou blokování přístupu uživatelů k konkrétnímu webu.


**Obrázek 1 – Zpráva blokovaného přístupu v Íránu**
**Zdroj: [2]**

Na základě jedné z nejnovějších studií prováděných společností OpenNet, která se snaží monitorovat situaci cenzury v různých zemích po celém světě, bylo v Íránu zhruba 30 procent (501 webů z 1479) vyšetřovaných webů zablokováno. Výsledky výzkumu zveřejněné ve třiceti stránkové zprávě ukazují, že Írán aplikoval jeden z nejtěžších a nejpřísnějších filtračních systémů. Souhrn výsledků této studie je následující:

- V současné době je filtrování v Íránu zaměřeno na otázky týkající se Íránu, zejména na stránky v perském jazyce. Weby, které nejsou propojené s Íránem, jsou mnohem méně v ohrožení cenzury.

- Cenzura se konkrétně zaměřila na osobní blogy a weby poskytující služby blogů. Během období 2004 až 2005 se cenzura blogů zvýšila, i když bylo pro ně snažší blokovat weby poskytující služby blogů, ale vláda místo toho často blokovala blogy zvlášť. Cílem Íránu je povolit přístup jen některým blogům a opoziční blogy blokovat.
- Další oblastí cenzury jsou zpravodajské servery. Podle statistik je pouze pět procent anglických zpravodajských serverů cenzurováno, ale toto číslo u íránských zpravodajských serverech dosahuje padesáti procent.
- Cenzurovány jsou také stránky obsahující pornografický obsah.
-Tato studie předpovídá, že kromě skutečnosti, že v Íránu je filtrování mírně rozšířeno, bude také kvalita filtračních postupů časem sofistikovanější a přesnější. [3]

### 3.1.3. Web filter

Web filter je technologie, která uživatelům brání přístup na určité URL adresy nebo webové stránky. Webové filtry jsou vyrobeny pro různé účely a poskytují různá řešení pro individuální, rodinné nebo podnikové použití.

Web filtr může zablokovat stránky, které pravděpodobně zahrnují nežádoucí reklamu, pornografický obsah, spyware, viry a další nežádoucí obsah. Nástroje Web filtru pracují s aktualizovanou URL databází, která ukazuje weby a domény spojené s hostováním malwaru, phishingu, virů nebo jinými nástroji pro škodlivé činnosti.

Největší skupiny, které používají Web filter, jsou:

**Rodiče** – chtějí svým dětem zabránit v přístupu k nežádoucím a nevhodným obsahům.

**Firmy** – chtějí zamezit zaměstnancům v přístupu na stránky, které se netýkají jejich obsahu práce.

**Školy** – používají Web filter za stejným účelem, jako rodiče a firmy, zároveň doufají, že budou chráněny před napadením malwaru.

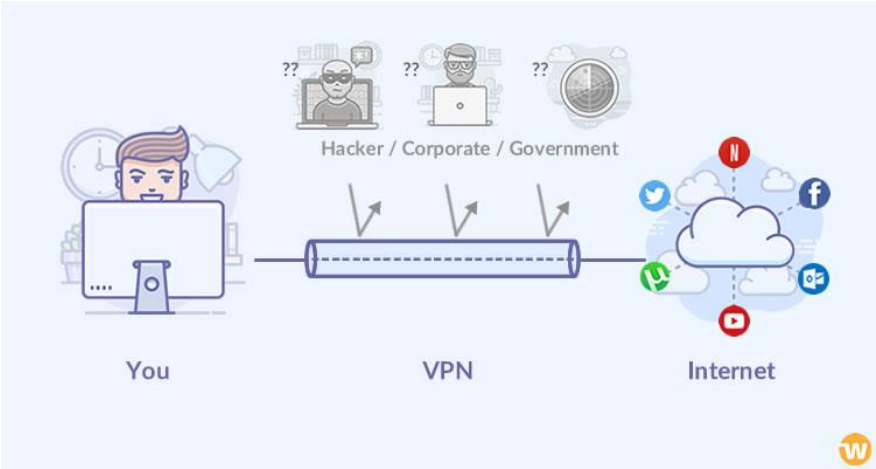
Web filter blokuje přes klíčová slova (Keywords) nebo přes Blacklist a Whitelist (černá a bílá listina).

Filtrování webu je vynikajícím nástrojem, který pomůže zabránit útokům či ztrátě zabezpečení. Bezpečnost podniku je důležitá. Sledováním a filtrováním toho, co zaměstnanci sdílejí, pomáhá aktivně prosazovat zásady IT a také zabraňuje úniku dat. Webové filtry mohou uživatelům bránit přístup na weby, které v počítači uživatele provádějí škodlivý kód. [4]

### 3.1.4. Virtuální privátní síť (VPN)

VPN je soukromá síť, která používá veřejnou síť k vzájemnému propojení vzdálených uživatelů nebo webů. VPN používá „virtuální“ připojení směrovaná přes internet ze soukromé sítě firmy nebo z VPN služby třetí strany na vzdálený web nebo osobu. VPN zajišťuje zabezpečení a data jsou šifrovaná. Také zajistí dokonalou online anonymitu a již není potřeba používat síť TOR, která přesměrovává připojení mezi připojenými hostiteli. VPN je alternativou k technologii TOR.

Výhodou VPN je, že vás ukryje dokonale a nikdo nedokáže zjistit, odkud se doopravdy připojujete. Pokud je poskytovatel VPN solidní, tak vám nabídne IP adresy z různých míst po celém světě. Například přijedete do Vídně a zjistíte, že stránka, kterou doma obvykle navštěvujete, není v Rakousku dostupná. Ve VPN si budete muset nastavit IP adresu ze své země a pokud z domova budete chtít navštívit stránku, která je dostupná pouze v Rakousku, tak si nastavíte tamní IP adresu.




**Obrázek 2 – VPN**
**Zdroj: [5]**

Existují dva základní typy VPN. První je VPN pro vzdálený přístup, která umožňuje uživatelům připojení k jiné síti přes soukromý šifrovaný tunel.

Druhým typem je Site-to-site VPN (router-to-router VPN). Tato VPN je používána především v podnikových prostředích – zejména v případech, kdy má podnik sídla na různých místech. Site-to-site VPN vytváří uzavřenou interní síť, přes kterou se lze připojovat k jednotlivým pracovištím. Pro tuto síť se také používá pojem intranet.

Existuje několik způsobů zabezpečení VPN. Tím nejstarším je PPTP (point-to-point tunneling protocol), který je dnes stále používán a také považován za jeden ze slabších protokolů. Dalšími jsou IPSec, L2TP, SSL, TLS, SSH a OpenVPN. Řada lidí dává přednost OpenVPN,

který je opensourcový software. To znamená, že když se objeví nějaká chyba, někdo si jí brzy všimne a bude rychle opravena. [6]

### 3.1.5. Reverzní filtrování

Problémy, které mají Íránci s používáním internetu, mohou být jedinečné na celém světě. Zatímco íránská vláda je spolu s Čínou hrdá na to, že je jedním z největších internetových cenzorů na světě, tak díky zákonům Spojené státy zpřísnily přístup k internetu íránským uživatelům. Podle těchto pravidel americké společnosti zastavily své poskytování služeb pro státy jako je Írán, Kuba, Severní Korea, Sýrie a Súdán. Hlavním cílem těchto sankcí bylo zpočátku neumožnit finanční transakce a internetové platby. Bohužel se tyto sankce tak moc rozšířily, že dokonce některé společnosti brání uživatelům těchto zemí stahovat jejich software.

Tento typ filtrování se neprovádí u zdroje, ale v místě určení. Server poskytovatele služby nejprve zkontroluje IP adresu klienta před poskytnutím jakékoli služby a pokud je IP adresa z výše uvedeních zemí, tak jim odmítne poskytnout službu. Tento typ filtrování se nazývá reverzní filtrování (Reverse Filtering).

Většina amerických společností odmítají přijímat internetové platby z Íránu, což znepříjemňuje situaci iránským uživatelům nakupovat online. I když se k platbě používají americké nebo mezinárodní kreditní karty jakou jsou MasterCard a Visa Card, tak transakce jsou stále nemožné, jelikož probíhají z Íránu. V případě internetových plateb je způsob fungování těchto společností jedním ze tří způsobů:

– Řada těchto společností zcela brání přístupu na jejich webové stránky íránským uživatelům. Když uživatel chce přejít na jejich web z Íránu, tak setká se s takovými chybami jako jsou: Time out a Forbidden

– Některé společnosti, jako je PayPal, umožňují uživateli navštívit jejich webové stránky, ale v případě, že uživatel chce provádět finanční transakcí, tak obdrží varovnou zprávu, že jeho IP adresa je ze sankciované zemí a z toho to důvodu transakce nemůže probíhat.

– Existuje další skupina společnosti, která poskytuje všem uživatelům plný přístup k jejich webu, a dokonce jim dovolí provádět transakci. V případě, že uživatel pochází ze sankciované země, tak zhruba do dvou dnů od transakce, dostane zprávu, že transakce nemohla proběhnout, jelikož pocházíte ze sankciované zemí. Je třeba podotknout, že v případě online platby je tam obvykle 72 hodinový časový interval, který umožňuje dodavatelské firmě ověřit

informace o zákazníkovi a během tohoto intervalu se neodečítají žádný peníze z účtu zákazníka. [7]

## 3.2. Základy internetového filtrování

Než budete chtít prolomit cenzuru a projít filtrem, musíte mít informace ohledně obsahu a fungování filtrovacích systému. Jak jíž víte, internet je síť tisíců menších sítí a milionů počítačů sdílejících informace. Když se rozhodnete navštívit nějakou webovou stránku, tak váš počítač pošle požadavek serveru a tento požadavek cestou projde desítkami možná stovkami dalších počítačů. Váš poskytovatel internetu a vaše místní telekomunikační síť jsou na začátkem této terasy. Nyní si představme, že místní síť je vybavená filtračním systémem. Tak průběh bude následující:
– Váš počítač požaduje webovou stránku.
– Tato žádost bude nejprve odeslána vašemu poskytovateli služeb internetu a odtud do vaší místní sítě.
– Před tím, než je požadavek z místní sítě odeslán na server, na kterém je webová stránka hostována, je zkontrolován filtračním systémem.

Zde se vyskytnou dvě cesty:

a) Filtrační systém zkontroluje váš požadavek a v případě, že není v rozporu, tak umožňuje mu vyhovět. V tomto případě se vaše žádost dostane na server a následně vám bude zaslána hledaná stránka.
b) Filtrační systém detektuje, že váš požadavek je neautorizovaný a zablokuje jej. V takovém případě požadavek se nedostane server a místo toho obdržíte varovnou zprávu.

Technicky může být filtrační systém umístěn na ISP, ale bohužel to nemá žádný vliv na výsledek. Výše uvedené kroky jsou naprosto stejné, kromě toho, že tentokrát jsou žádosti zpracovány na úrovni ISP. Filtrační systém porovná požadavky se seznamem, který má v sobě, a pak rozhodne, zda jim umožní projít nebo ne. Tento seznam se nazývá černý seznam (Black list). Black list se skládá ze tří složek:

a) Adresa domény (Domain Address): Toto je název webu, ke kterému chcete přistupovat. Např.: www.google.com.
b) IP Adresa: Tato adresa je číselná. Adresa se podobá telefonnímu číslu a každý počítač, který má připojení k internetu, má svou vlastní IP adresu. Např. www.google.com má IP adresu: 66.249.93.104
c) Klíčová slova (Keywords): Jedná se o fráze nebo slova, kterým, pokud jsou na černé listině, počítač blokuje požadavek.

   Když váš požadavek dorazí do filtračního systému, tak systém jej porovná s názvy domén, IP adresami, a navíc se slovami ve své černé listině. Pokud je vše v pořádku, bude žádost považována za tzv. čistou (clean) a povolí mu projít. V případě, že filtrační systém najde shodu s černou listinou, tak označí požadavek za špinavý (dirty) a nepovolí projít. Uživatel následně dostane varovnou zprávu ve tvaru „Nelze získat přístup k dotyčnému webu“. [8]

### 3.2.1. Druhy filtrování

Existují různé druhy filtrování, které lze použít v závislosti na okolnosti a požadavky. Porozumět těmto metodám je nezbytné, protože pro konfrontaci s nimi, je třeba použít různé cesty. Zde je několik nejčastějších způsobů filtrování: [9]

#### 3.2.1.1. Filtrování přes DNS

Tato metoda je jednoduchá a není tolik nákladná. Na druhé straně je snadné a jednoduché obejít tento filtr. DNS je systém doménových jmen. Jak jíž víte, systém internetového adresování je založen na IP adrese a každý počítač připojený k internetu má svou vlastní IP adresu. IP adresa se podobá telefonnímu číslu a skládá se ze čtyř různých čísel oddělených tečkou. Například adresa IP webu Google je 66.249.93.104.

Jelikož bylo pro lidi obtížné si zapamatovat čísla, tak byla vytvořena doménová jména. Doménová jména jsou tvořena z písmen a slov. Tento systém převádí doménové jméno na odpovídající IP adresu. Například v prohlížeči zadáte google.com, váš počítač odešle požadavek na server DNS a jako odpověď obdrží IP adresu Google 66.249.93.104. Tento děj probíhá na pozadí, mimo váš dohled. [10]

#### 3.2.1.2. Filtrování přes Proxy

V tomto případě poskytovatel služeb internetu omezuje přímý přístup k internetu a vyžaduje použití proxy serveru. V nastavení prohlížeče musíte zadat adresu proxy serveru, kterou vám poskytl poskytovatel pro přístup k internetu. Tím se všechny vaše požadavky odešlou na proxy server, a pokud je vše v pořádku, tak si proxy ten soubor z internetu stáhne a pošle je vám. Je třeba podotknout, že proxy servery mají mnoho využití. Mohou být použity jak pro filtrování, tak i pro anti-filtrování. [11]

#### 3.2.1.3. Filtrování přes Router

Routery neboli směrovači jsou jedno z hlavních součástí sítí. Tato zařízení jsou zodpovědná za směrování a řízení provozu v síti. Když bude cenzura probíhat přes router, tak se to obvykle děje ve výstupní místě s názvem brána (Gateway), kde se místní síť připojí na internet. Router je nakonfigurován tak, aby přesměroval požadavek filtrovací systém. Systém kontroluje požadavek, zda neobsahuje nevhodná slova a neautorizované stránky, v případě, že ano, tak ho blokuje. [12]

#### 3.2.1.4. Filtrování přes DLP (Data Leak Prevention)

Prevence úniku dat umožňuje zabránit úniku citlivých dat. Když se definují datové vzory, tak data odpovídající těmto vzorům budou blokována nebo zaznamenána a povolena při průchodu jednotkou. Systém DLP se dá nakonfigurovat vytvořením jednotlivých filtrů na základě formátu souboru, velikosti souboru, regulárního výrazu, pokročilého pravidla nebo složeného pravidla.

Přestože hlavní funkce DLP je zastavení citlivých dat od opuštění vaší sítě, lze ji také použít pro zabránění nechtěných dat v přístupu do vaší sítě. [13]

#### 3.2.1.5. Software na cenzurování

Cenzura se obvykle provádí prostřednictvím serverového počítače, ale někdy je prováděna přes software nainstalovaným v klientském počítači. Tomuto programu se říká Censorware. Obvykle se používá v domácnostech (kontrola rodičů nad dětmi), školách a univerzitách. Tento program je nainstalován samostatně na každém počítači, aby se zabránilo uživatelům v přístupu k neautorizovaným

stránkám. Zde jsou některé z následujících programů: Cyber Patrol, Cyber Sitter a Net Nanny. [14]

#### 3.2.1.6. Blokování portů

Porty jsou jako brány, kterými server poskytuje své služby. Každému portu je přiděleno číslo mezi 0 až 65535. Pokud se nějaký port zablokuje, tak všechny služby poskytované prostřednictvím tohoto portu, již nebudou k dispozici. Většina internetových cenzorů blokuje porty 80, 1080, 3128 a 8080. Protože se jedná o konvenční porty pro proxy servery a většina proxy serverů nabízí prostřednictvím těchto portů své služby. Pokud budou zablokovány další porty, tak následně nebudou přístupné služby poskytované prostřednictvím těchto portů. Například, jestli zablokujeme port 110, tak nebude možné přijímat e-maily. Níže vidíte některé důležité porty a služby poskytované prostřednictvím nich. [15]

**Tabulka 1 – Druhy portu**

| Číslo portu | Druh portu | Popis portu |
|---|---|---|
| **20,21** | FTP | přenos souborů |
| **23** | Telnet | připojení ke vzdálenému počítači |
| **25** | SMTP | přenos zpráv elektronické pošty |
| **53** | DNS | převod doménových jmen a IP adres uzlů sítě |
| **80** | HTTP | internetový protokol |
| **80** | Proxy | Proxy |
| **110** | POP3 | stahování e-mailových zpráv |
| **443** | SSL (HTTPS) | Zabezpečená komunikace |
| **1080** | Socks Proxy | Proxy |
| **3128** | Proxy | Proxy |
| **8000** | Proxy | Proxy |
| **8080** | Proxy | Proxy |

**Zdroj: [16]**

#### 3.2.1.7. Blacklist a Whitelist

Většina filtračních systémů funguje prostřednictvím Blacklistů. Blacklist obsahuje adresy stránek, které nejsou povoleny, a stránky, které nejsou v blacklistu, jsou automaticky povoleny. Někdy kromě adres stránek se používají také i klíčová slova. Pokud na požadovaném webu se najde slovo, které je v blacklistu, tak filtrační systém zablokuje požadavek. Používání klíčových slov je v systému filtrování přísnou metodou. Umožňuje identifikovat neautorizované weby, které dosud nebyly zkontrolovány z hlediska obsahu a jejich adresa nebyla na blacklistu. Použití klíčových slov navedou filtrační systémy k chybám a přílišnému blokování. Tato metoda se používá ve zvláštních případech, například pro pojmy sex a porno. [17]

Whitelist funguje opakem Black listu. To znamená, že obsahuje soubor stránek, které jsou povolené a ostatní stránky jsou považovaný za nepovolené. Whitelist je nejpřísnější způsob filtrování a je velmi obtížné jej obejít. Tato metoda se používá zřídka, protože přes Whitelist internet ztrácí svůj význam. Tento druh filtrování najdeme v organizacích, které chtějí, aby jejich zaměstnanci měli přístup pouze k několika webovým stránkám souvisejících s jejich prací. [18]

## 3.3. Jak se čelit proti filtrování

Pro boj s filtrováním neexistuje jednotná a komplexní metoda. Při výběru vhodné metody se musí brát v úvahu několik faktorů např. druh filtrování, finanční a právní záležitosti atd.

Jak je již uvedeno výše v tématu druhy filtrování, existuje několik způsobů filtrování, které cenzoři zvolí v závislosti na jejich potřebách a požadavcích. Bohužel vám nemůžeme pomoci určit druh filtrování. Je proto na vás, abyste určili druh použitého filtrování ve vaší oblasti a vybrali vhodná protiopatření.

Další věc, kterou je třeba si uvědomit, je, zda máte na to rozpočet. Ačkoli existuje mnoho metod, které můžete použít pro objetí cenzory a jsou zdarma, tak jsou méně spolehlivé a efektivní než peněžní metody. Většina z těchto metod je rychle identifikována a neutralizována úřadem a vy budete muset hledat nové metody. Zkušenost ukazuje, že čas a náklady, které strávíte v průběhu jednoho roku při hledání Proxy a anti-filtračních metod, vám vyjde dráže než peněžní metody.

V některých zemích je filtrační systém legálně podporován vládou a těm, kteří se ho snaží obejít, hrozí pokuty, a dokonce i odnětí svobody. Je jasné, že v takových případech musíte být velmi opatrní a používat pouze metody, na které nelze přijít.

Níže jsou vysvětlené metody, kterými se dá obejít cenzura. Pokusili jsme se věnovat více pozornosti metodám, které jsou použitelné v Íránu. Jelikož zhruba 80 procent poskytovatelů internetových služeb v Íránu jsou ohledně filtrování závislí na telekomunikační úřad, zaměřujeme se tedy na metody, které jsou proti tomuto typu filtrování účinné. [19]

### 3.3.1. Změna poskytovatele internetové služby (ISP)

Pokud se můžete pomocí zahraničních firem nebo satelitu najít internetové připojení, pak bude váš problém s filtrováním zcela odstraněn. Satelitní internet vyžaduje speciální vybavení a nemusí být pro běžného domácího uživatele příliš cenově dostupné.

Pokud jde o filtrování, tak íránští poskytovatelé internetu mají odlišné situace. Vzhledem k tomu, že v Íránu neexistuje jednotný systém filtrování, tak se někdy stává, že určitý web je filtrován některými poskytovateli internetových služeb, zatímco stejný web je přístupný prostřednictvím jiných poskytovatelů. Nejlepší je vyhnout se těmto poskytovatelům internetu.

Další metody filtrování popsané níže mohou být pro některé ISP velmi efektivní, zatímco pro jiné neúčinné. Abychom pochopili, která metoda je pro váš ISP nejlepší, tak je možné pouze na základě znalosti přesného systému filtrování nebo pomocí pokusu a omylu. [20]

### 3.3.2. Změna DNS

Filtrování přes DNS je nejjednodušší a nejméně nákladnou metodou cenzury a také se dá jednoduše obejít. Pokud je cenzura přes DNS, ignoruje všechny požadavky na neautorizované weby nebo je přesměruje na stránku, která obsahuje varovnou zprávu. Řešení je velmi jednoduché: vyměňte cenzurovaný DNS za jiný bezplatný DNS. Například:

- 171.64.7.55 (caribou.Stanford.EDU)

- 171.64.7.77 (cassandra.Stanford.EDU)

Telekomunikační úřad tuto metodu filtrování nepoužívá, ale někteří poskytovatelé internetových služeb ji mohou používat kvůli nízkým nákladům. [21]

### 3.3.3. Manipulace URL

URL je zkratka pro Uniform Resource Locator, což znamená jednotná adresa zdroje. Je to adresa webové stránky na internetu, kterou vidíte v adresním poli prohlížeče. URL se skládá ze tří komponent:

– Protokol používaný pro komunikaci: Pro webové stránky je to protokol HTTP.

– Název domény (Domain): Toto je název serveru, na kterém je umístěn hledaný soubor.

– Cesta (Path): Tato část určuje umístění požadovaného souboru na serveru.

Podívejte se na URL této stránky v adresním řádku prohlížeče. Tato adresa URL označuje, že protokol HTTP byl použit pro komunikaci s webovým serverem Nofilter. Zbytek adresy URL určuje umístění souboru f1_howto_bypass.htm na serveru Nofilter. [22]

- http://www.no-filter.com/censor/f1_howto_bypass.htm

Většina filtračních systémů fungují přes Black list. Black list obsahuje adresu URL sady webů, kterým je odepřen přístup. Filtrační systémy někdy i do Black listu zařadí klíčová slova. Když požádáte o návštěvu webové stránky, tak filtrační systém porovná URL stránky s Black listem a pokud najde shodu, zablokuje ji.

Existuje způsob, jak tento problém vyřešit. Lze změnit URL adresu tak, aby již nebyla shodná s Black listem, ale zároveň stále ukazovala požadovanou stránku. Zde je několik triků:

Zkuste namísto názvu domény použít IP adresu webu. Například místo adresy www.google.com napište 66.249.93.104 a přivede vás to na web Google. Pokud nemáte IP adresu webu, otevřete ve Windows Příkazový řádek (Command Prompt) a zadejte následující příkaz:

- C:\> ping www.google.com

Také existuje řada webových stránek, které vám poskytují IP adresu hledaného webu.

Tato metoda jev Íránu poněkud účinná. Účinek této metody závisí na tom, zda je IP adresa požadovaného webu na Black listu nebo ne. Také některé weby jsou hostovány na sdílených serverech a sdílejí společnou IP adresu s jinými weby.

Přidejte číslo portu na konec názvu domény. Například místo google.com napište google.com:80. Port 80 je výchozí port pro protokol HTTP. Tato metoda není účinná při filtrování telekomunikačního úřadu.

Na konec názvu domény přidejte tečku. To znamená, že místo google.com/ napište google.com./. Tato metoda pro některé ISP funguje velmi dobře.

Triky s manipulaci URL jsou založeny na chybách v návrhu a konfiguraci filtračních systémů. Proto nejsou tak spolehliví. Jakmile se zjistí poruchu systému, opraví ji a tyto triky budou neutralizovány.

### 3.3.4. Použití mezipaměti (Cache) vyhledávače

Když přes vyhledávač jako je třeba Google něco vyhledáte, tak výsledky hledání se zobrazí na jedné stránce. Předpokládejme, že kliknete na jeden z těchto výsledku a místo očekávané stránky se Vám zobrazí zpráva „Nelze získat přístup na stránku“. Jednoduchým řešením je jít zpět na stránku s výsledky vyhledávání. Tentokrát místo kliknutí na výsledek vyhledávání klikněte na výraz mezipaměti (Cache), která je o něco níže. Poté se vám zobrazí kopie hledané stránky, která je archivovaná na serveru vyhledávače. Tato kopie je stará několik dny a obvykle postrádá fotografie a multimédia, ale každopádně může se Vám hodit.

V případě, že chcete zobrazit stránku přímo prostřednictvím mezipaměti Google, nejprve zadejte do vyhledávacího pole slovo „cache:“ a poté zadejte adresu požadované stránky. Např.: cache:https://www.aljazeera.com/topics/country/iran.html

Tato metoda před nějakou dobou v Íránu fungovala dobře, ale v poslední době díky vylepšenému systému filtrování je méně účinná. V případě, že se Vám nepodaří odbourat filter pomocí mezipaměti, tak zkuste mírně změnit URL adresu webu. Např. odstraňte WWW adresy webu nebo použijte IP adresu Google. [23]

### 3.3.5. Peer-to-peer sítě

Peer-to-peer (P2P) jsou virtuální sítě, které jsou vytvářeny v rámci internetu na základě propojení počítačů. V P2P neexistuje žádný centrální server. Informace jsou distribuovány do všech počítačů v síti a každý počítač funguje jako server a zároveň i klient. Vzhledem k rozšířenosti a necentralizovanosti těchto sítí, není možné je kontrolovat anebo cenzurovat.

Chcete-li se připojit k jedné z těchto sítí, musíte do počítače nainstalovat software. Tímto způsobem můžete sdílet své oblíbené soubory s ostatními uživateli v síti a také je používat. Tyto sítě byly původně vytvořeny pro sdílení hudebních a softwarových souborů, ale v dnešní době na nich lze nalézt téměř cokoli. eDonkey a eMule jsou příkladem peer to peer softwaru. [24]

### 3.3.6. Používání jiných protokolů

Jak již bylo zmíněno, filtrování je nákladná záležitost. Proto se vždy snaží aplikovat cenzuru pouze na podstatné a citlivé části. Například v Íránu se filtrování vztahuje pouze na protokol HTTP (webové stránky) a ostatní protokoly jsou téměř bez cenzury. To znamená, že ačkoli je váš přístup na daný web zablokován, můžete s webem komunikovat přes e-mail. Prostřednictvím zabezpečeného připojení (HTTPS nebo SSL) můžete mít přístup k stránkám na tomto webu nebo přes FTP dostat se k souborům umístění na webu. V některých případech lze i komunikovat s webem přes chat. Samozřejmě to všechno záleží na konkrétním webu, zda tyhle služby poskytuje nebo ne. [25]

### 3.3.7. Proxy

Proxy je počítač, který umožňuje ostatním počítačům nepřímo komunikovat s jejich cílem. Použití Proxy je velmi rozmanité. Mohou být použity jak pro filtrování, tak pro anti-filtrování. Další informace ohledně Proxy najdete níže.

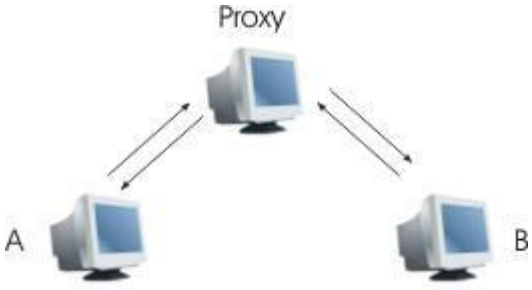
## 3.4. Co je to Proxy

Proxy doslovně znamená „právník“ a „ve jménu někoho, něco udělat“. Ve světě internetu proxy se říká počítači, který umožňuje ostatním počítačům komunikovat přímo s jejich cílem. Předpokládejme, že pracujete v kanceláři. Každá kancelářská místnost má telefonní linku, která je připojena k ústřední kanceláři. Pokud chcete zavolat z kanceláře do domů, musíte vytočit číslo (například 1) a poté požádat centrálu, aby vás spojili s domovem. Tohle přesně funguje jako proxy na internetu. Pokud je počítač připojen k internetu přes proxy a chce získat přístup k souboru, nejprve pošle svůj požadavek na proxy. Proxy se poté připojí k cílenému počítači, obdrží požadovaný soubor a poté jej odešle žadatelovi.

Tento obrázek ukazuje přímé spojení mezi klientskými počítači a klientem.

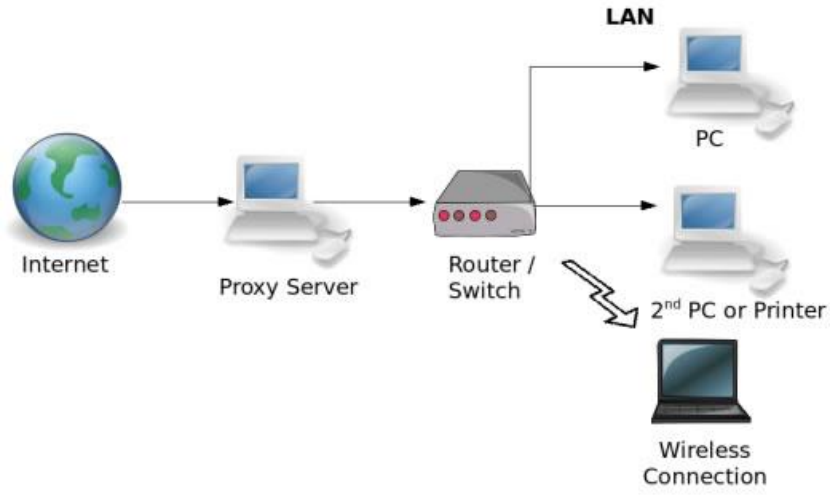

**Obrázek 3 – Přímé spojení**
**Zdroj: [26]**

Další ukazuje formu komunikace přes proxy. Jak vidíte, neexistuje prakticky žádné přímé spojení mezi serverovým počítačem a klientským počítačem.




**Obrázek 4 – Proxy spojení**
**Zdroj: [27]**

Jak vidíte, proxy zde funguje jako prostředník a mezi klientským a serverovým počítačem není prakticky žádné přímé spojení. Proxy zvýší efektivnost pro uživatele a může žádat o cenzuru (jak pro zavedení cenzury, tak i pro objetí cenzury). [28]




**Obrázek 5 – Proxy jako prostředník**

**Zdroj: [29]**

### 3.4.1. Zvýšení zabezpečení sítě

Správci sítě někdy používají proxy ke zvýšení zabezpečení sítě a ochraně uživatelů před hackery. V tomto případě místo toho, aby uživatele jednotlivě se připojili k internetu, tak všichni se připojí přes proxy na internet. Tímto způsobem může správce sítě s instalací firewallů a dalších softwaru a monitorováním proxy kontrolovat a chránit celou síť.

### 3.4.2. Omezování uživatele

Někdy správci sítě používají proxy k omezení uživatelů. Tato omezení neznamenají pouze filtrování nebo cenzuru, ale mohou pouze omezit používání určitého softwaru (například chatu) pro jeho uživatele.

### 3.4.3. Caching

Jednou z nejdůležitějších funkcí proxy je ukládání do mezipaměti. Cache je archivovaná verze internetového obsahu v proxy. Předpokládejme, že v proxy síti je několik set uživatelů. Nyní jeden z těchto uživatelů by chtěl číst zprávy z webu BBC News, takže pošle žádost na proxy a proxy tu stránku odešle jemu. Zde může proxy uložit kopii této stránky na pevný

disk. Pokud o tuto stránku požádá jiný uživatel, proxy se již nebude muset znovu stahnout tu stránku, ale jednoduše odešle z pevného disku. Zvýší se tím rychlost a efektivita sítě a zároveň se sníží provoz a zatížení sítě. Operace ukládání do mezipaměti má samozřejmě složitý algoritmus a proxy to musí zvládat tak, aby zabránil zasílání zastaralých informací.

### 3.4.4. Proxy port

Proxy nabízí svoje služby na konkrétních portech. Běžné porty pro proxy jsou 80, 1080, 3128 a 8080. Číslo proxy portu se napiše na konci proxy adresy se dvěma tečkami (:), například: 195.175.37.6:8080 anebo proxy.net:3128.

Mnoho internetových cenzorů blokuje porty, které jsou běžné, aby zabránili uživatelům používat proxy servery. V takovém případě byste měli hledat proxy server, který nemá blokované porty.

V Íránu port 80 nebude fungovat. Proxy, které jsou na portech 3128 a 8080, jsou často nespolehlivé, protože poskytovatele internetových služeb a také telekomunikační úřad je často blokuji. Ostatní porty jsou neblokované, avšak není snadné je najít. [30]

### 3.4.5. Proxy filtr

Někdy se můžete setkat s nechráněnými proxy servery, které jsou navrženy pro cenzuru. Vzhledem k tomu, že tyto proxy servery patří jiným zemím, je možné je použít pro přístup k filtrovaným politickým webům.

Jak je výše uvedeno, tak bude fungovat pouze několik proxy serverů. Dalším krokem pro získání fungujících proxy serverů je ověření jejich funkčnosti pro vás. Pro kontrolu proxy serverů existují programy, které od vás vezmou seznam proxy serverů a testují je jeden po druhém. Tento software se nazývá Proxy Checker. Zde najdete pár takových softwaru: MultiProxy, ProxyAnalyzer a ProxyScanner.

Jakmile najdete vhodný proxy, dalším krokem je nastavení prohlížeče, aby používal proxy místo přímého připojení k internetu.

Pokud jste úspěšně dokončili výše uvedené kroky, nyní můžete svobodně surfovat po internetu. Pouze pro filtrované weby používejte proxy a pro ostatní weby proxy deaktivujte, protože to může zpomalit rychlost vašeho internetu.

Nyní jste obeznámeni se základy a postupy proxy, ale také musíte vědět něco o druzích proxy. Proxy jsou rozděleny do několika skupin, z nichž nejdůležitější jsou:

**HTTP proxy:** Většina proxy serverů, se kterými se zabýváte, pochází z této skupiny. Tyto servery proxy jsou určeny k prohlížení webových stránek a podporují pouze protokol HTTP. Tyto proxy servery jsou určeny k prohlížení webových stránek a podporují pouze protokol HTTP. Někdy je však protokol FTP také podporován. Tyto proxy servery nelze použít k zobrazení zabezpečených (Secure) stránek, protože protokol používaný pro tyto stránky je HTTPS.

**HTTPS proxy**: Obvykle tyto proxy servery podporují protokoly HTTP i HTTPS a lze je použít pro procházení šifrovaných webových stránek a lze je také použít k procházení šifrovaných webových stránek.

**Socks proxy**: Tyto proxy servery, které jsou rozděleny na Socks 4 a Socks 5, jsou navrženy tak, aby podporovaly všechny internetové protokoly a jsou často umístění na portu 1080.

**Web proxy (CGI-Proxy)**: Tyto proxy servery se zásadně liší od výše uvedených proxy serverů. Toto jsou webové stránky, které umožňují uživatelům přístup k jiným webovým stránkám. Používají skripty, které jsou napsané ve webových programovacích jazycích (např. PHP a Perl). Tyto proxy servery se staly velmi populární, jelikož s nima se snadno pracuje. [31]

## 3.5. Jak se čelit Reverznímu filtrování

Reverzní filtrování je výsledkem amerických sankcí proti Íránské islámské republiky. Tyto sankce byly původně kvůli tomu, aby omezili finanční a obchodní transakce Íránu a dalších několika zemí, ale postupně se to rozšířilo také na stahování softwarů a dalších bezplatných internetových služeb.

Tento typ filtrování se zásadně liší od filtrování, o kterém jsme již mluvili. Tento typ filtrování není prováděn íránskou vládou, ale americkými společnostmi a je založen na kontrole klientovy IP adresy. Pokud IP adresa klienta patří do sezamu sankcionovaných zemí, tak webová stránka mu nebude poskytovat žádné služby.

Existuji tří způsoby, jak se vypořádat s tímto typem filtrování: Najít pvyužívající služby podobných společností (mimo USA), a za druhé, změna IP adresy. Způsoby zpětného filtrování jsou následující: Využití služeb podobných společností (mimo USA), změna ISP anebo použití Mirrors. [32]

### 3.5.1. Změna ISP

Jak již bylo zmíněno, základem reverzního filtrování je blokování íránských IP adres americkými společnostmi. Proto je nejlepším řešením najít internetový server, jehož IP adresy nejsou zaregistrovány ve jménu Íránu. Nově založení poskytovatelé a také stálí poskytovatelé internetu, kteří poskytují vlastní šířku pásma přes satelit nebo zahraniční společnosti, mohou být nápomocní.

Pokud nemůžete najít vhodného ISP v zemi, možná budete muset použít zahraniční ISP. Ve Windows máte přístup k seznamu poskytovatelů internetových služeb z různých zemí. Tito poskytovatelé internetových služeb jsou většinou zdarma, ale mějte na paměti, že vám bude účtován mezinárodní hovor za jejich připojení. V naléhavých případech jako jsou online platby, je rozumnější zaplatit náklady na několik minut mezinárodního volání, než risknout problémy a rizika používání veřejných proxy.

### 3.5.2. Mirrors

Pokud je problémem reverzního filtrování pouze ve stahování souborů nebo softwaru, tak je pro vás jednodušší použít Mirrory než změnit si IP adresu. Mirrory jsou kopie obsahu a souborů jedné webové stránky na jiných stránkách. Pokud vám hlavní web neumožňuje stáhnout požadovaný soubor, zkuste jej stáhnout z jiných webů. Přes filemirrors.com můžete najít vhodný Mirror.

### 3.5.3. Proxy

Proxy vytváří nepřímé spojení mezi klientským počítačem a serverem hostitelské společnosti. Pomocí proxy klient muže překonat problém reverzního filtrování. Protože v tomto případě je IP adresa klienta před hostitelskou společností skrytá a hostitelský počítač

ve skutečnosti vidí proxy IP adresu namísto skutečné IP adresy klienta a předpokládá, že klient sídlí v zemi, kde je proxy umístěn.

Pokud plánujete používat veřejné proxy servery pro citlivé úkoly, nezapomeňte zvážit bezpečnostní rizika při používání těchto serverů. Důvodem je, že můžete hackerům nebo zlodějům poskytnout důležité informace. Veřejné proxy servery se v žádném případě nedoporučuje pro důležité úkoly jako jsou internetové platby.

Pro citlivé kroky, jako například vložení informací o kreditní kartě, používají protokol zabezpečeného připojení nebo šifrované protokoly (SSL) a měli byste použit HTTPS nebo Socks proxy. Normální proxy typu HTTP v tomto případě nemá význam použit. Většina proxy serverů také nepodporuje zabezpečené připojení a není pro tento účel vhodná.

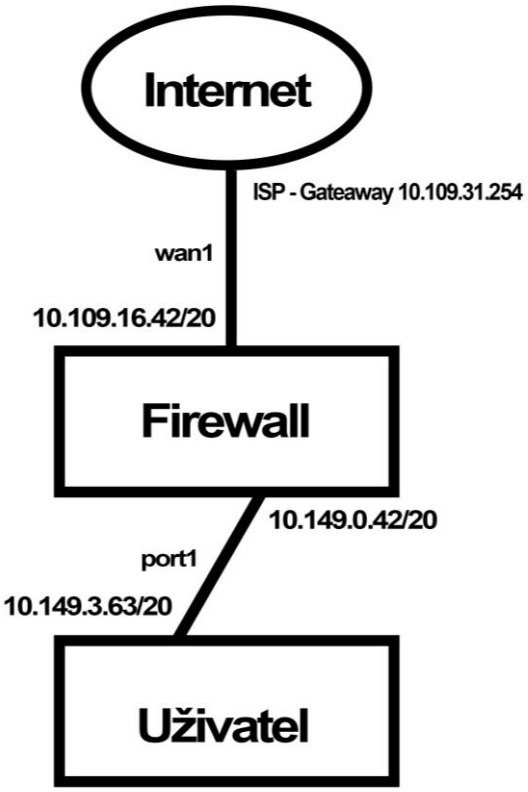
Váš proxy musí být anonymní, aby hostitelskému webu neukázal vaši skutečnou IP adresu.

Používání proxy serverů je přesně to, co hackeři a zloději používají k tomu, aby nebyli identifikovatelní. Proto jsou banky a online finanční instituce, jako je PayPal, velmi citlivé na používání proxy serverů a pokud zjistí, že pro přístup k vašemu účtu byl použit proxy nebo že na váš účet byl opakovaně přístup z různých IP adres, je možné, že Váš účet pozastaví a budete je muset kontaktovat. [33]

# 4. Aplikování technik cenzury

V poslední kapitole budu aplikovat techniky cenzury v praxi. Cílem je prokázat, jak jednoduše je možné něco cenzurovat a následně ověřit funkčnost cenzury. Pro svou práci jsem si vybral platformu FortiGate, která je primárním Fortinet produktem pro firewall a VPN a tvoří jádro zabezpečení přístupu na internet a celé zabezpečovací infrastruktury sítě. Pomocí nastaveného firewallu se pokusím cenzurovat některé webové stránky.

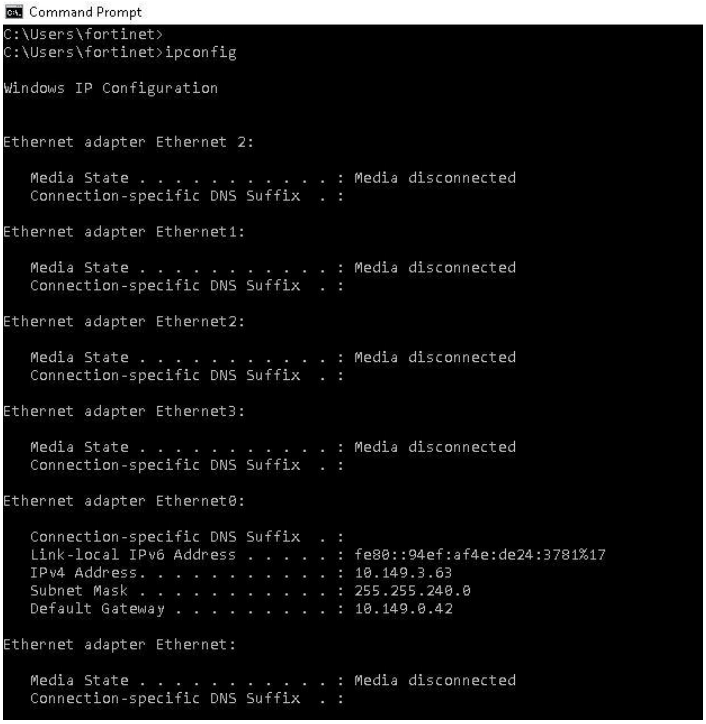
## 4.1. Ověření dostupností internetu




**Obrázek 6 – Nastavení IP adres**

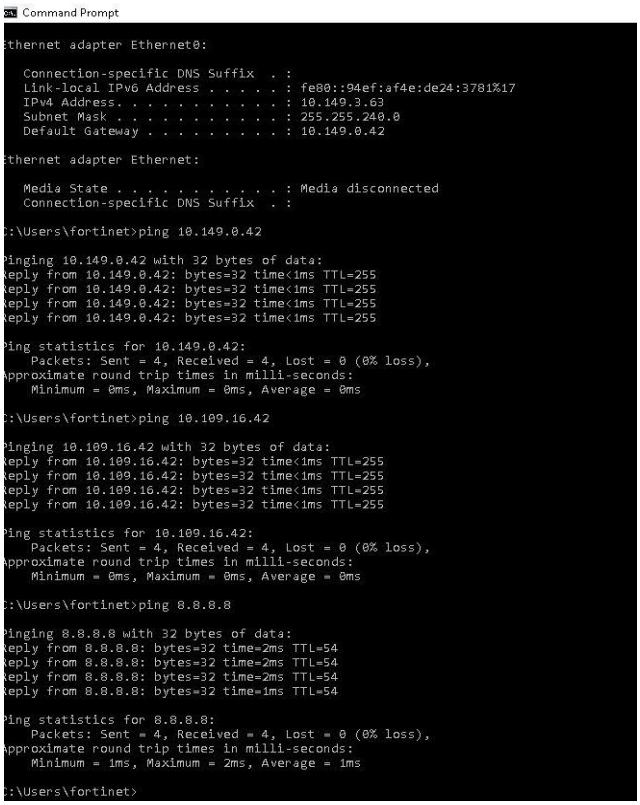
**Zdroj: autor**

V prvním kroku zjistím, zda vůbec mám internet v počítači. Otevřu si příkazový řádek (Command Prompt) a přes příkaz ipconfig, zjistím, zda mi běží internet.




**Obrázek 7 – Zjištění IP adresy**
**Zdroj: autor**

Poté přes ping ověřím funkčnost ostatních uvedených ip adres. Příkaz ping odesílal 4 pakety a přijal také čtyři pakety a žádná paketa nebyla ztracena, což znamená, že internet běží v pořádku.

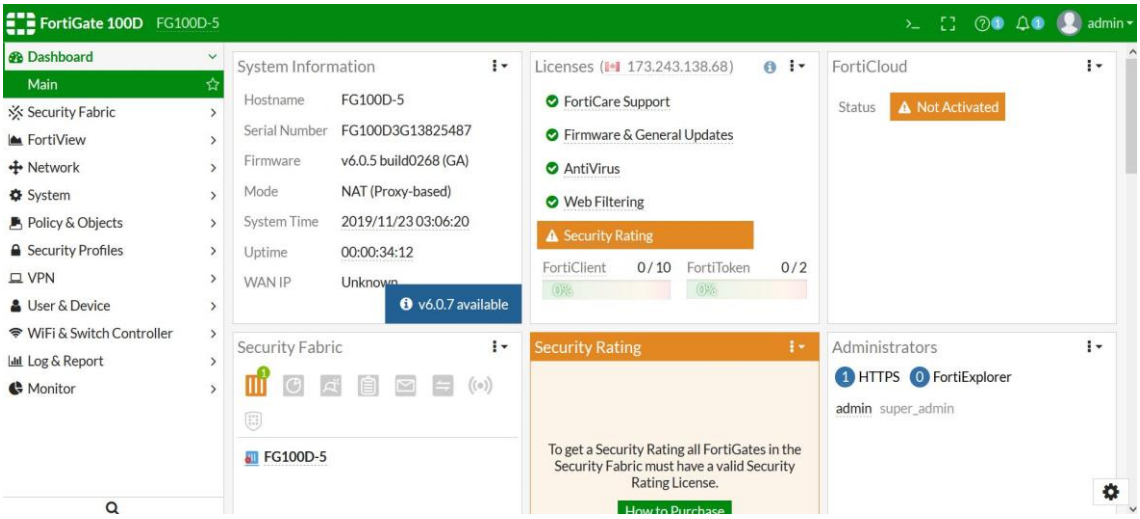



**Obrázek 8 – Zjištění dostupností internetu**
**Zdroj: autor**

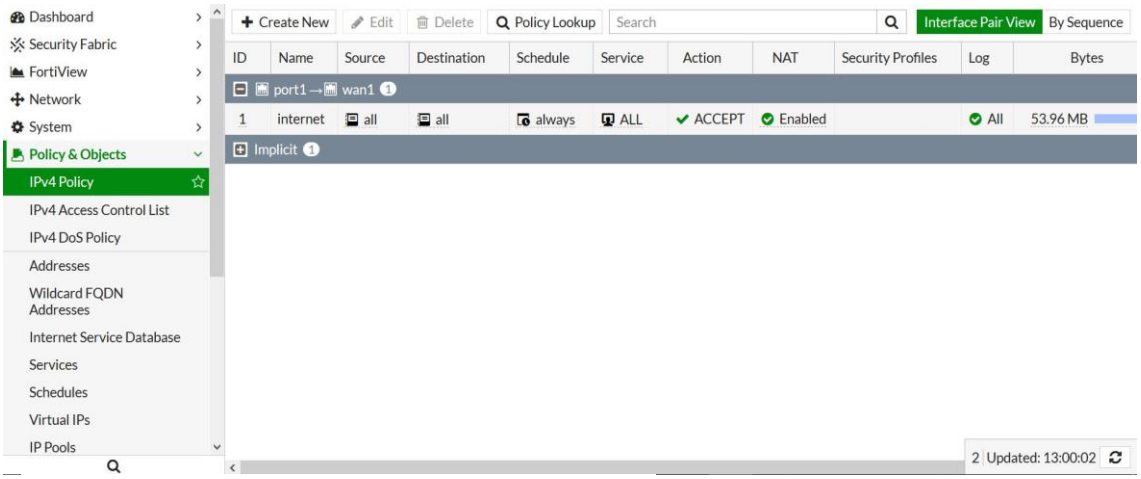
## 4.2. Nastavení Firewallu

Jak jsem již uvedl, tak pro svou práci jsem si vybral platformu FortiGate, která je z firmy Fortinet.

Proto abych mohl začít filtrovat, tak musím nejdříve vytvořit v sekci Policy & Objects nastavení, podle kterého se bude filtrovat.

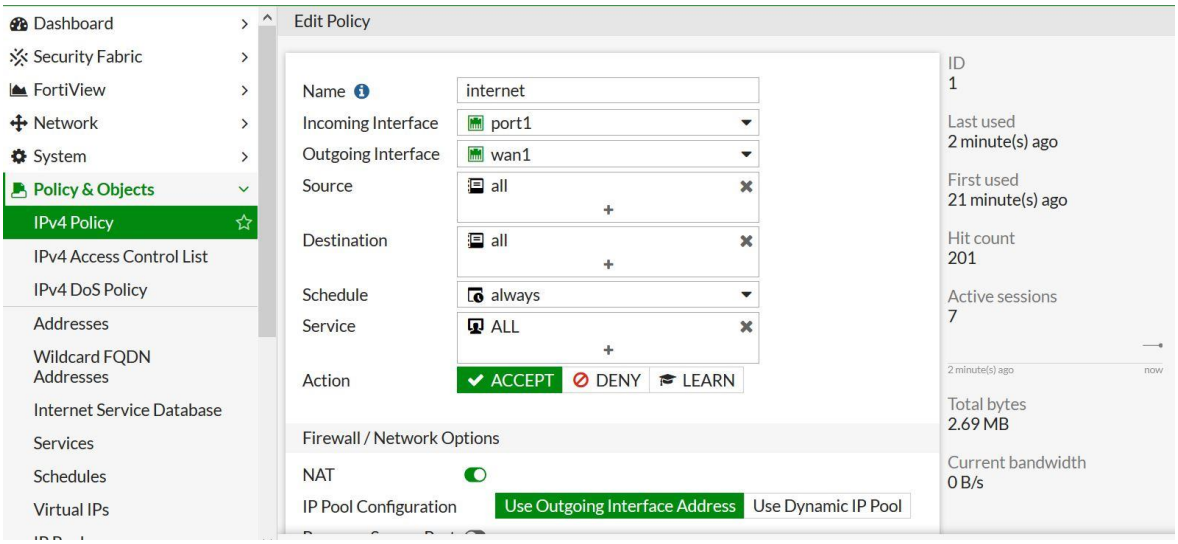



**Obrázek 9 – Hlavní menu FortiGate**
**Zdroj: autor**



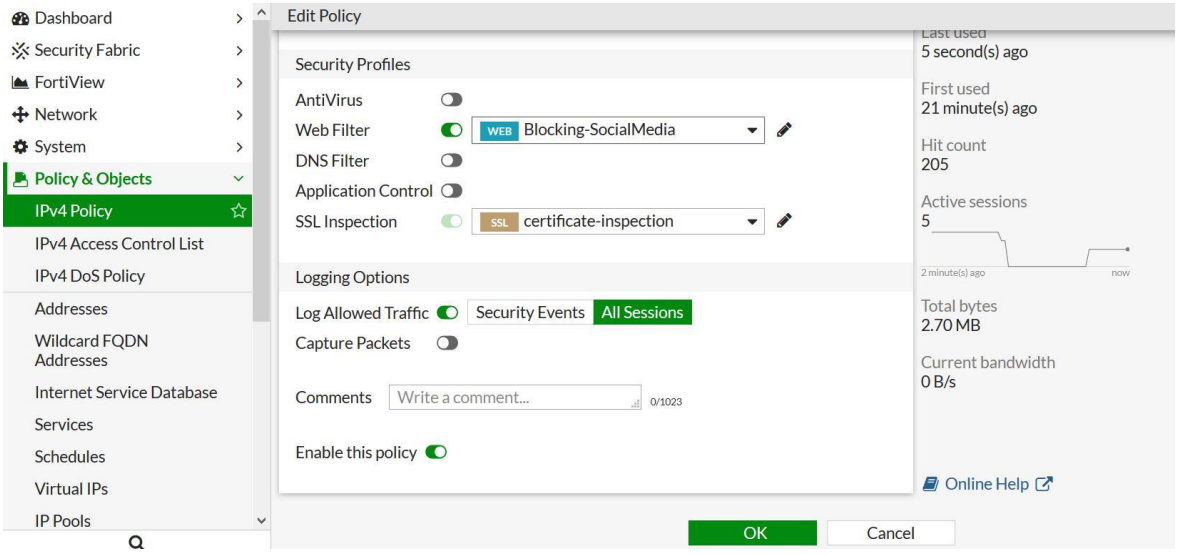

**Obrázek 10 – Nastavení policy**
**Zdroj: autor**

V sekci IPv4 Policy máme různé nastavení. Nastavil jsem příchozí (port1) a odchozí (wan1) rozhraní, které jsem si předem nadefinoval, dále je zde možnost nastavit zdroj, destinace, čas nebo období, kdy bude filtr aktivní atd. Tato nastavení jsem nechal defaultně.




**Obrázek 11 – Nastavení policy 2**
**Zdroj: autor**

Dále uživatel neboli cenzor musí vybrat, jakým způsobem by chtěl zablokovat přístup ostatních na internet. Jsou tu různé možnosti jako je Web filter, DNS filter, DLP atd. Já jsem si vybral Web Filter, kterou jsem si aktivoval níže.

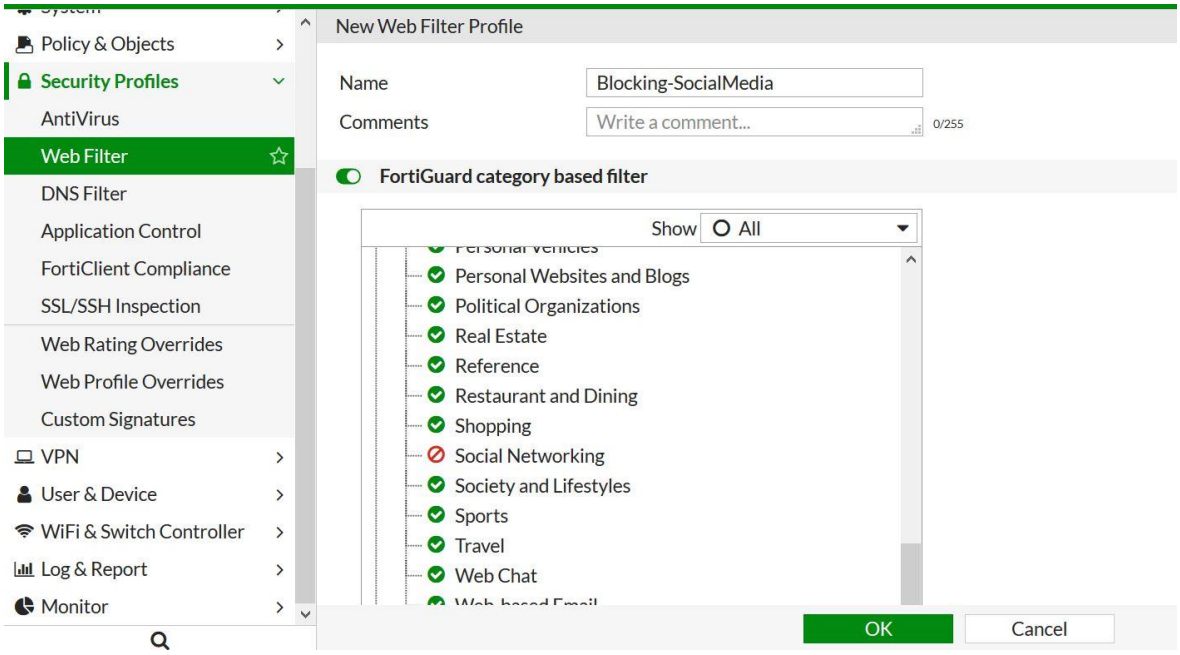



**Obrázek 12 – Nastavení policy 3**

**Zdroj: autor**

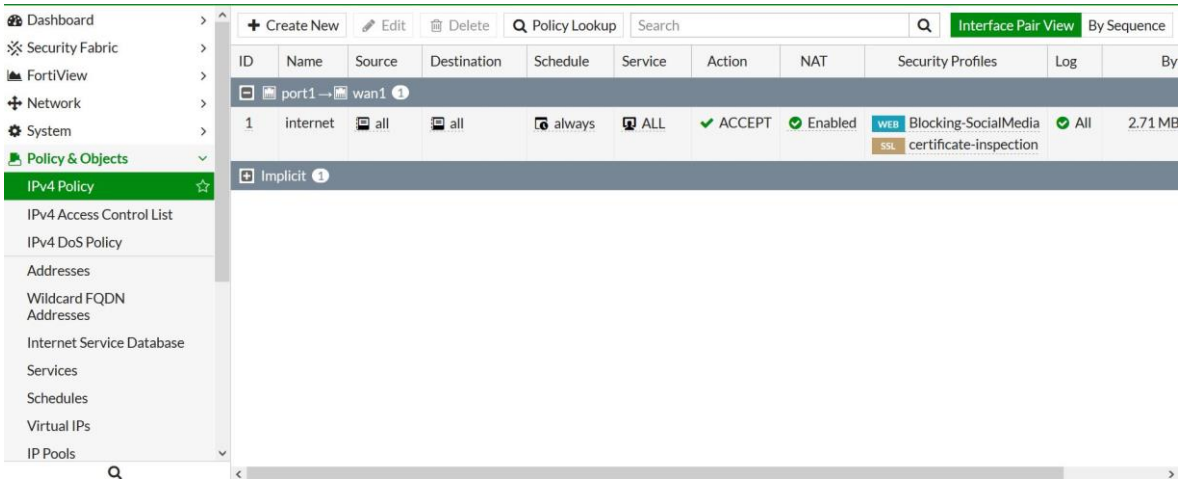
Předtím, než jsem si mohl v sekci Policy & Objects vybrat možnost Web filter, tak jsem ho musel nadefinovat v sekci Security profiles – Web filter. Zde jsem nejdříve nastavil jméno pro filtr. Dále zde musí cenzor vybrat, na jaké téma by chtěl omezit, blokovat či varovat uživatele. Vybral jsem si Social Networking, což znamená, že nepřeju, aby uživatel měl přístup na

sociální média, jako jsou Facebook a Twitter. To znamená, že uživatel při hledání takových stránek bude mít zablokovaný přístup.




**Obrázek 13 – Nastavení web filteru**
**Zdroj: autor**

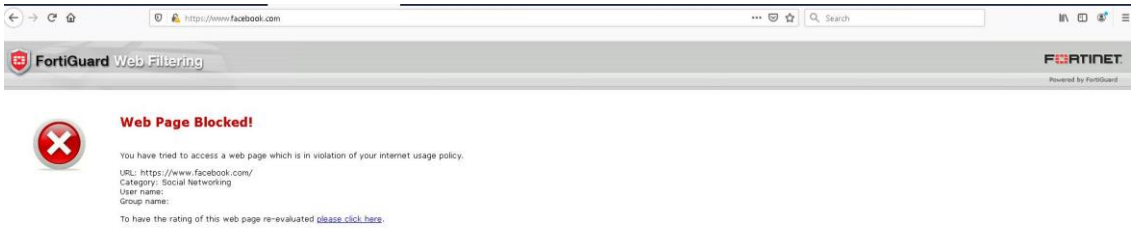
Poté, co jsem nastavil kategorii filtrování pro Web filter, tak jsem to potvrdil a následně aplikoval.




**Obrázek 14 – Aplikování policy**
**Zdroj: autor**

## 4.3. Aplikování cenzury

Pak jsem si nastavil způsob filtrovaní, aby již uživatel neměl mít přístup na webové stránky, které spadají pod kategorii Social Networking. Pro ověření funkčností web filtru jsem zkusil přejít na Facebook.com a Twitter.com. Níže je vidět, že uživatel má zablokovaný přístup.



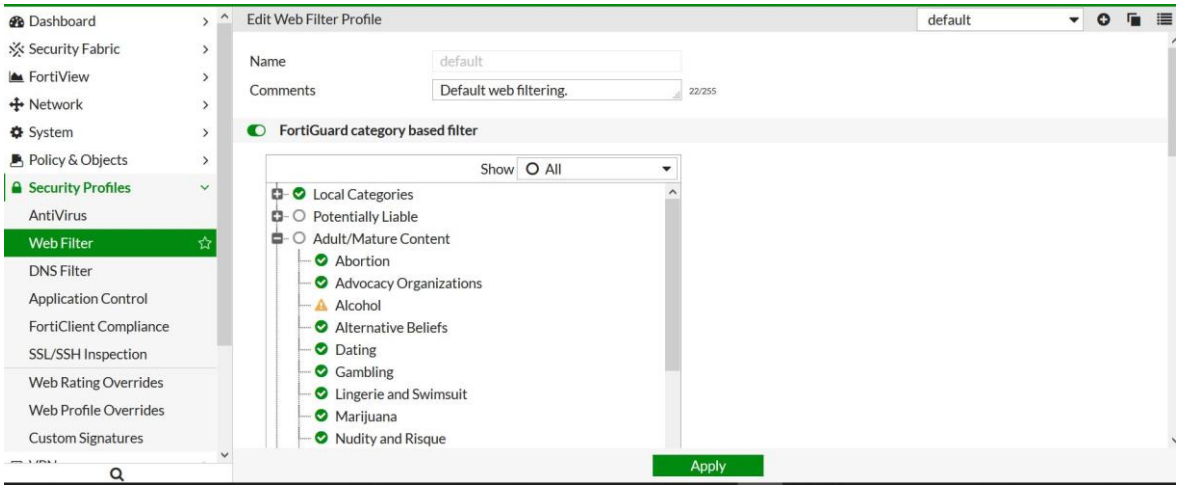

**Obrázek 15 – Nedostupný Facebook**

**Zdroj: autor**


**Obrázek 16 – Nedostupný Twitter**

**Zdroj: autor**

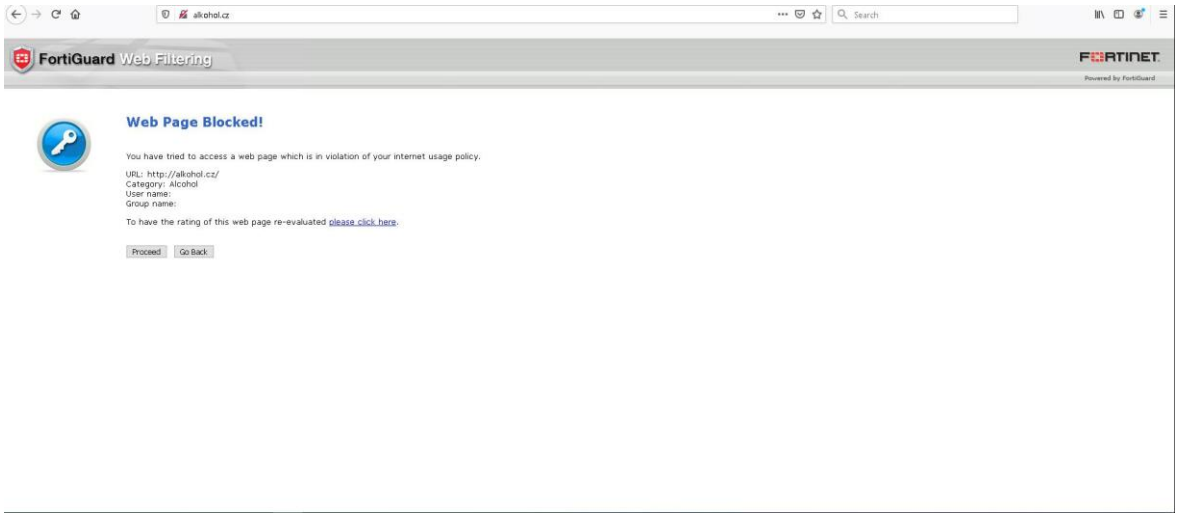
V sekci Web filteru, jak jsem již uvedl, máme různé možnosti, například můžeme blokovat, varovat nebo monitorovat. Tentokrát bych chtěl uživatele pouze varovat, že přichází na webovou stránku, která obsahuje téma alkohol.




**Obrázek 17 – Nastavení varováni na alkohol**

**Zdroj: autor**

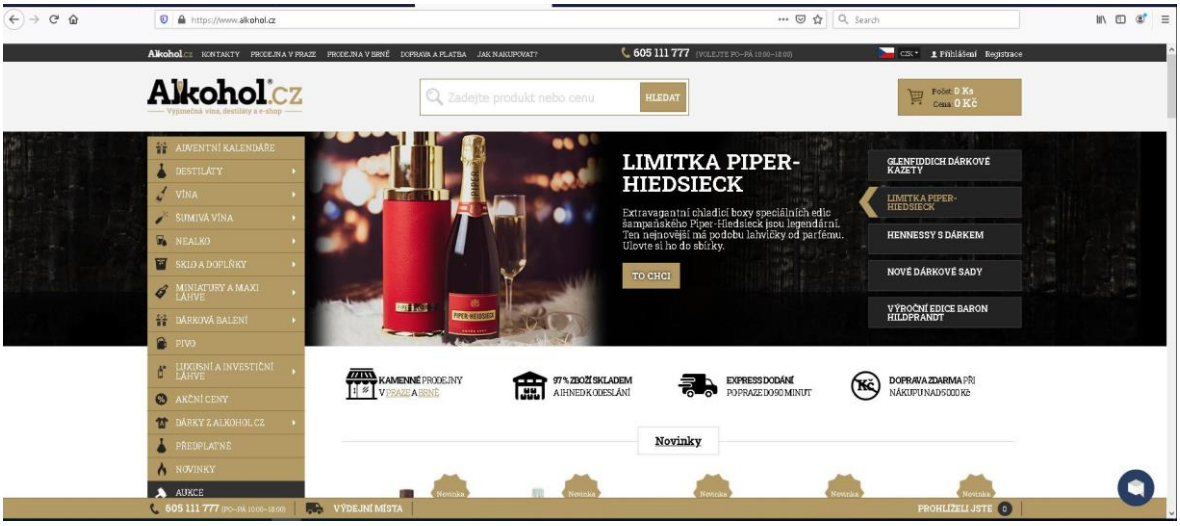
V případě, že uživatel přistoupí na webovou stránku, která obsahuje jakýkoliv téma ohledně alkoholu, tak předem dostane varovnou zprávu, že tato stránka obsahuje téma alkohol, a poté, co klikne na tlačítko Proceed, může přejít na webovou stránku.




**Obrázek 18 – Varování na alkohol**

**Zdroj: autor**

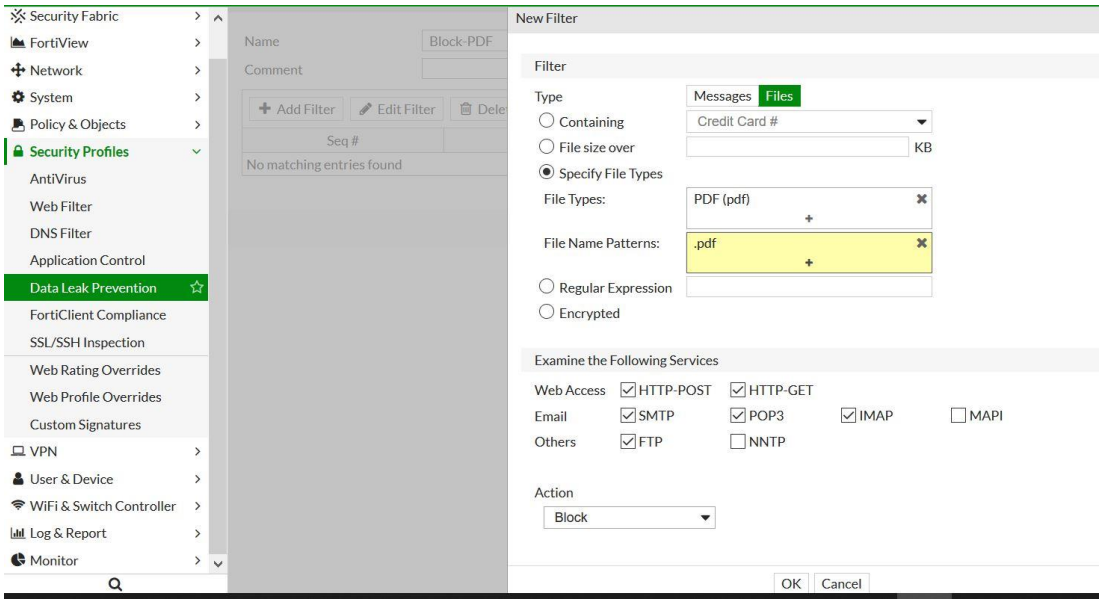
Níže je vidět, že po kliknutí na tlačítko Proceed, uživatel má bez jakéhokoliv omezení přístup na webovou stránku.




**Obrázek 19 - Webová stránka Alkohol.cz**

**Zdroj: autor**

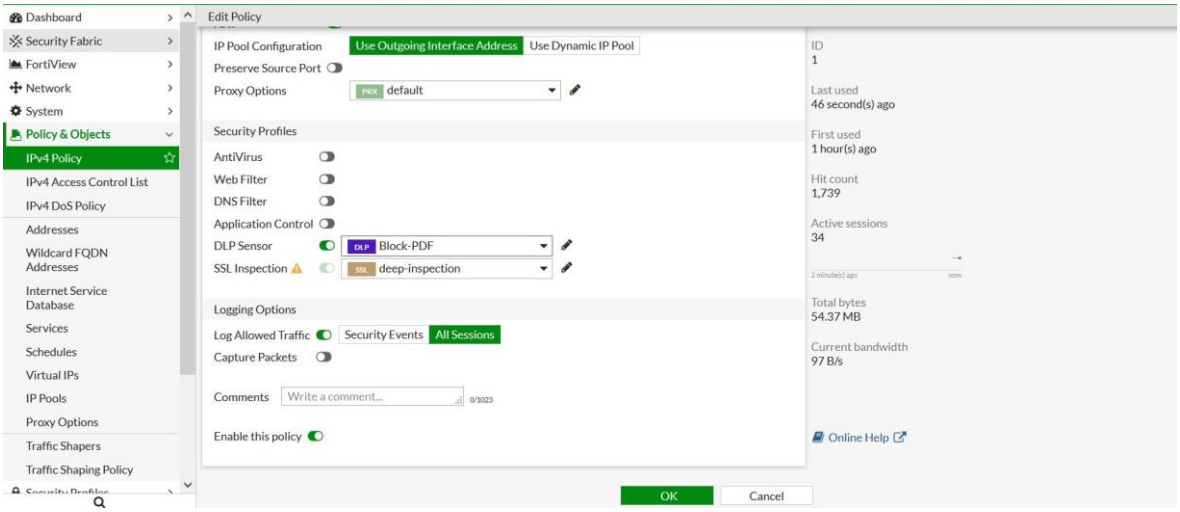
Jak jsem již výše vysvětlil, tak existují různé cesty pro blokování nebo omezení uživatele. Další cenzura, kterou jsem si vybral, je filtrování přes DLP. Zde cenzor má široký výběr, kde si může vybrat, jakým způsobem zablokuje uživatele. Zde je možnost blokovat zprávy nebo soubory. Já jsem si zvolil blokování souboru konktrétně soubor formátu PDF.




**Obrázek 20 – Nastavení DLP v policy**

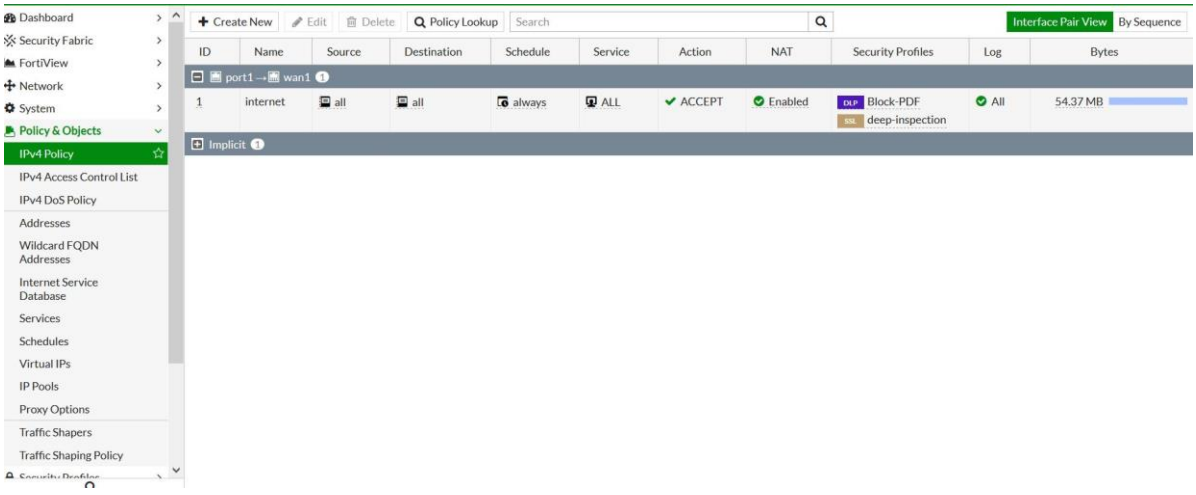
**Zdroj: autor**

Proto aby DLP filter fungoval, tak musím v sekci Policy změnit Web filter na DLP sensor, nebo také je tu možnost mít zapnuté oba druhy filtru. Dále bych chtěl, aby tato cenzura fungoval co nejstriktněji. Proto v sekci SSL inspection vybral možnost Deep inspection, což znamená, že filter se bude provádět hluboce a s větší pozornosti. V případě, že by uživatel chtěl stáhnout pdf soubor, který je schovaný v zipu, tak firewall uživatelovi také zablokuje přístup.




**Obrázek 21 – Nastavení DLP filtru**

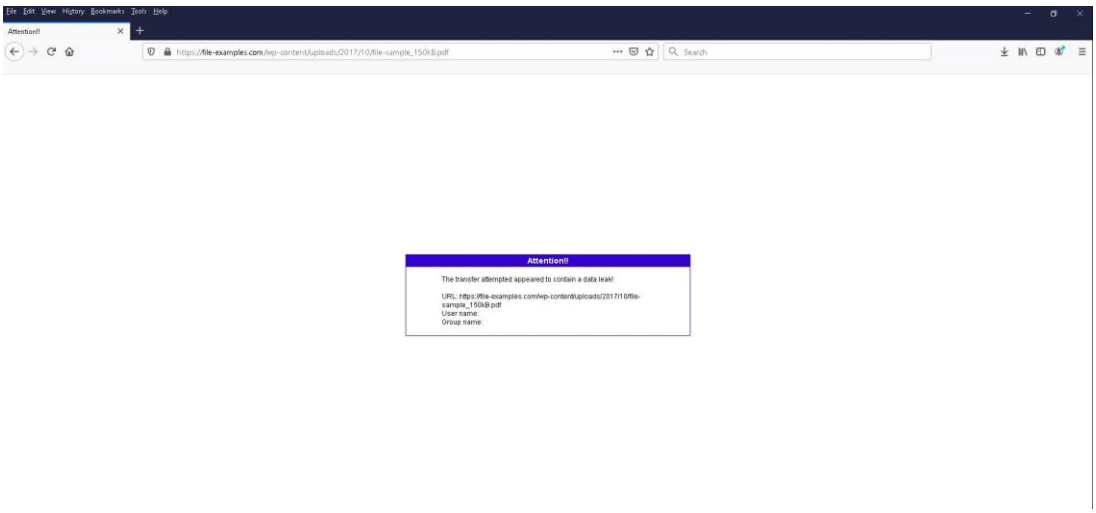
**Zdroj: autor**




**Obrázek 22 – Aplikování DLP**

**Zdroj: autor**

V případě, že uživatel by chtěl z nějaké stránky stáhnout soubor formátu pdf nebo jiný soubor, která obsahuje pdf, tak bude mít zablokovaný přístup viz. níže.



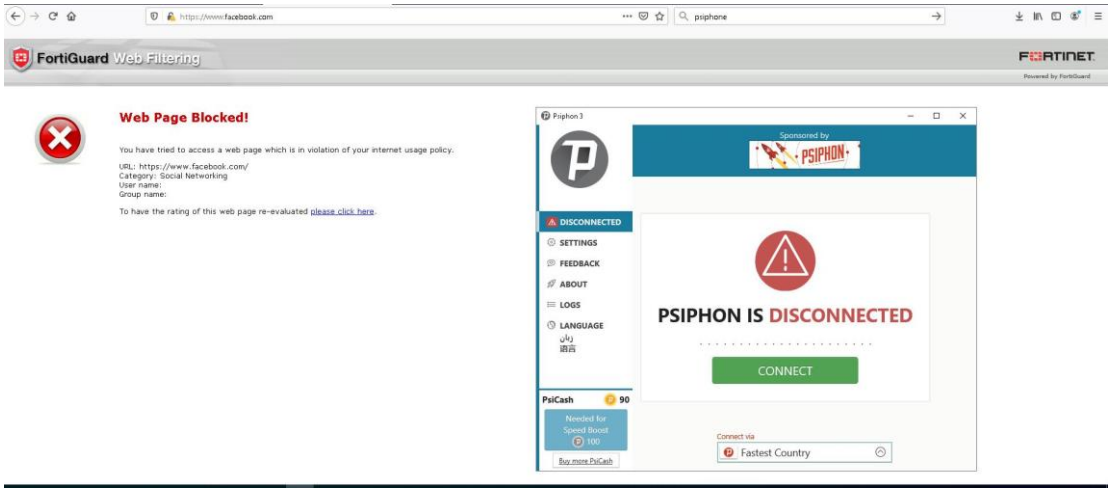

**Obrázek 23 – Nelze stáhnout pdf**
**Zdroj: autor**

## 4.4. Obcházení cenzury přes VPN

Jak jsem již v teoretické části vysvětlil, existuje mnoho cest pro obcházení cenzury. Některé jsou těžké a některé naopak lehké. Pro obcházení Web filteru jsem se rozhodl, že využiju VPN, konkrétně nástroj Psiphon, který je bezplatný a používá kombinaci zabezpečených komunikačních a zastaralých technologií (VPN, SSH a HTTP Proxy).

Po stáhnutí a nainstalování nástroje Psiphon nemusíte téměř nic dělat. Vše probíhá automaticky a vy jenom musíte kliknout na tlačítko Connect, které vás po chvíli připojí a již můžete surfovat po internetu bez omezení.

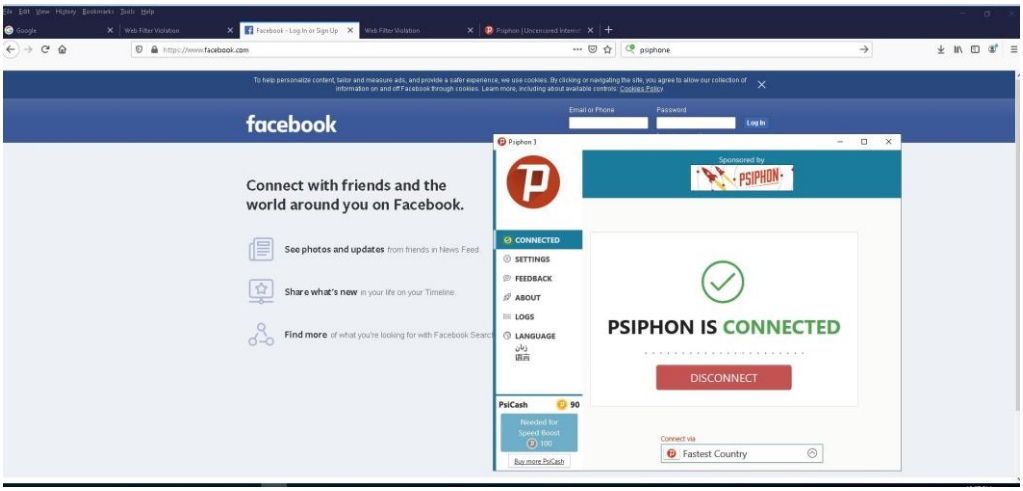
Zde je vidět, že nástroj Psiphon není připojen a uživatel má zablokovaný přístup na webovou stránku Facebook.com. Tato stránka je dle kategorie Social Networking přes Web filter blokovaná.




**Obrázek 24 – Nepřipojený Psiphon**

**Zdroj: autor**

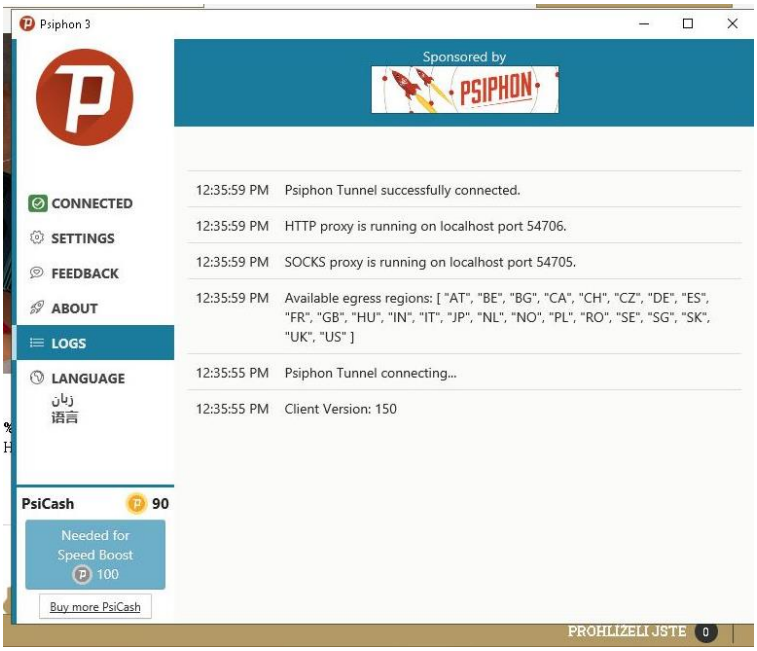
Poté, co uživatel klikne v nástroji Psiphon na tlačítko Connect, po chvilce je nástroj aktivní a uživatel může volně surfovat po internetu. Níže je vidět, že webová stránka Facebook.com, která byla blokovaná, je již volně přístupná.




**Obrázek 25 –Připojený Psiphon**

**Zdroj: autor**

V nástroji Psiphon máme možnost si nahlednout do logu a podívat se pomocí čeho nástroj obcházel cenzuru. V našem případě šlo o obcházení pomocí proxy.




**Obrázek 24 – Log nástroje**
**Zdroj: autor**

## 4.5. Shrnutí

Aplikování cenzury probíhalo pomocí platformy FortiGate. FortiGate Firewall nabízí cenzorovi mnoho způsobů, jak blokovat či omezit přístup uživatele k internetu. Byly zvoleny dva druhy cenzur. První cenzura byla přes Web filter a bránila přístup uživatele na webové stránky typu sociální média (Facebook a Twitter). Druhá cenzura byla také přes Web filter, ale tentokrát měla za úkol uživatele pouze upozornit, že přistupuje na webovou stránku, která obsahuje tématiku alkoholu. Třetí cenzura proběhla přes DLP a nedovolila uživateli stáhnout soubory, které jsou ve formátu pdf.

Obcházení cenzury probíhalo přes VPN, kde uživatel po stáhnutí VPN nástroje mohl jednoduše obejít cenzuru.

# Závěr

Bakalářská práce byla věnovaná internetové cenzuře a situaci cenzury v Íránu. Prvním krokem bylo přiblížit problematiku a příčiny cenzury. Poté jsem popisoval druhy a mechanismy, které se používají pro filtrování, následně jsem ukázal určité cesty, kterými se dá obejít cenzuru.

V praktické části jsem pro představu přiblížil způsob filtrování na webové stránky a následně ověřil i funkčnost filtru.

Cenzura internetu je závažné téma. Filtrování a cenzura informací je častá metoda kontroly informací na internetu. Jak jíž víte, tak to jsou hlavně vlády jednotlivých států, pro které je cenzura internetu prostředek politické moci. V posledních letech s rostoucí celosvětovou dostupností internetu lze očekávat i nárůst cenzury do více zemí. Metody aplikování cenzury jsou velmi účinné a dokážou znesnadnit přístup uživatele k informacím.

Možná filtrování se může zdát jako dobrý způsob znepřístupnit cestu k některým obsahům, ale bude lepší, když budeme zlepšovat naši kulturu chování než omezit komunitu. Existuje mnoho způsobů, jak obcházet cenzuru, ale toto omezení dokáže způsobit problémy jako je internetová kriminalita. Jak víte, když někoho od něčeho omezíte, tak se člověk naopak více na to zaměří a udělá pro to cokoliv, aby toto omezení překonal.

Jedinou cestou, jak zabránit cenzury, je zvýšit tlak na subjekty určující pravidla cenzury a apelovat na právo svobodného přístupu k informacím.

# Seznam použitých zdrojů

[1] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1

[2] Iranian Censorship and Internet Filtering | Welcome to Aussie24. Welcome to Aussie24 | Let's Work Together to reach FREEDOM [online]. Copyright © [cit. 28.11.2019]. Dostupné z: https://aussie24.com/education/iranian-censorship-and-internet-filtering/

[3] Iran | OpenNet Initiative. OpenNet Initiative [online]. Copyright © The OpenNet Initiative 2007. All Rights Reserved. [cit. 21.11.2019]. Dostupné z: https://opennet.net/research/profiles/iran

[4] [online]. Dostupné z: https://www.barracuda.com/glossary/web-filtering

[5] 4 Ways VPN Can Benefit Your SEO Strategy | Pole Position Marketing. Digital Marketing for Enterprise Businesses | Pole Position Marketing [online]. Copyright © 1998 [cit. 28.11.2019]. Dostupné z: https://www.polepositionmarketing.com/emp/vpn-benefit-your-seo-strategy/

[6] Co je VPN a jak funguje? Váš základní průvodce.. Avast Blog [online]. Copyright © Avast Software s.r.o. [cit. 21.11.2019]. Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje

[7] Zero-order Reverse Filtering. 403 Forbidden [online]. Dostupné z: https://arxiv.org/abs/1704.04037

[8] BBCPersian.com. BBC - Homepage [online]. Dostupné z: https://www.bbc.com/persian/science/story/2006/01/060120_fb_filtering.shtml

[9] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1

[10] What is DNS & How Does DNS Filtering Work? | Webroot. 301 Moved Permanently [online]. Copyright © Copyright 2004 [cit. 28.11.2019]. Dostupné z: https://www.webroot.com/au/en/resources/glossary/what-is-dns-filtering

[11] Proxy & Content Filtering: Definition & Examples | Study.com. Study.com | Take Online Courses. Earn College Credit. Research Schools, Degrees & Careers [online]. Copyright © copyright 2003 [cit. 28.11.2019]. Dostupné z: https://study.com/academy/lesson/proxy-content-filtering-definition-examples.html

[12] Network security: 9.4 Packet-filtering router - OpenLearn - Open University - T823_1. 302 Found [online]. Copyright ©1999 [cit. 28.11.2019]. Dostupné z: https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-9.4

[13] Data leak prevention. Fortinet Online Help [online]. Copyright © [cit. 28.11.2019]. Dostupné z: https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-security-profiles-54/DLP/dlp_chapter.htm

[14] What is censorware? - Definition from WhatIs.com. Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia [online]. Dostupné z: https://whatis.techtarget.com/definition/censorware

[15] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1

[16] [online]. Dostupné z: https://www.my-proxy.com/blog/proxy-port-proxy-type

[17] Blacklisting - Wikipedia. [online]. Dostupné z: https://en.wikipedia.org/wiki/Blacklisting

[18] xpcom - What is whitelist and blacklist data? - Stack Overflow. Stack Overflow - Where Developers Learn, Share, & Build Careers [online]. Dostupné z: https://stackoverflow.com/questions/1453285/what-is-whitelist-and-blacklist-data

[19] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1

[20] 400 Bad Request. HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#4.1

[21] [online]. Dostupné z: http://www.zensur.freerk.com/#4.2

[22] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1

[23] CacheBrowser: Bypassing Chinese Firewall Without Proxies. infatica.io - Global Peer to Business Proxy Network [online]. Copyright © 2019 All Rights Reserved. Infatica Pte. Ltd. [cit. 28.11.2019]. Dostupné z: https://infatica.io/blog/cachebrowser-bypassing-chinese-firewall-without-proxies/

[24] How to bypass P2P block? - Use a P2P VPN to bypass torrent block!. Best VPN UK 2019: Your definitive guide for the best UK VPN service [online]. Copyright ©2015 [cit. 28.11.2019]. Dostupné z: https://thebestvpn.uk/bypass-p2p-block/

[25] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1
[26] Základní stavba a funkce místních sítí | Kevin Computers. Kevin Computers, Kevin, Computers, Computer [online]. Copyright © [cit. 28.11.2019]. Dostupné z: http://kevincomputers.4fan.cz/?page_id=703
[27] How to Setup a Proxy Server. The Tech-FAQ [online]. Copyright © [cit. 28.11.2019]. Dostupné z: https://www.tech-faq.com/how-to-setup-a-proxy-server.html
[28] HOWTO bypass Internet Censorship, a tutorial on getting around filters and blocked ports [online]. Dostupné z: http://www.zensur.freerk.com/#1.1
[29] How to Setup a Proxy Server. The Tech-FAQ [online]. Copyright © [cit. 28.11.2019]. Dostupné z: https://www.tech-faq.com/how-to-setup-a-proxy-server.html
[30] PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List. PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List [online]. Copyright © 2001 [cit. 21.11.2019]. Dostupné z: http://www.proxyblind.org/
[31] PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List. PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List [online]. Copyright © 2001 [cit. 21.11.2019]. Dostupné z: http://www.proxyblind.org/
[32] 302 Found. 302 Found [online]. Dostupné z: https://www.cacheguard.com/index.php/reverse-proxy/
[33] PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List. PROXY SERVER: Free Anonymous Proxy List, Hide IP Address - WEB Proxy List [online]. Copyright © 2001 [cit. 21.11.2019]. Dostupné z: http://www.proxyblind.org/