# איך ליצור שכבת אנונימיות לבית ע"י בידוד מערכות ורשת TOR

מאת עדן ברגר

## הקדמה

בדומה לרשת ה-WWW או ל-"Clearnet", TOR הינה רשת לכל דבר, והיא נועדה לספק אנונימיות ע"י שליחת חבילות המידע בין רשת מחשבים לפני הגעתן ליעד - לדוגמה שאילתת חיפוש אל השרתים של גוגל.

אפשר לדמות את TOR להלבנת הון מהבחינה שככל שהכסף עובר יותר ידיים ככה יהיה קשה יותר לאתר את מקורו, במקרה של TOR, נראה כי שלוש ידיים זה מספיק. TOR יצאה לאור בשנת 2002 ולתקופה מאוד ארוכה הייתה איטית ולא ניתן היה להסתמך עליה בשביל גלישה יומיומית.

בשנים האחרונות תחום האנונימיות צמח בהרבה, למיטב הבנתי, בעקבות הצעדים העיקריים:

- בזכות הפיתוח של התוכנה Vidalia שמציגה באופן גרפי את החיבור אל רשת TOR.
- השילוב של Vidalia עם פיירפוקס שיצא תחת השם החדש TORBrowser.
- זרקורי המדיה פנו אל אידיאולוגיית אנונימוס וציינו שהקבוצות האנונימיות משתמשות ברשת TOR או בכנויה: "ה-Darknet", בשביל לבצע את המחאות שלהן, לאחר מכן גם TOR נשארה בכותרות בזכות האתר Silkroad שהתפרסם מהמוצרים היחודיים שלו.

המדיה הציגה את אותן הקבוצות והמעשים שלהן, אך לא דאגה להסביר את האידיאולוגיה שעומדת מאחוריהן. מאוד בקצרה: מדובר בזכות להיות לא מנוטר בפעולות אינטרנטיות ע"י הממשלות, וכחוק גלובלי לכל קבוצת האקרים אנונימית לחתום את שמה כ-Anonymous בשביל להקשות על הזיהוי, זו גם הסיבה שאי אפשר להכליל אותן, לדוגמה: קבוצות אנונימוס שונות שתוקפות את הודו וגם את פקיסטן. הקבוצות בדר"כ מחפשות צדק וחופש לפי הזווית ראייה שלהן, אם זה למען הכלל ולא מלחמה עם מדינה, אז הם יקראו Hacktivist-ים, שהם לרוב מגנים על עוד זכויות, כמו חופש המידע (פגיעה בזכויות יוצרים, WhistleBlowers וכו').

בזכות גידול המשתמשים והטכנולוגיה החדישה כיום אפשר לצפות ב-Streaming בנוחות של בערך 200KB.

## הבעיה והפתרון

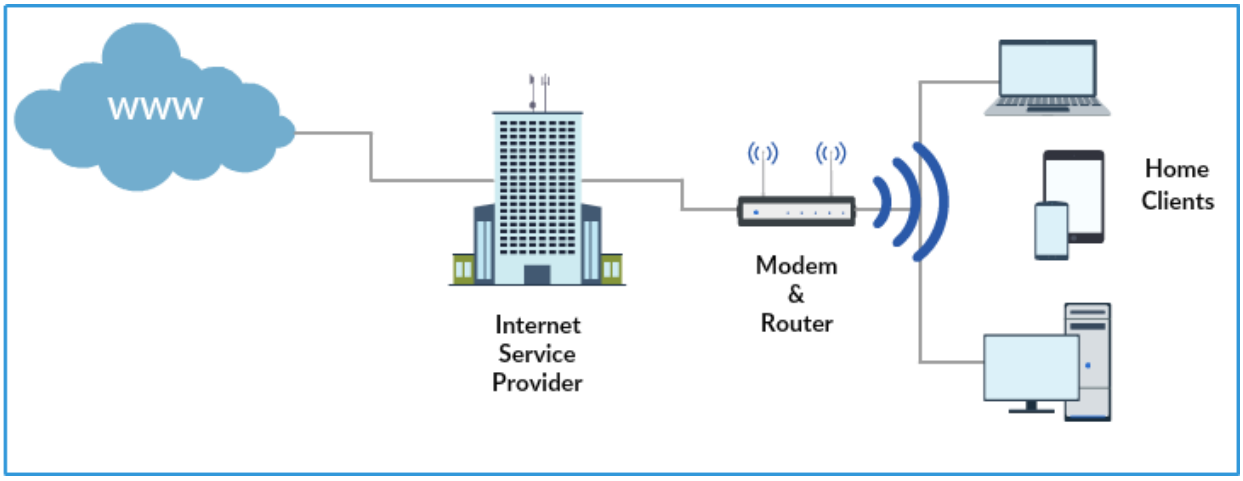
כעת, ניקח מצב שבו אנחנו מתקינים TOR על מערכת ההפעלה שלנו ומגדירים את הדפדפן המועדף עלינו להעביר את התקשורת שלו דרך ה-Proxy המקומי אל TOR, במצב כזה, אנו מיד ניצבים בפני שלוש בעיות אנונימיות:

- ה-Useragent של הדפדפן חשוף.
- תוכנות ושירותים שמותקנים במחשב לאו דווקא מוגדרים לעבור דרך הפרוקסי המקומי של TOR.
- קיים קוד JavaScript המסוגל ליצור חיבור ישיר עם המחשב וככה לגלות את האייפי האמיתי או לקרוא מאפיינים נוספים מהדפדפן.

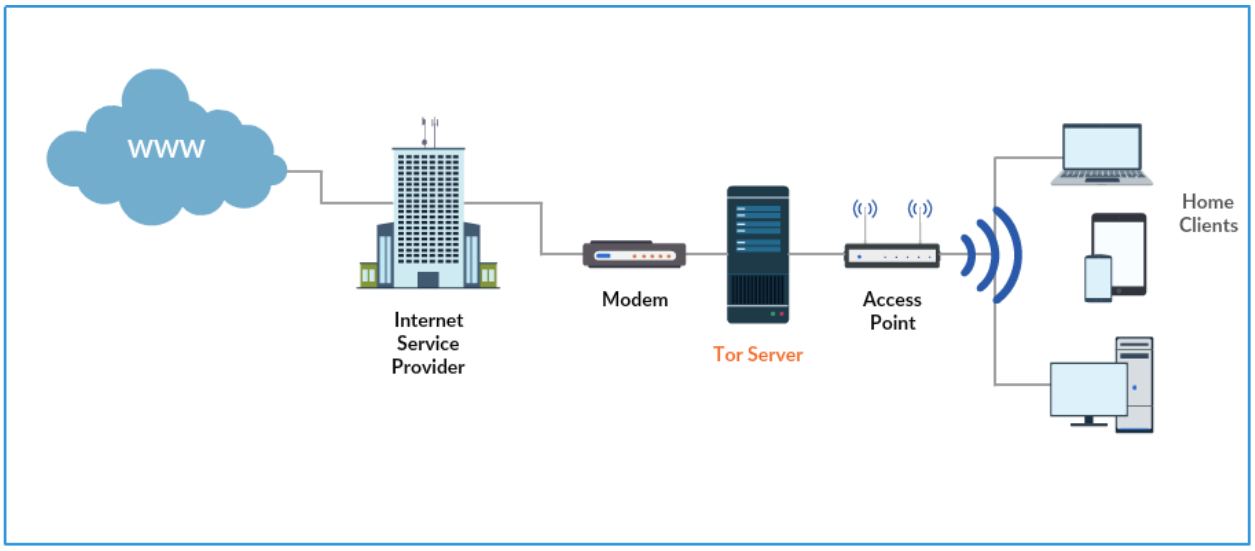
בשביל לפתור את בעיות האנונימיות האלו נפתחו מספר פרויקטים, TailsOS לדוגמה היא מערכת מבוססת דביאן שמטרתה היא להתחבר אל TOR ולהעביר את תעבורת המחשב לשם, ולהזהיר אותך לפני שאתה שולח מידע ישיר אל רשת ה-ClearNet.

בנוסף נפתחו גם הפרויקטים TorVM ו-Whonix, שמהם נצטרך לבחור ונרחיב עליהם בהמשך. אני הולך להציג כאן מימוש של ניתוב מידע מהרשת הבייתית אל רשת TOR, כך שלא יהיה צורך בהתעסקות בטלפונים או עם מחשבי המשתמשים.

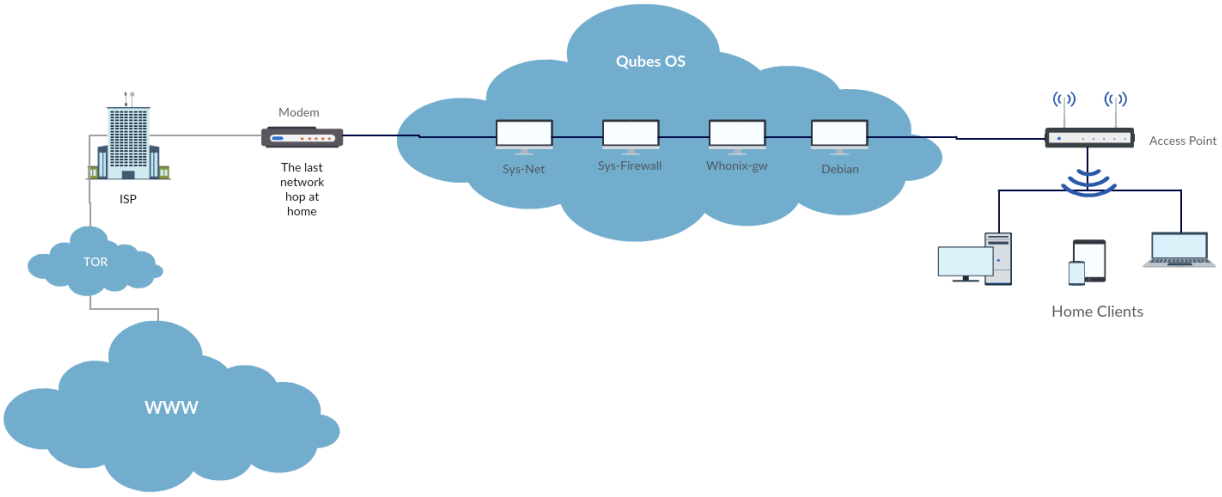
רשת בייתית נראת (בדרך כלל) כך:



לאחר שנרכיב את הפתרון שלנו, אותה רשת בייתית, תראה באופן הבא:




על ה-TOR Server נתקין מערכת ניהול וירטואליזציה בשם QubesOS. ומתחתיה את המערכת האנונימית Whonix בהמשך אפרט על שתי מערכות ההפעלה. מערך בשילוב עם מערכות ההפעלה יראה כך:




- נחבר את המודם אל המערכת sys-net.
- את ה-AP נחבר אל המכונת Debian.
- מכונת ה-Debian תספק ל-AP אינטרנט.
- שאר המחשבים יתחברו אל ה-AP, המידע של כולם ינותב דרך רשת TOR ללא צורך בהתעסקות נוספת, ונוכל למנוע DataLeaks למניהם.

## תיכנון ראשוני

הדברים שנצטרך הם:

- שני ראוטרים או מודם אחד ו-switch אחד
- מחשב יעודי עם שני חיבורי רשת, Onboards או אחד חיצוני

בנוסף, חשוב לי להדגיש כי אני לא שם דגש על אבטחת מידע או על אנונימיות מוחלטת מכיוון שהנושא רחב מדי לסקר במסמך, אלו לינקים אל עמודי הבית של המערכות להמשך קריאה ונקודות בסיסיות:

1. בשביל לוודא שהמערכות הפעלה והעדכונים שלהן תקינים, נבצע בדיקת אמינות בעזרת GPG.
2. בהנחה שזו הרשת של הבית והמכשירים מחוברים, המון מידע אישי עובר, לדוגמה מהאפליקציות שמותקנות על הטלפונים (facebook).
3. כל מערכת שאנחנו מתקינים חשוב לשנות את הסיסמה של היוזר root והיוזר user.
4. עוד המון מידע מעניין על אבטחה ואנונימיות בדוקומנטציה של QubesOS ו-Whonix.

- www.qubes-os.org/doc
- www.whonix.org/wiki/Documentation

המערכות הפעלה שהשתמשתי בהן הן:

- www.qubes-os.org
- www.whonix.org
- www.ddwrt.com

חשוב להבין את שמות הכתובות ברשת TOR, אם הלינק שאנחנו עכשיו בתוכו מכיל קוד hash ארוך ולא מובן ומסתיים ב-onion. סביר להניח שאנחנו גולשים באתר שיושב בתוך רשת TOR, ולאנשים הגולשים ב-Clearnet אין route בשביל להגיע לאותם האתרים. ישנם אתרי proxy לגלישה אל תוך רשת TOR.

### Qubes OS

Qubes הינה סביבת וירטואליזציה, היא מיועדת לספק אבטחה ע"י הפרדה, היא משתמשת בטכנולוגיית xen לווירטואליזציה, וכאשר נתקין ונפעיל אותה לראשונה, יהיו מולנו שלוש מערכות הפעלה וירטואליות מבוססות פדורה:

- **DOM0** - אחראית על ניהול המשאבים (זכרונות ומעבד) ועל יצירת מערכות וירטואליות חדשות, חוץ מעדכונים, אין למערכת גישה לאינטרנט.
- **Sys-net** - מערכת שהיעוד שלה הוא לנתב את תעבורת האינטרנט מהראוטר אל תוך Qubes.
- **Sys-firewall** - מספקת שכבת הגנה בין sys-net אל שאר המכונות.

בהתקנה דיפולטיבית של Qubes יגיעו איתה שלוש מערכות בנוסף:

- פרטית
- עבודה
- בנק

כל אחת כמובן עם כתובת MAC משלה ואין להן תקשורת אחת עם השנייה. ככה שנניח שנדבקתי בוירוס דרך המערכת הפרטית, אז לאו דווקא שהוירוס יצליח להדביק את שאר המערכות. ובנוסף אליהן, קיימת גם מכונה בשם DisposableVM שזו מכונה וירטואלית שנוצרת מחדש כשמפעילים אותה ונמחקת כשמכבים אותה.

### Whonix

המערכת תמיד תגיע בשתי מערכות, אחת בשם Whonix-GW ואחת בשם Whonix-WS.

- תפקידה של ה-Gateway הוא להתחבר לרשת TOR
- תפקידה של ה-Workstation הוא להעביר את תעבורת האינטרנט שלה דרך ה-Gateway, וככה אנחנו נמנע Data leaks מה-Workstation.

שיטה ממולצת ע"י היוצרים שלה היא להתקין אותה בתוך Qubes.

### Debian instead of whonix-ws

מצאתי שיותר פשוט לנתב את התעבורה ממכונת Debian מאשר מ-Whonix-ws, אני מניח שזה בגלל ההקשחה שהמערכת עברה בשביל למלא את מטרתה.

זו היא אינה הדרך המומלצת ע"י היוצרים של Whonix, אך אני חושב שהיא מספקת טוב שכבת TOR מעל מכשירים אישיים של הבית, לאנונימות מוחלטת צריך לעבוד קשה מהבית או קל מחוצה לו.

## שלב ההתקנה

המסך הראשון של שלב ההתקנה הינו בחירת שפה - לטובת שמירת האחידות עם יחידות אנונימיות כמו שלנו, בכללי כדאי להשאיר הגדרות בדיפולט. כאן אפשר להיות יצירתיים ולהחליף את השפה לסינית, או שפה אחרת בעלת קהל משתמשים רב. במסך השני, אחרי קביעת השפה אני ממליץ לשנות ב- Software selection ל-Qubes OS with Xfce בשל אי צורך ב-KDE או בשניהם יחדיו. ובנוסף - תוסיפו את ההתקנה של Debian מצד ימין, אנו נשתמש בה בהמשך.

בשלב הבא אתם מתבקשים להגדיר את סיסמת ה-root, אין לנו צורך בליצור חשבון ליוזר root, תהיה לנו גישה ל-root בעזרת:

```
[user@dom0 ~]$ sudo -i
```

לאחר שההתקנה הושלמה והמחשב אותחל מחדש, תבחרו שם משתמש וסיסמה ואת הזמן הרצוי עליכם. לאחר מכן תגיעו למסך: "Create Service VMs", אני ממליץ לבחור באפשרות השנייה:

Just create default service VMs.

האפשרות הראשונה תתקין לנו את המערכות Personal, Work ו- Banking שאנו לא נשתמש במערכות האלו כאן. והאפשרות השלישית תתן לנו מכונה ריקה.

לאחר עליית המערכת, ביחרו ב-Use default config במסך ה-Panel:

Welcome to the first start of the panel

אחרת נגדיר פאנל עליון בעצמנו.

דבר ראשון שנעשה יהיה להיכנס לטרמינל של שתי המערכות ולשנות את הסיסמאות של המשתמשים:

Qubes logo on toolbar → ServiceVM: sys-firewall → sys-firewall: Terminal

נקליד את הפקודות הבאות:

```
[user@sys-firewall ~]$ sudo -i
[root@sys-firewall ~]$ passwd
[root@sys-firewall ~]$ passwd user
```

את אותו הדבר נעשה גם ל-Sys-net ולכל שאר המכונות שנתקין.

כעת, ניגש להתקין Template של Whonix-gw. בטרמינל של dom0, נקליד:

```
[user@dom0 ~]$ sudo -i
[root@dom0 ~]$ qubes-dom0-update --enablerepo=qubes-templates-community qubes-
template-whonix
[root@dom0 ~]$ exit
```

אחרי שההורדה הסתיימה, אנחנו יכולים ליצור את שתיהן:

```
[user@dom0 ~]$ qvm-create -l purple gw --proxy --template=whonix-gw
[user@dom0 ~]$ qvm-prefs -s gw netvm sys-firewall
```

ו:

```
[user@dom0 ~]$ qvm-create -l gray ws -template=debian-8
[user@dom0 ~]$ qvm-prefs -s ws netvm gw
```

השלב הבא יהיה להוריד מ-Sys-net את אחד מה-Interfaces שהתווסף אליה (בהנחה שבחרנו ב-Create default service VMs) בשלב ההתקנה.

מ-dom0:

```
[user@dom0 ~]$ qvm-pci -l sys-net
[user@dom0 ~]$ lspci |grep Eth
```

כעת ננסה למחוק אחד מהכרטיסים (לא ניתן להבדיל איזה מהם, אנחנו אמורים למחוק ע"פ הפלט של qvm-pci וlspci) ונבדוק אם יש למכונה אינטרנט. אם אין אינטרנט סימן שהוצאנו את הכרטיס השגוי, אז נוסיף אותו בחזרה ונמחק את השני.

נכבה את כולן בשביל שנוכל לערוך את רכיבי החומרה שלהן:

```
[user@dom0 ~]$  qvm-shutdown -all
```

נמחק מ-Sys-net את ההתקן (06:00.0 זו דוגמה מהמחשב שלי):

```
[user@dom0 ~]$  qvm-pci -d sys-net 06:00.0
```

ונוסיף אל המכונה שתהיה מקושרת אל ה-AP:

```
[user@dom0 ~]$  qvm-pci -a ws 06:00.0
```

ונדליק אותן בחזרה:

```
[user@dom0 ~]$  qvm-start sys-net
[user@dom0 ~]$  qvm-start sys-firewall
[user@dom0 ~]$  qvm-start gw
[user@dom0 ~]$  qvm-start ws
```

דבר מעניין שטוב לדעת: במערכות בתוך Qubes, אחרי כל ריסטרט המערכת חוזרת להגדרות הראשוניות שלה ומוחקת קבצים וערכים חדשים, הדרך בה מוסיפים למערכת הגדרות היא ע"י הוספת סקריפטים וחבילות אל תיקיית /rw/.

כעת ניצור את הסקריפט שיכין את ההגדרות רשת בזמן עליית המערכת, בחלון טרמינל של WS נקליד:

```
user@ws:~$ sudo -i
root@ws:~# cd /rw/config
```

ונערוך את rc.local בעזרת העורך טקסט המועדף:

```
root@ws:~# nano rc.local
#!/bin/bash
```

נוסיף הגדרות לנוחות:

```
# Aliases
echo 'alias ls="ls --color"' >> /etc/bash.bashrc
echo 'alias ll="ls -l"' >> /etc/bash.bashrc
```

נשנה את ההגדרות של ה-Interface שמחובר אל ה-AP:

```
# Etherenet & IP.
/sbin/ifconfig eth1 192.168.0.1 netmask 255.255.255.0

# Fails if run more than once
set +e
/sbin/route add -net 192.168.0.0 netmask 255.255.255.0 gw 192.168.0.2
set -e
echo 1 > /proc/sys/net/ipv4/ip_forward
```

נשחזר הגדרות שהגדרנו מראש ל-IPTables:

```
# Iptables
/sbin/iptables-restore -c < /rw/config/rules.iptables
```

וכאן נסיים עם הסקריפט.

השתמשתי בסט פקודות הבא (שימו לב שזה ימחוק את טבלאות ה-IPTables):

```
root@ws:~# iptables -F
root@ws:~# iptables -t nat -F
root@ws:~# iptables -table nat -append POSTROUTING -out-interface eth0 -j
MASQUERADE
```

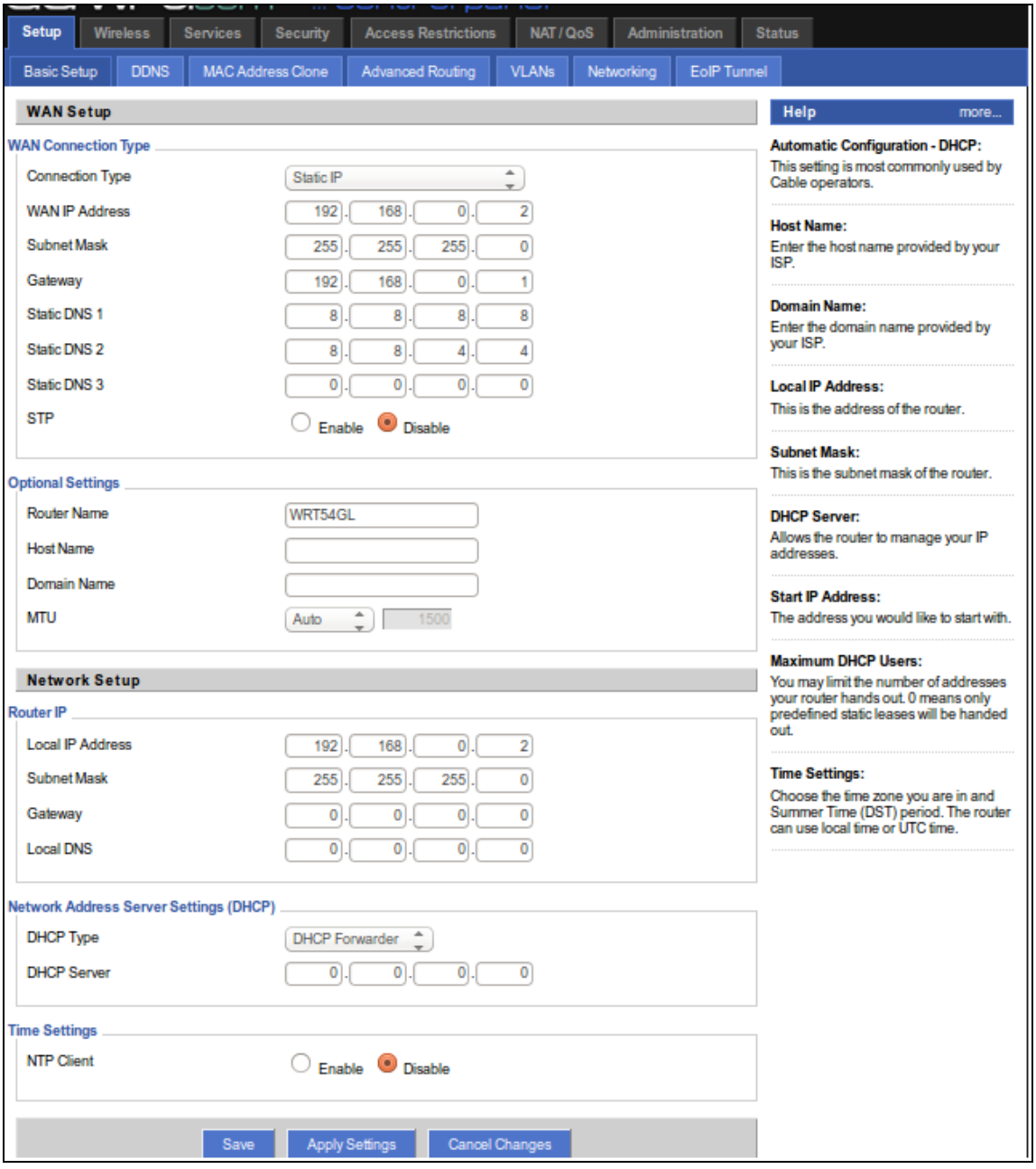
על מנת שנוכל לייצא אל הקובץ בעזרת iptables-save, נקליד:

```
root@ws:~# iptables-save > /rw/config/rules.iptables
```

בשלב הזה TOR Server צפוי לחכות לתעבורה, עכשיו נשאר לנו להגדיר את ה-AP, יש לנו שתי אפשרויות עיקריות:

- ה-AP משמש כ-Switch ולשם כך נצטרך להתקין DHCP על TOR Server, לינק להתקנת dhcp ב-Debian למטה.
- ה-AP משמש כ-Router ומחלק כתובות עם DHCP, נצטרך להגדיר לו את יציאת ה-WAN בתור IP סטטי באותו ה-Subnet עם TOR server.

הגדרות ה-switch שהשתשמתי בהן מופיעות בתמונה הבאה:



## סיכום

בחרתי להשתמש ב-QubesOS בשילוב עם Whonix מפני שכשהתחלתי לחקור את הנושא זה הפתרון המלא הראשון שהכרתי. את אותו הפתרון אפשר לממש בדרכים אחרות, לדוגמה - RaspberyPi עם כרטיס Ethernet נוסף. יתרון טוב בלהשתמש ב-QubesOS הוא הקלות להוסיף הגנה על הרשת הבייתית עם Snort שירחרח את התעבורה, להוסיף מכונת Honeypot או להתקין קושחת חומת אש וירטואלית במקום Sys-firewall.

זו היא דרך אחת לממש נתב אל רשת TOR על שרת יעודי, את Whonix-gw אפשר להתקין גם על VirtualBox לדוגמה, או להחליף ב-TorVM בקלות לפי המדריך הזה:
www.qubes-os.org/doc/privacy/torvm

**מה עושים ב-TOR?**

דבר ראשון יהיה לבחון את Hidden Wiki, אתר וויקיפדיה שאנשים אנונימים מפרסמים לינקים אל האתרים שלהם, עם תקציר לאיזה סוג שירות הם מציעים, יש שם מגוון מאוד רווח ומעניין של השירותים שאנשים מציעים. בנוסף ל-Hidden Wiki ישנם גם מנועי חיפוש בתוך רשת TOR, עם מגוון של כתובות אתרים.

אפשר לכוון יותר ממכונה אחת להעביר את המידע שלה דרך Whonix-gw, לדוגמה מכונת Whonix-ws או את ה-DisposableVM.

אני מקווה שנהנתם, כמובן שלא סיקרתי את כל הנושא ככה ששאלות, תהיות, הארות והערות יתקבלו בברכה כאן בתגובות או בכתובת האימייל: eden@edenberger.io

## לינקים

**Routing:**

- https://wiki.debian.org/DHCP_Server
- https://openwrt.org

**Switch:**

- http://www.dd-wrt.com/wiki/index.php

**TORcheck:**

- https://check.TORproject.org

**Copy to dom0:**

- https://www.qubes-os.org/doc/copy-to-dom0