

Esarettten Kaçış

written by Mert SARICA | 1 April 2019

If you are looking for an English version of this article, please visit [here](#).

Yıllarca internet servis sağlayıcılarının ADSL modemini kullanmış ve bunlar üzerinde yapmış olduğum güvenlik araştırmaları (Hediye Modemler Ne Kadar Güvenli? , Donanım Yazılımı Analizinin Önemi) ile bilgi güvenliği farkındalığını arttırmaya çalışmış biri olarak hediye modem kullanmaya bireysel olarak sıcak baktığımı pek söyleyemem. Bunun başlıca nedenlerinden bazılarını sayacak olursam; modemlerde internet servis sağlayıcıları tarafından kullanılan gömülü kullanıcı hesaplarının herkes tarafından öğrenilebilmesi ve son kullanıcının modem'in/yönlendiricisinin yönetim sayfasını internetten erişime açması durumunda başkaları tarafından kötüye kullanılabilmesi, donanım yazılımının (firmware) özel sürüm olması sebebiyle son, en güvenli sürüme güncellenmemesi, bağlantı kısıtlamasının (firewall) her bağlantı noktası (port) için yapılamaması, kısıtlı yönetim sayfaları diyebilirim.

Yaklaşık iki yıl önce evime fiber internet altyapısının gelmesi ile birlikte ADSL modemin yerini yönlendirici (router) aldı. Internet servis sağlayıcımın kullanmaya zorunlu tuttuğu Tilgin marka, kendi web sitesinde dahi adı sanı bulunmayan HG1332 model yönlendirici ile internetten aldığım keyifli günler yerini esarete bıraktı. Vasat ötesi WiFi sinyal gücü, 7 yıl önce yönlendiricilerin desteklemeye başlayıp günümüzde sıradan hale gelmiş OpenVPN desteğinin olmaması, modern güvenlik dünyasının şifreli dns iletişimini (DoH) desteklememesi, dinamik dns (DDNS) desteğinin oldukça sınırlı olması gibi bir çok olumsuz neden sayabilirim.

Bu yönlendirici ile kısa süreli mutsuz bir beraberlikten sonra internet servis sağlayıcımıyla yönlendiriciyi değiştirmek üzere iletişime geçtiğimde ne yazık ki olumsuz yanıt aldım. Internet üzerinde bu yönlendiriciden kurtulmak için araştırma yaptığında da bol bol şikayet dışında elle tutulur 1 kaynak bulamadığım ve buna ayıracak zamanım da pek olmadığı için zaman içinde kaderime boyun eğmek zorunda kaldım.

Tilgin HG1332 ile geçirdiğim mutsuz zamanların süresi arttıkça bu yönlendiriciden kurtulmak için aradan 1 yıl geçtikten sonra internette arama yaptığında internet servis sağlayıcısının bu yönlendiriciyi köprü modunda kullanarak kendi yönlendiricinizi kullanmaya izin verdiğini öğrendim. Zaman

içinde HG1332'den nefret ettiğim için tamamıyla kurtulmanın yollarını aramaya başladım. Sosyal ağ hesaplarım üzerinden yardım çağrısında bulduğumda sağolsun epey bir kişi bu konuda yardımcı olmak için seferber oldu. Aykut ALPER'in farklı bir internet servis sağlayıcısında Mikrotik yönlendirici ile bunu yaptığı, bir başka yardımseverin VLAN ID ve PPPOE kullanıcı adı ve parolası ile HG1332'den kurtulabileceğimi belirtmesinden sonra ihtiyaç listesi üzerinde çalışmaya başladım. Listeyi hazırlamak için akıma gelen sorulardan bazıları şunlar oldu;

1. Hangi marka ve model yönlendirici almam gereklidir ?

Yıllarca Asus modem ve yönlendiricilere DD-WRT, Tomato, Asuswrt-Merlin gibi özel donanım yazılımlarının (custom firmware) kolayca yüklenebildiğini bildiğim için tercihimi Asus markasından yana yaptım. Donanım yazılımı olarak da güvenlik özellikleri hoşuma gittiği için Asuswrt-Merlin'i tercih ettim. Asuswrt-Merlin'in desteklediği modeller genel olarak pahalı olduğu için, fiyat ve performans açısından benim için en uygun olan RT-AC1900U modelini satın aldım.





2. VLAN ID'ım nedir ?

Tılgın HG1332'nin arayüzüne admin kullanıcısı ile bağlandığında maalesef VLAN ID'mi görebileceğim yönetim sayfalarının çoğu gizlenmişti. Internet üzerinde HG1332'ye yönelik araştırma yaptığında, bu yönlendiriciden kurtulmaya çalışan bir kişinin yazdığı bir yazıdan, HG1332 yönlendiricisinde de tanımlı olan kullanıcı adı ve parolaları elde etmeye başarıran İlteriş EROĞLU isimli genç bir arkadaşın başarılı çalışmasına rastladım. 2015 yılında Donanım Yazılımı Analizinin Önemi başlıklı yazımında benim de dikkat çektiğim şifresiz kanal üzerinden TR-069 iletişimini gerçekleştirmesinin yıllar sonra İlteriş'in çalışmasında da hala devam ettiğini görmek beni oldukça şaşırttı. Yazıda yer alan root kullanıcısı ile HG1332'nin arayüzüne bağlandıktan sonra VLAN ID'mi kolay bir şekilde öğrenebildim.

Sağlama

Yönetim protokolü
Yönetim sunucusu
Yoklama
TR-069

LAN Ayarları

LAN yapılandırması
Güvenlik duvarı/NAT
hizmetleri

WAN Ayarları**Bağlantılar****Bağlantıyı düzenle****Genel**Ad:

Bağlantı noktası: WAN

Tip: PPPoE (Ethernet Üzerinden PPP)

Açıklama: Durum: Çevrimiçi

Çalışma süresi: 5 gün 22 saat 37 dakika

 Etkin**Ethernet arabirimleri**Öncelik: VLAN kimliği: **Köprü**Tip: Yok PPP geçiş GenelLAN grubu: **PPP**Kullanıcı adı: Şifre: MRU: Maxfail: Canlı tutmayı yeniden:

dene:

Canlı Tutma Aralığı: Erişim Yoğunlaştırıcı: Hizmet: Proxy ARP Kalıcı İstek ÜzerineBoşta kalma süresi: Hata ayıkla**Güvenlik duvarı** Güvenlik duvarı NAT ...

3. Internet servis sağlayıcımı aramadan PPoE kullanıcı adı ve parolamı nasıl öğrenebilirim ?

root kullanıcısı ile arayüze girdikten sonra PPoE kullanıcısının parolası maskeli olduğu için mevcut konfigürasyonu yönlendiriciden indirip içinden PPoE parolasını elde edebildim.

Geliştirme[WebUI](#)**Fabrika**[Araç kümесini
karşıya yükle](#)**Bakım**[User account](#)
[Yönetici hesabı](#)
[Bakımcı hesabı](#)
[Teşhis](#)
[MIT dökümü](#)
[VoIP hata ayıklama](#)
[Sistemi yeniden
başlatın](#)
[Konsol ve CRM](#)**Ağ**[Ping](#)
[Algılayıcı](#)
[Speed test](#)**Yapılandırma****Aktar**
[Yedekle/Geri yükle](#)
[Varsayılan ayarları
geri yükle](#)**Aktar****Karşıdan yükle**

En son kaydedilen konfigürasyonu karşıdan yüklemek için aşağıdaki butona basın.

[Konfigürasyonu karşıdan yükle](#)**Karşıya yükle****Not:**

Konfigürasyon karşıya başarıyla yüklendiğinde sistem yeniden başlatılacaktır

Tamamı:[Choose File](#) No file chosen[Konfigürasyonu karşıya yükle](#)

```

427     in "config_map" string ""
428     out "link" "" "/connection/device/table/1/configured/4"
429 }
430 find "/connection/device/table/1/configured/4/layer" {
431     in "type" link "/connection/layer/ip_ipcp"
432     out "/connection/device/table/1/configured/4/layer/3"
433 }
434 find "/connection/device/table/1/configured/4/layer" {
435     in "type" link "/connection/layer/ppp"
436     out "/connection/device/table/1/configured/4/layer/2"
437 }
438 set "/connection/device/table/1/configured/4/layer/2/param/username" string "████████"
439 set "/connection/device/table/1/configured/4/layer/2/param/password" string "████"
440 set "/connection/device/table/1/configured/4/layer/2/param/service_name" string ""
441 set "/connection/device/table/1/configured/4/layer/2/param/ac_name" string ""
442 set "/connection/device/table/1/configured/4/layer/2/param/padi_timeout" s32 "0"
443 set "/connection/device/table/1/configured/4/layer/2/param/auth_type" string "Auto"
444 set "/connection/device/table/1/configured/4/layer/2/param/mru" u16 "1500"
445 set "/connection/device/table/1/configured/4/layer/2/param/persist" boolean "True"
446 set "/connection/device/table/1/configured/4/layer/2/param/maxfail" u16 "0"
447 set "/connection/device/table/1/configured/4/layer/2/param/demand" boolean "False"
448 set "/connection/device/table/1/configured/4/layer/2/param/idle" u16 "60"
449 set "/connection/device/table/1/configured/4/layer/2/param/proxyarp" boolean "False"
450 set "/connection/device/table/1/configured/4/layer/2/param/debug" boolean "False"
451 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_retry" u16 "5"
452 set "/connection/device/table/1/configured/4/layer/2/param/keepalive_interval" u16 "60"
453 action "/connection/device/table/1/add" {
454     in "index" string "2"
455     in "type" string "DHCP"
456     in "name" string "Management"
457     in "description" string ""
458     in "config_map" string ""
459     out "link" "" "/connection/device/table/1/configured/2"
460 }

```

RT-AC1900U için Asuswrt-Merlin'in web sayfasından ilgili donanım yazılımı sürümünü (RT-AC1900U için RT-AC68U yazılımı kullanılmalıdır.) indirip, web arayüzü üzerinden sorunsuz bir şekilde kurulumu gerçekleştirdim. Ardından PPPOE ve VLAN ID tanımlarını da yaptıktan sonra yönlendiricinin başarıyla interneete bağlanabildiğini gördüm.

<input type="checkbox"/> Name	Date modified	Type	Size
<input type="checkbox"/> Changelog-NG.txt	2.2.2019 21:01	Text Document	32 KB
<input type="checkbox"/> README-merlin.txt	2.2.2019 21:01	Text Document	10 KB
<input checked="" type="checkbox"/> RT-AC68U_384.9_0.trx	2.2.2019 22:20	TRX File	37.052 KB
<input type="checkbox"/> sha256sum.sha256	2.2.2019 22:20	SHA256 File	1 KB

ASUS RT-AC1900U

Oturumu Kapat Yeniden Başlat Türkçe ▾

İşlem Modu: **Kablosuz Yönlendirici** Donanım Yazılımı Sürümü: **3.0.0.4.384_20308**

SSID: **[REDACTED]** App    

İşlem Modu Sistem Donanım Yazılımı Yükseltme Ayarları Geri Yükle Geri Bildirimi

Yönetim - Donanım Yazılımı Yükseltme

Not:

1. En son firma yazılımı sürümüne önceki sürümüne ait güncellemeler dahildir.
2. Eski ve yeni donanım yazılımindaki yapılandırma parametresi için, ayarları yükseltme işlemi sırasında korunur.
3. Yükseltme işleminin başarısız olması durumunda, RT-AC1900U otomatik olarak acil durum moduna geçer. RT-AC1900U üzerindeki LED sinyalleri bu tür durumları gösterir. Sistem kurtarma işlemi için CD'deki Yazılım Sürümünü Kurtarma yardımcı programını kullanın.
4. En son aygit yazılımı sürümünü <http://www.asus.com/support/> adresindeki ASUS Destek sitesinden edinin.

Donanım Yazılımı Sürümü

Check Update Kontrol

AiMesh router

RT-AC1900U	Current Version : 3.0.0.4.384_20308-gead790e Manual Firmware Update : Karşıya Yükle
------------	--

Note : Manual firmware update will update this AiMesh router / node only, if you are using AiMesh system, please make sure you are uploading proper firmware version.

Hızlı Internet Kurulumu Genel Ağ Eşleme Misafir Ağı AiProtection Uyaranabilir QoS Trafik Çözümleyici USB uygulaması AiCloud 2.0 Gelişmiş Ayar Kablosuz Yerel Ağ WAN IPv6 VPN Güvenlik Duvarı **Yönetim** Sistem Günlüğü

ASUS RT-AC1900U

Oturumu Kapat Yeniden Başlat Türkçe

Hızlı Internet Kurulumu

Genel

Ağ Eşleme

Misafir Ağı

AiProtection

Uyarlanabilir QoS

Trafik Çözümleyici

USB uygulaması

AiCloud 2.0

Gelişmiş Ayarlar

Kablosuz

Yerel Ağ

WAN

IPv6

VPN

Güvenlik Duvarı

Yönetim

Sistem Günlüğü

İşlem Modu: **Kablosuz Yöneticisi** Donanım Yazılımı Sürümü: **3.0.0.4_384_20308**
SSID:

İşlem Modu Sistem Donanım Yazılımı/Yükseleme Ayarları Geri Yükle Geri Bildirim

Yönetim - Donanım Yazılımı/Yükseleme

3%

Not: **Donanım yazılımı yükseltiliyor. Lütfen 3 dakika kadar bekleyin.**

1. En son güncelleme: 2023-07-10 10:45:00
2. Eski yazılım sürümü: 3.0.0.4_384_20308
3. Yükseltme işleminin başarısız olması durumunda, RT-AC1900U otomatik olarak açık durum moduna geçer. RT-AC1900U üzerindeki LED sinyalleri bu tür durumları gösterir. Sistem kurtarma işlemi için CD'deki Yazılım Sürümünü Kurtarma yararını programını kullanın.
4. En son aygit yazılımı sürümüne <http://www.asus.com/support/> adresindeki ASUS Destek sitesinden edinin.

Donanım Yazılımı Sürümü

Check Update Kontrol

AiMesh router

RT-AC1900U Current Version: 3.0.0.4_384_20308_9ead790e
Manual Firmware Update [Hizmete Yükle](#)

Note: Manual firmware update will update this AiMesh router / node only. If you are using AiMesh system, please make sure you are uploading proper firmware version.

ASUS RT-AC1900U Powered by Asuswrt-Merlin

Oturumu Kapat Yeniden Başlat Türkçe

Hızlı Internet Kurulumu

Genel

- Ağ Eşleme
- Misafir Ağı
- AiProtection
- Uyaranabilir QoS
- Trafik Çözümleyici
- USB uygulaması
- AiCloud 2.0
- Tools

Gelişmiş Ayar

- Kablosuz
- Yerel Ağ
- WAN
- IPv6
- VPN
- Güvenlik Duvarı
- Yönetim

İşlem Modu: Kablosuz Yönlendirici Donanım Yazılımı Sürümü: 384.9 SSID:

Internet durumu: Ağ kablosu bağlı değil.

Güvenlik düzeyi: WPA2-Personal

İstemciler: 1 Listeyi Görüntüle

USB 3.0 Aygit Yok

USB 2.0 Aygit Yok

Sistem Durumu

2.4GHz	5GHz	Durum
İşlemci		
Core 1 10%		
Core 2 7%		

İşlemci: Core 1 10% Core 2 7%

Bellek

Kullanılan	Bos	Toplam
65MB	191MB	256MB
25%		

Kullanılan: 65MB Bos: 191MB Toplam: 256MB

Ethernet Bağlantı Noktaları

Bağlantı Noktaları	Durum
WAN	Unplugged
LAN 1	100 Mbps
LAN 2	Unplugged
LAN 3	Unplugged
LAN 4	Unplugged

ASUS RT-AC1900U

Powered by
Asuswrt-Merlin

Logout Reboot English

Quick Internet Setup

General

- Network Map**
- Guest Network**
- AiProtection**
- Adaptive QoS**
- Traffic Analyzer**
- USB Application**
- AiCloud 2.0**
- Tools**

Advanced Settings

- Wireless**
- LAN**
- WAN**
- IPv6**
- VPN**
- Firewall**
- Administration**

Operation Mode: **Wireless router** Firmware Version: **384.9** SSID: **[REDACTED]**

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

WAN - Internet Connection

RT-AC1900U supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of RT-AC1900U.

Basic Config	
WAN Connection Type	PPPOE
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP UPnP FAQ	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable secure UPnP mode	<input checked="" type="radio"/> Yes <input type="radio"/> No
UPNP: Allowed internal port range	1024 to 65535
UPNP: Allowed external port range	1 to 65535

WAN IP Setting	
Get the WAN IP automatically	<input checked="" type="radio"/> Yes <input type="radio"/> No

WAN DNS Setting	
Connect to DNS Server automatically	<input checked="" type="radio"/> Yes <input type="radio"/> No

Account Settings	
Username	[REDACTED]
Password
Disconnect after time of inactivity (in seconds)	0

LAN Port

Select ISP Profile	Manual Setting
Internet	VID 3001 PRIO 0
LAN Port 4	VID PRIO 0
LAN Port 3	VID PRIO 0

Special Applications

Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
Enable efficient multicast forwarding (IGMP Snooping)	Disable
UDP Proxy (Udpxy)	0

Apply

Sıra yönlendiricinin gerçekleştirdiği tüm DNS trafiğini şifreli (Dns over HTTPS – DoH) hale getirmeye geldiğinde ilk işim yönlendiriciye yüklenen paketleri kurabileceğim ve çalıştırabileceğim bir USB disk bağlamak oldu. Ardından komut satırından entware-setup.sh komutunu çalıştırarak kurulumu kısa sürede tamamladım. DoH desteğine sahip dnscrypt-proxy aracını kurmak için ise curl -L -s -k -0

```
https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer
```

komutunu çalıştırıp kurulumu gerçekleştirdim. dnscrypt-proxy aracının başarıyla çalıştığını teyit etmek için de ülkemizde hala yasaklı olan wikipedia.org adresinin ip adresini çözümlemeye çalıştığmda aracın başarıyla çalıştığını gördüm.

```

Router X
mert@RT-AC1900U-6610:/tmp/home/root# curl -L -s -k -o https://raw.githubusercontent.com/thuantran/dnscrypt-asuswrt-installer/master/installer && sh installer ; rm installer
Info: Detected ARMv7 architecture.
Info: JFFS custom scripts and configs are already enabled
Info: Choose what you want to do:
1) Install/Update dnscrypt-proxy
2) Uninstall dnscrypt-proxy
3) Configure dnscrypt-proxy
4) Set timezone
5)_unset_timezone
6) Install (P)RNG
7) Uninstall (P)RNG
8) Install swap file
9) Uninstall ALL
q) Quit
=> Please enter the number designates your selection: [1-9/q]: 1
Info: This operation will install dnscrypt-proxy and related files (<6MB)
Info: to jffs, no other data will be changed.
Info: Also some start scripts will be installed/modified as required.

=> Do you want to install dnscrypt-proxy to /jffs? [y/n]: y
Info: managing to update software...
Info: Downloading dnscrypt-proxy-lime_arm-2.0.19.tar.gz
Info: Downloading public_resolvers.md
Info: Downloading public_resolvers.md.minisig
linux-arm/
linux-arm/example-whitelist.txt
linux-arm/example-forwarding-rules.txt
linux-arm/example-cloaking-rules.txt
linux-arm/LICENSE
linux-arm/example-dnscrypt-proxy.toml
linux-arm/example-blacklist.txt
linux-arm/dnscrypt-proxy
Info: config file /etc/dnscrypt-proxy.toml file already configured
Info: init-start file already configured
Info: wan-start file already configured
Info: Configuring dnscrypt-proxy...
Info: Checking dnscrypt-proxy configuration...
[2019-03-06 16:59:17] [NOTICE] source [public-resolvers.md] loaded
[2019-03-06 16:59:17] [NOTICE] configuration successfully checked
Info: Found previous dnscrypt-proxy config file
=> Do you want to use this file without reconfiguring? [y/n]: y
Info: Use previous settings file
Info: Starting dnscrypt-proxy...

Done.
Info: For dnscrypt-proxy version 2 to work reliably, you might also want to:
Info: - Add swap
Info: - Add a RNG
Info: - Set your timezone
Info: Operation completed. You can quit or continue
=====

```

```

Info: Choose what you want to do:
1) Install/Update dnscrypt-proxy
2) Uninstall dnscrypt-proxy
3) Configure dnscrypt-proxy
4) Set timezone
5)_unset_timezone
6) Install (P)RNG
7) Uninstall (P)RNG
8) Install swap file
9) Uninstall ALL
q) Quit
=> Please enter the number designates your selection: [1-9/q]: q
Info: Operations have been applied if any has been made
Info: In case of anomaly, please reboot your router!

```

```

Router X DO - Yeni | Batcave | Batcave (1)
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @195.175.39.49 www.wikipedia.org +short
195.175.254.2
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @8.8.8.8 www.wikipedia.org +short
; <>> DIG 9.11.5 <>> @8.8.8.8 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @1.1.1.1 www.wikipedia.org +short
; <>> DIG 9.11.5 <>> @1.1.1.1 www.wikipedia.org +short
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
mert@RT-AC1900U-6610:/jffs/dnscrypt# dig @127.0.0.1 www.wikipedia.org +short
103.102.166.224
mert@RT-AC1900U-6610:/jffs/dnscrypt# ./dnscrypt-proxy -resolve www.wikipedia.org
Resolving [www.wikipedia.org]

Domain exists: probably not, or blocked by the proxy
Canonical name: www.wikipedia.org.
IP addresses: 103.102.166.224, 2001:df2:e500:ed1a::1
TXT records:
Resolver IP: 162.158.250.137

```

Yönlendiricinin etinden sütünden faydalananın bir de VPN servisleri ile olan bağlantısını (Netflix kullanıcıları nedenini çok iyi anlayacaklardır. :)) test etmeye karar verdim. Bunun için ABD seyahatim esnasında televizyonda çokça reklamını gördüğüm NordVPN VPN servis sağlayıcısına üye oldum. Asuswrt-Merlin kullanıcıları için özel olarak oluşturdukları yardım sayfasındaki adımları gerçekleştirdikten sonra yönlendiricinin NordVPN sunucularından biriyle başarıyla bağlantı kurmasını sağladım.

NordVPN ile bağlantı kurduktan sonra internet bağlantımın herhangi bir web sitesine bağlanamayacak şekilde aşırı derecede yavaşladığını farkettim. "Bu VPN sunucusunda problem var sanırım", "Bu VPN sunucusu da mı yavaş ?" derken bağlandığım 10'a yakın sunucudan web sitelerine bağlanamadığımı farkettim. Tam NordVPN'in hizmet kalitesini sorgulamaya başlamışken bir anda aklıma sosyal medyada VPN servislerinin yavaşlatıldığı iddialarına yönelik okuduğum mesajlardan biri geldi.



M. Serdar Kuzuloğlu

@mserdark

Takip et



Sayın [@TurksatAsistan](#), 1 haftadır süren VPN yavaşlatma 'hizmetiniz' kalıcı bir politika mı, geçici mi? Benim gibi diğer [@turksat](#) müşterileri de bilmek istiyordur eminim. Diğer erişim sağlayıcılarda böyle bir sorun yok. Sizdeki 'hızım' ekteki gibi.



00:16 - 26 Eki 2018

19 Retweet 172 Beğeni



29

19

172



Yanıtını Tweetle

Bağlandığım NordVPN sunucularından Google'ın DNS sunucusu olan 8.8.8.8 ip adresini pinglediğimde sürelerin katlanarak arttığını farkettim.

**Quick Internet Setup****General****Network Map****Guest Network****AiProtection****Adaptive QoS****Traffic Analyzer****USB Application****AiCloud 2.0****Tools****Advanced Settings****Wireless****LAN****WAN****IPv6****VPN****Firewall****Administration**Operation Mode: **Wireless router** Firmware Version: **384.9** SSID: **[REDACTED]**

VPN Status VPN Server VPN Client TOR

OpenVPN Client Settings

OpenVPN PPTP/L2TP

Before starting the service make sure you properly configure it, including the required keys, otherwise you will be unable to turn it on.

In case of problem, see the [System Log](#) for any error message related to openvpn.

Client controlSelect client instance **2: NordVPN - VPN****ON**

Connected (Local: 10.7.3.3 - Public: 176.113.74.238) Refresh

 Yes No

Description

NordVPN - VPN

Import .ovpn file

Choose File **No file chosen****Upload****Network Settings**

Interface Type

TUN

Protocol

TCP

Server Address and Port

Address: **176.113.74.237**Port: **443**

Accept DNS Configuration

Relaxed

Create NAT on tunnel

 Yes No**Authentication Settings**

Authorization Mode

TLS

Username/Password Authentication

 Yes No

Username

[REDACTED]

Password

 Show password

```

mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref  Use Iface
176.113.74.237 *              255.255.255.255 UH   0      0    0 ppp0
192.168.1.0    *              255.255.255.0   UG   0      0    0 ppp0
10.7.3.0        *              255.255.255.0   UG   0      0    0 br0
169.254.0.0    *              255.255.0.0    UG   0      0    0 tun12
127.0.0.0       *              255.0.0.0    UG   0      0    0 vlan3001
default         [REDACTED] 0.0.0.0        UG   0      0    0 lo
[m] default        0.0.0.0        UG   0      0    0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun12 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=55 time=6648.268 ms
64 bytes from 8.8.8.8: seq=1 ttl=55 time=5648.283 ms
64 bytes from 8.8.8.8: seq=2 ttl=55 time=4648.953 ms
64 bytes from 8.8.8.8: seq=3 ttl=55 time=12224.073 ms
64 bytes from 8.8.8.8: seq=4 ttl=55 time=11224.201 ms
64 bytes from 8.8.8.8: seq=5 ttl=55 time=10224.202 ms
64 bytes from 8.8.8.8: seq=6 ttl=55 time=9614.864 ms
64 bytes from 8.8.8.8: seq=7 ttl=55 time=12234.947 ms
64 bytes from 8.8.8.8: seq=8 ttl=55 time=11235.023 ms
64 bytes from 8.8.8.8: seq=9 ttl=55 time=10235.036 ms
64 bytes from 8.8.8.8: seq=10 ttl=55 time=9235.121 ms
64 bytes from 8.8.8.8: seq=11 ttl=55 time=16509.917 ms
64 bytes from 8.8.8.8: seq=12 ttl=55 time=15509.886 ms
64 bytes from 8.8.8.8: seq=13 ttl=55 time=14510.849 ms
64 bytes from 8.8.8.8: seq=14 ttl=55 time=13510.848 ms
64 bytes from 8.8.8.8: seq=15 ttl=55 time=12510.775 ms
64 bytes from 8.8.8.8: seq=16 ttl=55 time=11512.011 ms
64 bytes from 8.8.8.8: seq=17 ttl=55 time=10513.375 ms
64 bytes from 8.8.8.8: seq=18 ttl=55 time=9513.429 ms
64 bytes from 8.8.8.8: seq=19 ttl=55 time=8513.435 ms
64 bytes from 8.8.8.8: seq=20 ttl=55 time=13145.176 ms
64 bytes from 8.8.8.8: seq=21 ttl=55 time=12145.169 ms
64 bytes from 8.8.8.8: seq=22 ttl=55 time=11147.973 ms
64 bytes from 8.8.8.8: seq=23 ttl=55 time=10147.933 ms
64 bytes from 8.8.8.8: seq=24 ttl=55 time=9147.860 ms
64 bytes from 8.8.8.8: seq=25 ttl=55 time=8147.774 ms
64 bytes from 8.8.8.8: seq=26 ttl=55 time=7147.687 ms
64 bytes from 8.8.8.8: seq=27 ttl=55 time=11516.101 ms
64 bytes from 8.8.8.8: seq=28 ttl=55 time=11761.391 ms
64 bytes from 8.8.8.8: seq=29 ttl=55 time=10761.391 ms
64 bytes from 8.8.8.8: seq=30 ttl=55 time=9761.313 ms
64 bytes from 8.8.8.8: seq=31 ttl=55 time=8761.224 ms
64 bytes from 8.8.8.8: seq=32 ttl=55 time=7761.279 ms
64 bytes from 8.8.8.8: seq=33 ttl=55 time=9896.576 ms
64 bytes from 8.8.8.8: seq=34 ttl=55 time=8896.620 ms
64 bytes from 8.8.8.8: seq=35 ttl=55 time=7898.961 ms
64 bytes from 8.8.8.8: seq=36 ttl=55 time=6898.912 ms
64 bytes from 8.8.8.8: seq=37 ttl=55 time=5898.834 ms
64 bytes from 8.8.8.8: seq=38 ttl=55 time=4898.749 ms
64 bytes from 8.8.8.8: seq=39 ttl=55 time=16923.183 ms
64 bytes from 8.8.8.8: seq=40 ttl=55 time=15923.461 ms
64 bytes from 8.8.8.8: seq=41 ttl=55 time=14924.623 ms
64 bytes from 8.8.8.8: seq=42 ttl=55 time=13924.561 ms
64 bytes from 8.8.8.8: seq=43 ttl=55 time=29231.054 ms
64 bytes from 8.8.8.8: seq=44 ttl=55 time=28231.044 ms
64 bytes from 8.8.8.8: seq=45 ttl=55 time=27231.986 ms
64 bytes from 8.8.8.8: seq=46 ttl=55 time=26231.979 ms
64 bytes from 8.8.8.8: seq=47 ttl=55 time=31198.969 ms
64 bytes from 8.8.8.8: seq=48 ttl=55 time=30198.990 ms
64 bytes from 8.8.8.8: seq=49 ttl=55 time=29198.962 ms
64 bytes from 8.8.8.8: seq=50 ttl=55 time=28198.983 ms
64 bytes from 8.8.8.8: seq=51 ttl=55 time=27198.956 ms
64 bytes from 8.8.8.8: seq=52 ttl=55 time=26201.187 ms
64 bytes from 8.8.8.8: seq=53 ttl=55 time=25201.248 ms
64 bytes from 8.8.8.8: seq=54 ttl=55 time=24201.256 ms
^C
--- 8.8.8.8 ping statistics ---
80 packets transmitted, 55 packets received, 31% packet loss

```

ASUS RT-AC1900U Powered by Asuswrt-Merlin Logout Reboot English

Quick Internet Setup

General Network Map Guest Network AiProtection Adaptive QoS Traffic Analyzer USB Application AiCloud 2.0 Tools Advanced Settings Wireless LAN WAN IPv6 VPN Firewall Administration

Operation Mode: **Wireless router** Firmware Version: **384.9** SSID: **[REDACTED]**

VPN Status VPN Server VPN Client TOR

OpenVPN Client Settings

Before starting the service make sure you properly configure it, including the required keys, otherwise you will be unable to turn it on.

In case of problem, see the [System Log](#) for any error message related to openvpn.

Client control

Select client instance	4: NordVPN - VPN - CA-US10
Service state	ON Connected (Local: 10.7.7.44 - Public: 91.132.137.70) Refresh
Automatic start at boot time	<input checked="" type="radio"/> Yes <input type="radio"/> No
Description	NordVPN - VPN - CA-US10
Import .ovpn file	Choose File No file chosen Upload

Network Settings

Interface Type	TUN
Protocol	TCP
Server Address and Port	Address: 139.28.218.44 Port: 443
Accept DNS Configuration	Relaxed
Create NAT on tunnel	<input checked="" type="radio"/> Yes <input type="radio"/> No

Authentication Settings

Authorization Mode	TLS
Username/Password Authentication	<input checked="" type="radio"/> Yes <input type="radio"/> No
Username	[REDACTED]
Password <input type="checkbox"/> Show password

```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway         Genmask        Flags Metric Ref    Use Iface
139.28.218.44  *               255.255.255.255 UGH   0      0        0 ppp0
                  *               255.255.255.255 UH    0      0        0 ppp0
192.168.1.0    *               255.255.255.0   U      0      0        0 br0
10.7.7.0        *               255.255.255.0   U      0      0        0 tun14
169.254.0.0    *               255.255.0.0    U      0      0        0 vlan3001
127.0.0.0       *               255.0.0.0     U      0      0        0 lo
default         0.0.0.0        0.0.0.0        UG     0      0        0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun14 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=47 ttl=117 time=866.553 ms
64 bytes from 8.8.8.8: seq=48 ttl=117 time=1191.751 ms
64 bytes from 8.8.8.8: seq=49 ttl=117 time=2292.490 ms
64 bytes from 8.8.8.8: seq=50 ttl=117 time=31483.191 ms
64 bytes from 8.8.8.8: seq=52 ttl=117 time=29483.216 ms
64 bytes from 8.8.8.8: seq=53 ttl=117 time=34078.320 ms
64 bytes from 8.8.8.8: seq=54 ttl=117 time=33078.304 ms
64 bytes from 8.8.8.8: seq=55 ttl=117 time=32078.228 ms
64 bytes from 8.8.8.8: seq=56 ttl=117 time=31078.140 ms
64 bytes from 8.8.8.8: seq=57 ttl=117 time=30078.070 ms
```

NordVPN'in Double VPN özelliğine sahip sunucularından birine bağlandığında bu

defa ping süresinin çok daha makul seviyelerde olduğunu ve web sitelerine bağlanabildiğiğini gördüm. Başka bir Double VPN sunucusuna bağlandığında ise bu yine bağlantımın inanılmaz derecede yavaş olduğunu farkettim. İki vpn sunucusunun OpenVPN bağlantı ayarlarını kıyasladığında, mesaj doğrulamasında kullanılan AUTH parametresinin (HMAC digest algorithm) farklı (SHA512 yerine SHA1) olduğunu tespit ettim. Tüm NordVPN sunucularının arasından AUTH parametresinin SHA1 olanlarına bağlanmayı denediğimde bağlantının yavaşlamadığını dolayısıyla bu yavaşlamayı tetikleyen unsurun SHA512 algoritması ile ilişkili olabileceğine kanaat getirdim.

PING sürelerinin gecikmesine neyin sebep olabileceğini LinkedIn üzerinden sorduğumda genel olarak gelen yanıtlar; hattın saturé olabileceği, aradaki yönlendiricinin bozuk olabileceği, ethernet kartında sorun olabileceği, yerel ağıda topraklama sorunu olabileceği, firewall bağlantı listesinin dolduğu, sistemin saldırısı altında olabileceği oldu. Ben de paylaştığım ekran görüntüleri ve Linkedin'den gelen yorumlar ışığında bu gecikmeye neyin sebep olduğunu bulunmasını, alıştırma olması adına siz sevgili okurlarıma bırakmaya karar verdim.

```

1 client
2 dev tun
3 proto tcp
4 remote 192.168.114.37 443
5 resolv-retry infinite
6 remote-random
7 nobind
8 tun-mtu 1500
9 tun-mtu-extra 32
10 mssfix 1450
11 persist-key
12 persist-tun
13 ping 15
14 ping-restart 0
15 ping-timer-rem
16 reneg-sec 0
17 comp-lzo no
18
19 remote-cert-tls server
20
21 #mute 10000
22 auth-user-pass
23
24 verb 3
25 pull
26 fast-io
27 cipher AES-256-CBC
28
29
30 <ca>
31 -----BEGIN CERTIFICATE-----
32 MIIE2TCCAJBgAwIBAgIjALIMXGgr/LxUhMAl0GCSqGSIB3DQEBCUAMIGfM0QswCQYD
33 VQGEWJQOTELMAkGA1UECBMQUEExDzANBgNVBACtB1hhbPfYTEQMA4GA1UEChMH
34 Tm9yZFR2QzTjEOMA4GA1UECxMHIm9yZFR2QzTjEEMBkGA1UEAxAdSY2EtDXMzLs5vcmR2
35 cG4uY29tMRRAWDgYDVQQEwdob3JkV1bMRw8HQYJKoZIhvcNAQkBFbjBzKJ0QG5v
36 cmR2cg4uY29tMB4XDTE3MTYvOTE1MzkwMjOgXDI1MTYNEzIMzMWoFwgg28xczaJ
37 bgNVBAYTAlBBM0swCQYDVQfIEmJQQTfEPM0GA1UEBMMQGUFyWlHMRawDgYDVQfQ
38 Ewdob3JkV1bMRRAWDgYDVQfQlEwdob3JkV1bMRwsGQYDVQfQDEExJjYs1lc2mub9y
39 ZH2wi5jb20xEDAOBgNVBCKTB05vcmRWUE4xHzAdBqkghkiG9w0BCQEWEGNlcnRA
40 bm9yZH2wi5jb20wgElMA0GCSqGSIb3DQEBAQUAAIBDwAwfgKvAIAQDjN803
41 3Qpe8tNGHbJqv3361y8DY1d6dvaw0WqkBg4MV+cSARYlin9ndgilv0Maij69vf19
42 LFcz9HPUSE5231bEH3zqNSLo4mFOuR5bNd359T178idhvPWWbDymLwqytAAspW

```

```

1 client
2 dev tun
3 proto tcp
4 remote 192.168.218.44 443
5 resolv-retry infinite
6 remote-random
7 nobind
8 tun-mtu 1500
9 tun-mtu-extra 32
10 mssfix 1450
11 persist-key
12 persist-tun
13 ping 15
14 ping-restart 0
15 ping-timer-rem
16 reneg-sec 0
17
18
19 remote-cert-tls server
20
21 #mute 10000
22 auth-user-pass
23
24 verb 3
25 pull
26 fast-io
27 cipher AES-256-CBC
28 +auth SHA512
29
30 <ca>
31 -----BEGIN CERTIFICATE-----
32 MIIFCj0CAvRkAwIBAgIjATANBgkqhkiG9w0BAQ0FADAS5MgwCQYDVQfQfGEwJQfQfEQ
33 MA4GA1UECHMHTn9yZFR2QzTjEYMBkGA1UEAxPfM0YfZFR2QzTjE2901ENBMB4XDTE2
34 MDEwMjAwMDAwMjQzMTM1MTIzMjIzMTIzNTk1OVwvOTELAkGA1UEBhMCUEExEDAOBgNV
35 BAoTB05vcmRUE4xGDAwBgNVBAMTD05vcmRWUE4gUm9vdCBQfTCACaiIWQDQYJKoZI
36 HvhvNAQEBBQAQDg1fPADCCAgcCgjBAMkxBHyoyfF1upsIMKwC6QvK2ps3NN2/eQF
37 kfqfIS1gq1oaejs8ErnYKaon8uZCTPxRHi1QNggs5D2gixd1mJuV3e3y9FJ-
38 XModKxDcBGBodvKyut61cfEVF6/txKcbgq2K9UfURHS9eJm3rpl/5huQMcppX7ku
39 eQ8dpCw3iK1Tqwd12udlqswAUvvgzC2H5Siya2/S/TncK31Q1UP6BksbbURcwOV
40 skEDsm6YoWDnn/IIZGOnYFrZxQH5jTz3j1OBVR1TuBuUkfxfh1PEwHwZlgrcxXu
41 MP+QgM54kezgziJaZcCM2zF31rvxMvXIMfNeI0JABy91jw969x08czCU51MvMa
42 371tv5Ec9U5h2uwk/9Q012+d/r6Jx0mlrS8gnCAKJg913ky2w6e4F28mYl4vpRR

```

Normal text file

length: 2.815 lines: 85 Ln:1 Col:1 Sel:0|0 Unix (LF) UTF-8 INS

```
mert@RT-AC1900U-6610:/tmp/home/root# route
Kernel IP routing table
Destination     Gateway      Genmask       Flags Metric Ref  Use Iface
68.168.114.37   0.0.0.0     255.255.255.255 UGH 0      0      0 ppp0
                  0.0.0.0     255.255.255.255 UH 0      0      0 ppp0
192.168.1.0     *           255.255.255.0   U 0      0      0 br0
10.7.7.0         *           255.255.255.0   U 0      0      0 tun13
169.254.0.0     *           255.255.0.0    U 0      0      0 vlan3001
127.0.0.0        *           255.0.0.0    U 0      0      0 lo
default          0.0.0.0     0.0.0.0     UG 0      0      0 ppp0
mert@RT-AC1900U-6610:/tmp/home/root# ping -I tun13 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=121 time=416.562 ms
64 bytes from 8.8.8.8: seq=1 ttl=121 time=163.178 ms
64 bytes from 8.8.8.8: seq=2 ttl=121 time=227.239 ms
64 bytes from 8.8.8.8: seq=3 ttl=121 time=163.491 ms
64 bytes from 8.8.8.8: seq=4 ttl=121 time=164.102 ms
64 bytes from 8.8.8.8: seq=5 ttl=121 time=163.397 ms
64 bytes from 8.8.8.8: seq=6 ttl=121 time=163.538 ms
64 bytes from 8.8.8.8: seq=7 ttl=121 time=165.894 ms
64 bytes from 8.8.8.8: seq=8 ttl=121 time=163.354 ms
64 bytes from 8.8.8.8: seq=9 ttl=121 time=163.095 ms
64 bytes from 8.8.8.8: seq=10 ttl=121 time=163.285 ms
64 bytes from 8.8.8.8: seq=11 ttl=121 time=180.063 ms
64 bytes from 8.8.8.8: seq=12 ttl=121 time=163.515 ms
64 bytes from 8.8.8.8: seq=13 ttl=121 time=183.941 ms
64 bytes from 8.8.8.8: seq=14 ttl=121 time=163.153 ms
64 bytes from 8.8.8.8: seq=15 ttl=121 time=164.452 ms
64 bytes from 8.8.8.8: seq=16 ttl=121 time=239.481 ms
64 bytes from 8.8.8.8: seq=17 ttl=121 time=247.684 ms
64 bytes from 8.8.8.8: seq=18 ttl=121 time=229.615 ms
64 bytes from 8.8.8.8: seq=19 ttl=121 time=163.541 ms
64 bytes from 8.8.8.8: seq=20 ttl=121 time=308.787 ms
64 bytes from 8.8.8.8: seq=21 ttl=121 time=163.751 ms
64 bytes from 8.8.8.8: seq=22 ttl=121 time=164.228 ms
64 bytes from 8.8.8.8: seq=23 ttl=121 time=189.868 ms
64 bytes from 8.8.8.8: seq=24 ttl=121 time=163.761 ms
64 bytes from 8.8.8.8: seq=25 ttl=121 time=163.222 ms
64 bytes from 8.8.8.8: seq=26 ttl=121 time=163.220 ms
64 bytes from 8.8.8.8: seq=27 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=28 ttl=121 time=163.683 ms
64 bytes from 8.8.8.8: seq=29 ttl=121 time=163.792 ms
64 bytes from 8.8.8.8: seq=30 ttl=121 time=163.429 ms
64 bytes from 8.8.8.8: seq=31 ttl=121 time=325.651 ms
64 bytes from 8.8.8.8: seq=32 ttl=121 time=178.039 ms
64 bytes from 8.8.8.8: seq=33 ttl=121 time=163.946 ms
64 bytes from 8.8.8.8: seq=34 ttl=121 time=163.651 ms
64 bytes from 8.8.8.8: seq=35 ttl=121 time=163.740 ms
64 bytes from 8.8.8.8: seq=36 ttl=121 time=340.520 ms
64 bytes from 8.8.8.8: seq=37 ttl=121 time=236.380 ms
64 bytes from 8.8.8.8: seq=38 ttl=121 time=433.735 ms
64 bytes from 8.8.8.8: seq=39 ttl=121 time=163.266 ms
64 bytes from 8.8.8.8: seq=40 ttl=121 time=163.345 ms
64 bytes from 8.8.8.8: seq=41 ttl=121 time=163.188 ms
64 bytes from 8.8.8.8: seq=42 ttl=121 time=163.783 ms
64 bytes from 8.8.8.8: seq=43 ttl=121 time=163.224 ms
64 bytes from 8.8.8.8: seq=44 ttl=121 time=163.706 ms
64 bytes from 8.8.8.8: seq=45 ttl=121 time=164.327 ms
64 bytes from 8.8.8.8: seq=46 ttl=121 time=163.542 ms
^C
--- 8.8.8.8 ping statistics ---
47 packets transmitted, 47 packets received, 0% packet loss
round-trip min/avg/max = 163.095/194.426/433.735 ms
```

Sonuç olarak yıllarca istemeyerek, şikayet ederek kullandığım Tılgın HG1332 yönlendiriciden kurtularak, güvenliğini kendimin sağlayabildiği, güvenlik özellikleri ile dopdolu yeni yönlendiricime yıllar sonra kavuşmuş oldum. Özellikle OpenVPN desteği sayesinde, alışveriş merkezleri, oteller, cafeler, havaalanları gibi halka açık alanlarda ücretsiz olarak sunulan fakat bilgi güvenliği adına kullanıcılar için risk teşkil eden ücretsiz/ortak WiFi

hizmetlerinden faydalananmak istediğimde, evimdeki yönlendiricime VPN ile güvenli bir şekilde bilgisayarımdan veya cep telefonumdan bağlanabilmek ve bu riski minimuma indirgeyebilmek de beni fazlaıyla mutlu etti.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.