Kingsmead Security Ltd

Residential VPNs:
A Rising Risk for OTT Services

Kingsmead Security Whitepaper

Executive Summary

The use of VPNs to access OTT streaming services is a persistent threat to the industry. VPNs can risk compliance with content licensing contracts and can impact service revenues. VPN vendors work hard to avoid detection by OTT services and are constantly evolving new techniques such as targeting high-value OTT services with service-specific proxy servers to further thwart detection.

This whitepaper describes some of the techniques premium VPN vendors use to avoid detection. This includes routing network traffic through data centre-hosted servers, AWS-hosted servers and/or residential homes. Our whitepaper shows that leveraging residential homes is now widespread amongst VPN vendors, and hundreds of thousands of homes are now being actively used to route VPN traffic. This is an increasing threat to OTT services, who must be aware of the issue and take appropriate action.

September 2022

1 Introduction

The last few years have seen significant growth in usage of over-the-top (OTT) video streaming services. Although requirements will vary across service providers, almost all services are required to verify the geographic location of their users. Common reasons include:

- Content licensing deals require restriction to licensed countries only.
- Services must comply with local laws and regulations (for example, content may be banned in certain countries).
- The country may require alternate versions of content to be streamed (for example, content language variants may be available, or content may be edited for material considered offensive in the country).
- Service revenues may be eroded if content is easily available from alternate countries with lower licensing costs.
- Advertising revenues may be eroded if advertising is served outside the licensed country.
- Restricting access to the licensed country helps to mitigate the risk of service abuse (for example, to reduce the options available to content pirates, or to reduce the market for credential sharing/sale).
- Additional content delivery costs are incurred if streaming content to unauthorised users.

OTT service providers use geo-location vendors in an attempt to identify the geographic location of a user based on the user's IP address. The OTT service provider will check the IP address against the geo-location vendor's database to find the country, region or city it is associated with and confirm the user is present in the authorised territory for the service.

OTT service users may be a genuine subscriber, an unauthorised out-of-territory subscriber, someone sharing credentials, or someone using stolen credentials. Some of these users may attempt to disrupt these geo-location checks by using VPN services to conceal their real location. OTT services must therefore perform two checks:

- Confirm that the user is located within the service territory.
- Detect any use of VPNs to conceal their location.

VPN vendors continue to evolve their technology to avoid detection. This whitepaper discusses some of these technologies. In particular, we discuss the use of both data centre and residential proxies, then analyse real-world data from production OTT services to confirm their use.

2 VPN Services

In a previous Kingsmead whitepaper[1], we discussed how VPNs can be used to circumvent geo-restriction of OTT services. Figure 2-1 shows how a VPN tunnel is created between the VPN client running in the user's home and a VPN server located in the country of the targeted service. The IP address presented to the target service is no longer the actual IP address in the user's country but is now the IP address presented by the VPN server in the target country.

[1] https://www.geocomply.com/resources/whitepaper/proxy-over-vpn-a-new-challenge-for-ott-services/

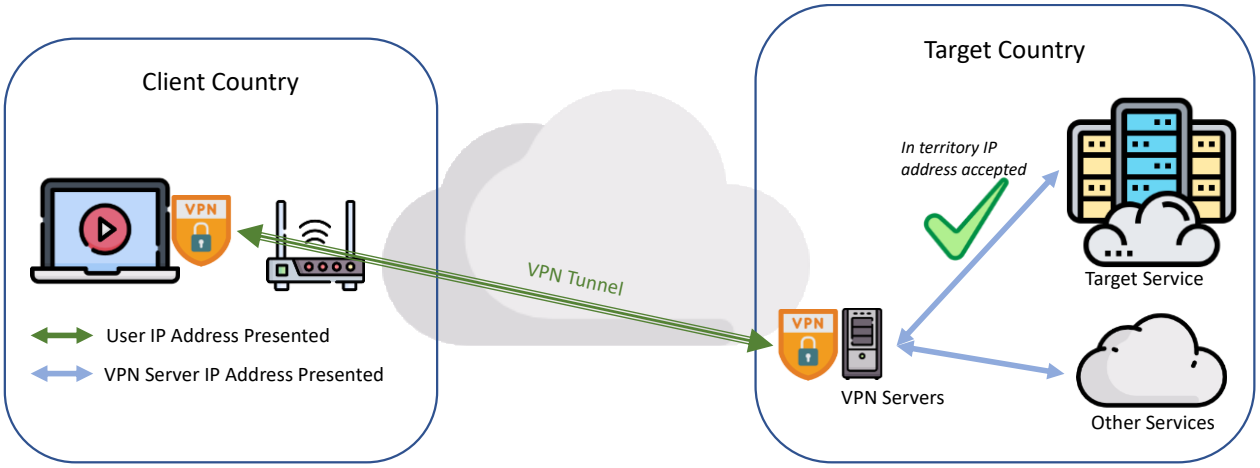

Figure 2-1 Connecting to a Remote Service using a VPN

These VPN servers have historically been relatively easy for a VPN detection vendor to detect, so VPN vendors may deploy hundreds of servers in a single country and ensure that the IP addresses of these servers change frequently. This makes it harder to detect these servers as the configuration is under constant change, but a reputable VPN detection vendor will still achieve a very high detection rate with this strategy. VPN vendors therefore evolved their strategy to deploy service-specific proxy servers to further conceal their services. This is often termed "Proxy over VPN" and is illustrated in Figure 2-2.

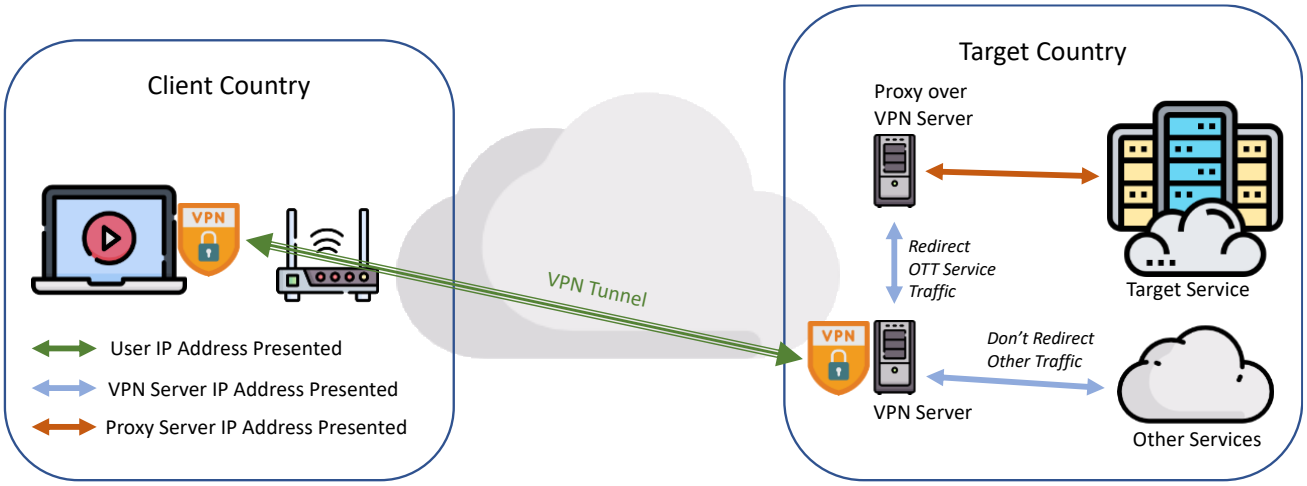

Figure 2-2 Proxy Server Routing using DNS

This configuration means that:

- The IP address presented to the target OTT service is the IP address of the proxy server.
- The IP address presented to all other services is the IP address of the VPN server.

Proxy servers can be a challenge for VPN detection vendors as proxy servers often target single OTT services. The targeted OTT service is the only service which can determine the IP address of the server – the IP address is invisible to other services, and invisible to VPN detection vendors. Further, VPN vendors can configure and optimise these servers to further avoid detection by using knowledge specific to the OTT services they are targeting. Leading VPN detection vendors should have solutions in place to meet the challenge of these proxy servers.

As we will see in the next section, re-routing specific OTT services like this is now widespread. A simple web search for "best VPN for streaming" gives some insight into the issue.

3 Targeted OTT Services

VPN vendors with Proxy over VPN technology typically re-route specific OTT service traffic by manipulating DNS entries. Other methods are possible, but DNS is quick, easy and widely used. The VPN client software ensures that DNS resolution is performed by the VPN vendor, allowing them the opportunity to manipulate results as they require.

By connecting to a range of VPN endpoints and performing DNS lookups, we can identify which VPNs are targeting which services. Table 3-1 gives the result of an analysis performed by Kingsmead during July 2022. Testing focused primarily on UK and US streaming services, but we also looked at several EU services too.

These results should not be interpreted as a comprehensive review of the issue, as we did not test all domains used by all services. VPN activity is also highly dynamic, so results will evolve over time. However, these results highlight that Proxy over VPN activity is very common amongst the leading VPN vendors.

OTT Service	Is DNS manipulated?					
	ExpressVPN	NordVPN	Surfshark	CyberGhost	StrongVPN	BulletVPN
Netflix (Various)	Yes	Yes	Yes	Yes	Yes	No
Amazon (Various)	Yes	Yes	Yes	Yes	Yes	Yes
Peacock (US)	Yes	Yes	Yes	No	No	Yes
Disney+ (Various)	Yes	Yes	Yes	Yes	No	No
HBO Max (US)	No	Yes	Yes	Yes	No	Yes
Discovery+ (Various)	No	Yes	Yes	No	No	No
BBC iPlayer (UK)	Yes	Yes	Yes	Yes	Yes	Yes
itvHub (UK)	Yes	Yes	Yes	Yes	No	Yes
All4 (UK)	Yes	Yes	Yes	No	Yes	Yes
My5 (UK)	Yes	Yes	Yes	No	No	Yes
Now TV (UK)	Yes	Yes	Yes	No	No	No
RTE Player (Ireland)	No	Yes	Yes	No	No	No
Play SRF (Switzerland)	No	Yes	Yes	No	No	No
TV4 Play (Sweden)	No	Yes	Yes	Yes	No	Yes
Maxdome (Germany)	No	Yes	Yes	No	No	No
Canal+ (France)	Yes	No	Yes	Yes	No	No
RAI Play (Italy)	Yes	Yes	Yes	Yes	Yes	No
Magenta TV (Germany)	No	Yes	No	No	No	No
TVP (Poland)	No	Yes	No	No	No	No
Ziggo Go (Netherlands)	No	No	Yes	No	No	No

Table 3-1 OTT Services Targeted by Proxy over VPN

As expected, major services such as Netflix, Amazon and BBC iPlayer are targeted by many VPN vendors.

During our testing, we observed that DNS manipulation is very country specific. OTT services tend only to be targeted when connecting to VPN endpoints in the home country of that service. For example, BBC iPlayer is only targeted by VPN endpoints in the UK. However, there are exceptions. For example, Surfshark targets the All4 and My5 UK-based services for US endpoints too, by routing traffic from the US VPN servers to UK-based proxies.

The DNS IP addresses returned by these VPNs suggest that VPN vendors have different proxy server architectures. The most common strategy appears to route each targeted domain to a different proxy server. For example, `www.bbc.co.uk` is routed to one proxy server, `www.disneyplus.com` (UK) to another, and `www.disneyplus.com` (US) to yet another.

However, there are many exceptions. For example:

- CyberGhost routes all targeted domains to a single proxy server IP address.
- NordVPN routes multiple ITV domains to a single proxy server IP address, but different BBC domains are routed through different proxy servers.
- Surfshark routes all HBO Max domains to a single proxy server for both US and UK endpoints. However, for Disney+ domains, Surfshark uses different proxy servers for US and UK endpoints.

We do not know the nature of these proxy servers. Each proxy server IP address may be assigned to a stand-alone physical server but could equally be assigned to a virtual server, cloud server or even a load-balanced cluster of servers.

DNS re-routing is explored further in Section 5.

4 VPN Endpoint Database

To understand more about the nature of the proxy servers used by VPN vendors, Kingsmead performed a detailed analysis of a database of VPN IP addresses presented to some major OTT services. This section describes the results of our analysis.

Kingsmead would like to thank GeoComply for supplying this database for our work.

4.1 Database Construction

From 7th June 2022 until 22nd July 2022, GeoComply performed a series of tests to capture the IP addresses presented to four leading OTT services – two in the UK and two in the US. During the test period, GeoComply made repeated connections using a range of VPN services, then queried the OTT services to obtain the IP address they were observing from each connection (we call each test a "visit").

The OTT services used in this test are known to be targeted by VPN vendor proxy servers, so the database was expected to contain IP addresses for VPN servers and proxy servers, as well as any other IP address types used by VPN vendors.

Fifty-nine different VPN services were used to construct the database. Table 4-1 lists some of them.

VPN Vendor	Number of Visits	VPN Vendor	Number of Visits
Privado	189055	IPVanish	178128
Hotspot Shield	162486	NordVPN	73766
MonVPN	47769	Surfshark	44963
Ivacy	39850	PureVPN	24046
VPNUnlimited	21828	HideIPVPN	18106
Watch UK TV Anywhere	14232	BolehVPN	11359
IWASEL	11037	FrootVPN	9806
Keenow	8225	Witopia	5501
WindScribe	4296	CyberGhost	4065
VPNShazam	3855	uVPN	3456
VPNac	2820	Private Internet Access NextGen	2452
StrongVPN	2182	ProtonVPN	1962
BritishTVAnywhere	1902	Hola!	1720

Astrill	1316	UltraVPN	768
AirVPN	590	VyprVPN	524

Table 4-1 Top VPN Vendors under Test

Due to the nature of the test process, the number of visits varies greatly across VPN vendors. A little caution is therefore needed when analysing our results. ExpressVPN is a very popular VPN and was represented within our database. However, due to the methods used during collection, the number of recorded visits was small for ExpressVPN.

The entire database consisted of almost 1.5 million visits. Each visit records:

- Date and time of the visit
- The VPN used to visit the OTT service
- The OTT service visited
- The IP address presented to the OTT service during that visit

To conduct a focussed study, Kingsmead analysed only the visits which targeted the two UK-based services:

- Number of "Service A" visits – 744,752
- Number of "Service C" visits – 151,630
- Total UK visits – 896,382

These tests provided a list of 171,788 unique IP addresses.

US-based services were not studied in this analysis.

4.2 High-Level View

To obtain a high-level view of the database, Kingsmead ran these IP addresses through a geo-location vendor. The geo-location vendor provides a range of information for each IP address:

- Owner of the IP address (business name)
- Usage type of the IP address (residential, hosting, cellular, etc)
- Location of the IP address

Note: Geo-location vendor data can contain incorrect or inaccurate information. However, due to the large database we're analysing, the nature of the IP addresses we're studying and our requirement to look at large-scale trends only, the accuracy of individual data points is not a major concern in this study. As noted later, UK ISPs were approached to validate some of our results.

Figure 4-1 shows the results of our initial analysis of IP addresses in our database.

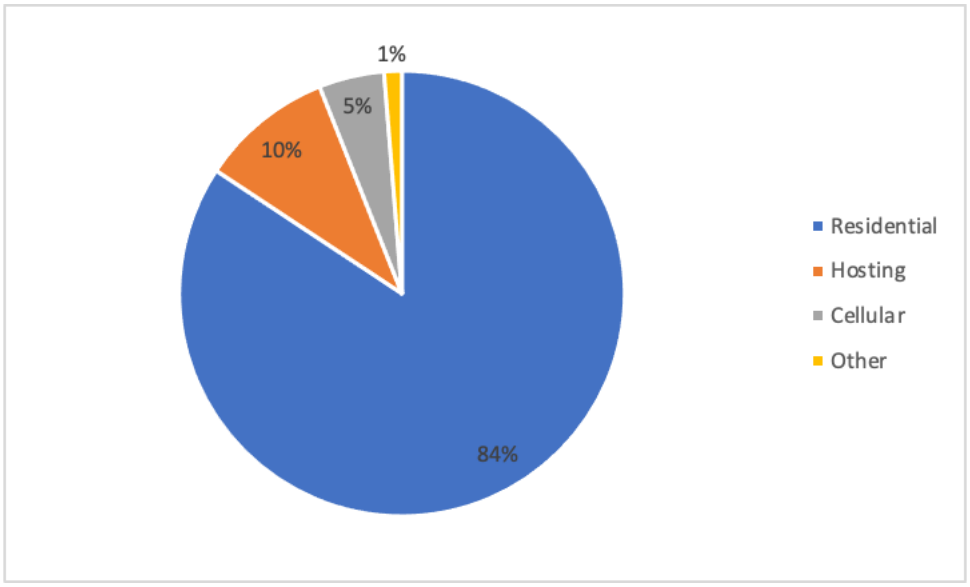

Figure 4-1 Types of VPN IP Addresses

The observation here is very simple – the majority of the VPN endpoint IP addresses presented to the two OTT services in this analysis are residential IP addresses. This is a significant result and confirms the industry fears that the use of residential proxies is becoming mainstream.

When we look at the number of visits instead (many IP addresses were visited multiple times), we see that residential IP addresses are still dominant (see Figure 4-2).

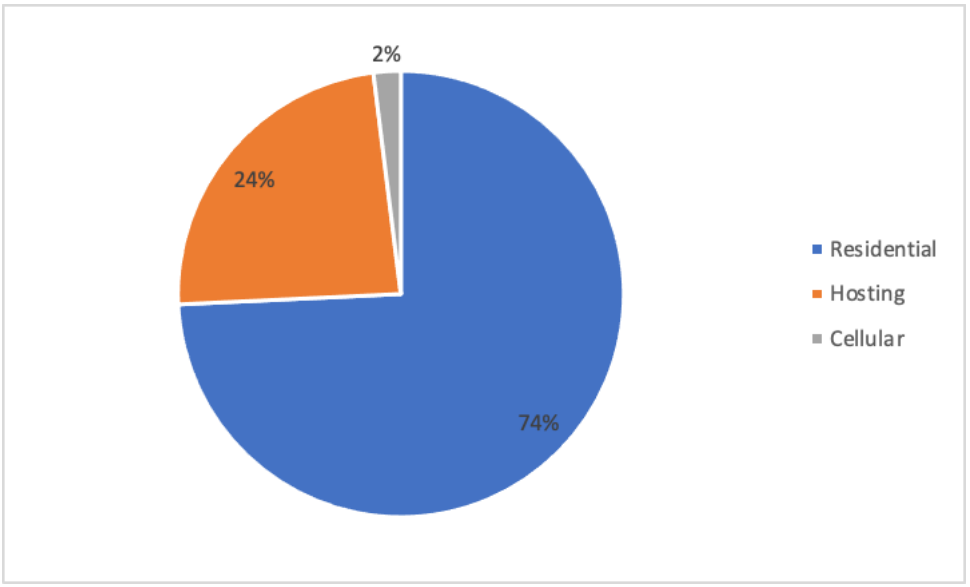

Figure 4-2 Number of Visits by Type

Table 4-2 shows the most presented IP addresses in the database.

Note: We have chosen to obscure IP addresses throughout this report. The first two octets are replaced with xxx.xxx..

IP	Number of Visits	Type of IP
xxx.xxx.45.28	5456	hosting
xxx.xxx.207.227	5131	residential
xxx.xxx.178.130	4688	residential

xxx.xxx.45.66	4631	hosting
xxx.xxx.207.254	4316	residential
xxx.xxx.207.231	4184	residential
xxx.xxx.239.15	3456	hosting
xxx.xxx.177.226	3416	hosting
xxx.xxx.197.230	2820	residential
xxx.xxx.189.86	2662	residential

Table 4-2 Top 10 Most Visited IP Addresses

The most surprising thing about this snapshot is that many of the most visited IP addresses are residential. In fact, if we look at the top 50 most visited IP addresses, 39 of them are residential IP addresses.

It is worth pausing to remind ourselves about the nature of our database. The database we are analysing reflects the VPN endpoint IP addresses presented to two UK-based services known to be targeted by VPN vendors. We can therefore expect to see a great deal of VPN vendor innovation applied to these services. For services not targeted by the VPN vendors, the database will be very different. We also expect the picture to vary across different countries.

Let's start to look at each type of IP address in more detail.

4.3 Hosting IP Addresses

Our initial analysis of the database provided a list of 16,600 hosting IP addresses. These IP addresses consisted of AWS IP addresses as well as data centre-hosting IP addresses. We look at these two types of IP addresses in the next two sections.

4.3.1 AWS Hosting

Our database contained 2,429 AWS IP addresses in total. All appear to be IP addresses from the eu-west-2.compute.amazonaws.com AWS region (which makes sense for targeting UK services).

Table 4-3 summarises which VPNs are presenting AWS IP addresses.

VPN Vendor	Number of IP Addresses Visited	Total Number of Visits
Watch UK TV Anywhere	1673	1709
Ivacy	701	702
PureVPN	617	618
VPNShazam	442	442
Privado	24	24
BolehVPN	15	15
Surfshark	10	10

Table 4-3 Top VPNs Using AWS IPs

Five further VPN vendors present AWS IP addresses, but in very small numbers.

Our analysis shows that few VPN vendors are presenting AWS IP addresses (12 out of 59 = 20%). However, "Watch UK TV Anywhere" is the biggest user of AWS IPs, followed by Ivacy, PureVPN and VPNShazam.

Comparing the number of IP addresses presented to the number of visits, we observe that AWS IP addresses are rarely re-used by VPN vendors. It is likely that VPN vendors regularly restart AWS instances in order to rotate IP addresses.

4.3.2 Non-AWS Hosting

Moving away from AWS, we can look at the other hosted IP addresses – 14,171 in total. Traditionally, VPN servers were hosted in data centres, so we expect to still see plenty of activity from hosted IP addresses.

Indeed, the most visited IP address in our database (see Table 4-2) is a hosting IP address used by Hotspot Shield.

Table 4-4 shows the top VPNs presenting hosting IPs.

VPN Vendor	Number of IP Addresses Visited	Total Number of Visits
Hotspot Shield	11835	18886
MonVPN	675	1348
HideIPVPN	564	923
Privado	479	499
Zenmate	221	279
NordVPN	183	364
AdGuard	161	184
UltraVPN	139	192
VPNUnlimited	130	130
PureVPN	112	112
SkyVPN	100	100
Surfshark	72	72
BolehVPN	64	64
Keenow	28	28
IWASEL	22	22
CyberGhost	22	27
Private Internet Access NextGen	12	12
FrootVPN	11	11
Ivacy	10	10
EasyHideIp	10	10

Table 4-4 Top VPNs Using Hosting IPs

One striking aspect to this data is the density of IP addresses in the database. The data suggests that VPN vendors are often allocated whole subnets allowing them to rotate through a range of IP addresses for presentation to the target OTT service. This is reflected in Table 4-4 – there is little re-use of IP addresses across visits.

For example, Table 4-5 shows IP addresses presented from a single hosting provider:

IP Addresses Visited	IP Addresses Visited

103.111.61.5	103.111.61.6	103.111.62.3	103.111.62.4
103.111.61.7	103.111.61.8	103.111.62.5	103.111.62.6
103.111.61.9	103.111.61.11	103.111.62.8	103.111.62.9
103.111.61.12	103.111.61.15	103.111.62.10	103.111.62.13
103.111.61.16	103.111.61.17	103.111.62.14	103.111.62.15
103.111.61.18	103.111.61.22	103.111.62.18	103.111.62.19
103.111.61.23	103.111.61.25	103.111.62.20	103.111.62.21
103.111.61.26	103.111.61.27	103.111.62.22	103.111.62.23
103.111.61.28	103.111.61.29	103.111.62.25	103.111.62.26
103.111.61.30	103.111.61.33	103.111.62.27	103.111.62.28
103.111.61.34	103.111.61.37	103.111.62.29	103.111.62.36
103.111.61.43	103.111.61.44	103.111.62.38	103.111.62.39
…	…	…	…

Table 4-5 Example IP Ranges for Hosting Provider

In total, our database contains 294 IP addresses from the subnets 103.111.61.0/24 and 103.111.62.0/24.

These IP ranges were used by both Hotspot Shield and UltraVPN, but not at the same time. UltraVPN only presented IP addresses from this range for a single day during the test period – Hotspot Shield used this range on 27 alternate days during the test period. This may suggest that subnets are re-allocated between VPN vendors over time as part of a strategy to avoid detection.

4.4 Residential IP Addresses

During testing, a total of 144,736 unique residential IPs were presented by VPN vendors. All major UK ISPs were represented in our test database. Table 4-6 shows the top 5 UK ISPs which contribute the majority of the residential IP addresses in the database:

ISP	Number of Residential IP Addresses Visited	Estimated Subscriber Base[2]
British Telecommunications PLC	38322	9.3 million
Virgin Media Limited	31308	5.6 million
Sky UK Limited	29396	6.7 million
TalkTalk	20365	4.2 million
Vodafone Limited	8028	1 million

Table 4-6 Observed IPs from the Top 5 UK ISPs

One of the key aims of this whitepaper was to establish that residential IPs were being used by VPN vendors, and also to confirm that these IP addresses were associated with genuine residential homes. We looked at various aspects of the data to confirm that these are indeed residential homes:

- The volume and density of the IPs – Simply put, there are a very large number of IP addresses in our database, and they span a huge number of networks. The high volume/low density suggests residential homes.

[2] Estimated subscriber base data taken from https://www.ispreview.co.uk/review/top10.php

- Geo-location vendor location confidence – For a large percentage of our dataset, our geo-location vendor has a high degree of confidence in the type and location of the IP address.
- Geo-location footprint – Results are shown below and cover the length and breadth of the UK. Again, this suggests residential homes.
- ISP outreach – We have contacted four major UK ISPs to validate a subset of our IP addresses. At the time of writing, two ISPs have responded and confirmed that our database contains IP addresses assigned by them to residential homes during the period of our testing.
- Local knowledge – Kingsmead has over 20 years' experience working with UK ISPs.

Figure 4-3 shows the geographical coverage of the residential IP addresses from our database. This map represents 113,748 IP addresses in 2,630 UK postcode districts (we discarded IP addresses where the location was identified with lower confidence by the geo-location vendor). As can be seen from the map, IP addresses span the length and breadth of the UK, and IP address density reflects UK population density.

Based on this information, we can be confident that the majority of these IP address are genuine residential homes in the UK.

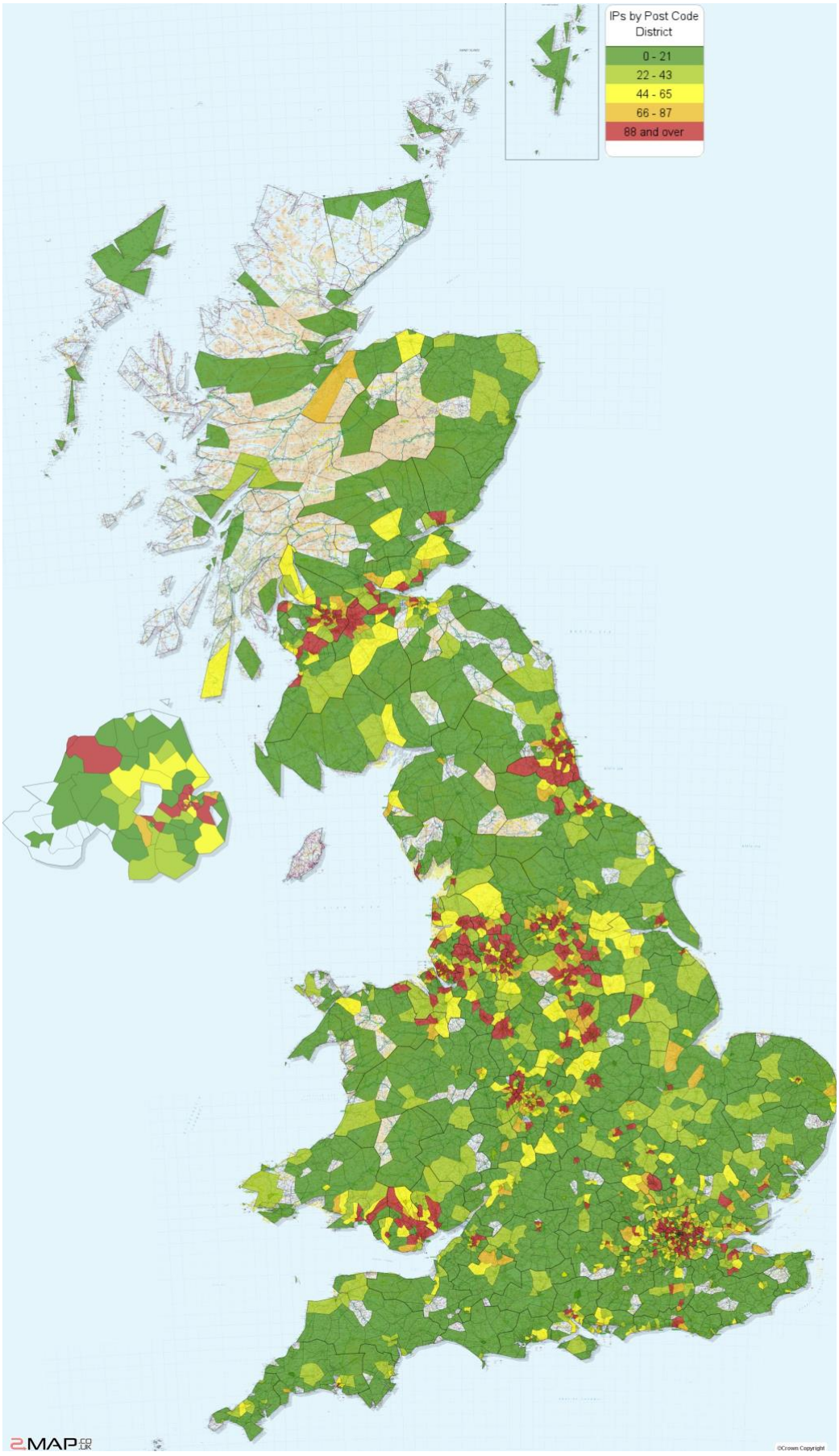

Figure 4-3 Geographical Coverage of Residential IPs

Table 4-7 shows the top VPNs using residential IPs.

VPN Vendor	Number of Residential IP Addresses Visited	Number of Visits	Average Visits per IP
Privado	93512	184829	2.0
MonVPN	20069	38426	1.9
VPNUnlimited	18202	21331	1.2
Surfshark	11350	43570	3.8
IWASEL	10307	10819	1.0
HideIPVPN	9990	14783	1.5
BolehVPN	8871	10703	1.2
NordVPN	7412	70460	9.5
PureVPN	2990	15368	5.1
Private Internet Access NextGen	2208	2360	1.1
IPVanish	1293	169811	131.3
Astrill	1117	1119	1.0
CyberGhost	1060	3572	3.4
Keenow	883	7205	8.2
Ivacy	690	29970	43.4
ProtonVPN	589	1845	3.1
StrongVPN	573	2040	3.6
VPNShazam	545	2870	5.3
Witopia	351	5410	15.4
Hotspot Shield	323	4225	13.1
BullGuardVPN	289	473	1.6
WindScribe	228	3471	15.2
HotBot	201	377	1.9
InternetShieldVPN	196	314	1.6
Hola!	186	1544	8.3
Private Internet Access	150	159	1.1
BritishTVAnywhere	102	1810	17.7
VyprVPN	68	507	7.5

Table 4-7 Top VPNs Using Residential IPs

Other VPNs also present residential IP addresses, but these are not listed as the numbers are lower. This includes ExpressVPN, who are also presenting residential IP addresses.

As we would expect from a large proxy network, the average number of visits to each IP address is relatively small. However, there are exceptions. IPVanish has an average number of visits to each IP address of 131.3 (79 of these IP addresses are visited over 500 times). Also, the VPN service VPNac deserves special mention. Only a single IP address visited by VPNac, but the IP is visited 2,820 times.

It is important to understand that the number of IP addresses visited may not represent the number of households visited. This is because ISPs have different strategies for IP address assignment, and a single household may have several IP addresses over time. For most households, their IP address is likely to change over a number of weeks. The number of households targeted by VPN vendors may therefore be lower than the number of observed IP addresses.

We cannot rule out cases where a business relationship has been established between a VPN or proxy vendor and an ISP to route traffic. Indeed, one of the smaller UK ISPs is significant:

- This ISP owns 387 IP addresses in our database (0.2% of IP addresses).
- This ISP is visited 47,493 times in our database (5.4% of visits).
- This ISP has 21 residential IP addresses in the top 50 most visited IP addresses (42% of the top 50).
- This ISP has an average number of visits per residential IP address of 126 (the average across all residential IPs is 4.5).
- Table 4-8 gives examples of some visited IP addresses from this ISP (in total our database contained 219 IP addresses from this /16 subnet). These examples contain several sequential IP addresses, which we would not expect to see across normal residential networks. Given that our testing will only visit a subset of available proxies, the density of IP addresses from this ISP is very high.

Visited IP Addresses From A Single /16 Subnet			
xxx.xxx.132.25	xxx.xxx.132.91	xxx.xxx.137.57	xxx.xxx.137.97
xxx.xxx.132.28	xxx.xxx.132.92	xxx.xxx.137.58	xxx.xxx.137.99
xxx.xxx.132.41	xxx.xxx.132.93	xxx.xxx.137.59	xxx.xxx.137.100
xxx.xxx.132.43	xxx.xxx.132.121	xxx.xxx.137.60	xxx.xxx.137.113
xxx.xxx.132.44	xxx.xxx.132.122	xxx.xxx.137.73	xxx.xxx.137.117
xxx.xxx.132.66	xxx.xxx.132.124	xxx.xxx.137.81	xxx.xxx.137.118
xxx.xxx.132.75	xxx.xxx.132.129	xxx.xxx.137.82	xxx.xxx.137.129
xxx.xxx.132.76	xxx.xxx.132.210	xxx.xxx.137.83	xxx.xxx.137.132
xxx.xxx.132.89	xxx.xxx.132.211	xxx.xxx.137.84	xxx.xxx.137.226
xxx.xxx.132.90	xxx.xxx.132.219	xxx.xxx.137.85	

Table 4-8 Selection of Visited IPs from a Smaller UK ISP

This ISP has a relatively low number of IP addresses in our database, but the IP address density is high, and the number of visits is high. Of course, this concentration of activity may simply reflect the type of network offered, and the demographic of the ISP customer base. However, this may be an area for future research.

4.5 Cellular IP Addresses

In total, 8,136 unique cellular IP addresses were presented by VPN vendors during testing. This shows that VPN vendors will leverage any IP connected device for traffic routing regardless of connectivity type (DSL, fibre, cellular, etc).

Table 4-9 shows the number of IP addresses presented from the top four UK cellular operators. Many other cellular operators were presented in the database, but the number of visits was small.

Operator	Number of Cellular IP Addresses Visited
Telefonica O2 UK	2207
EE Limited	1811

Vodafone Limited	1738
Three	1628

Table 4-9 Observed IPs from the Top UK Cellular Operators

Today, cellular networks are used by a variety of devices, including personal devices and mobile hotspots. This makes interpreting cellular results more difficult. IP address analysis is also complicated by the fact that the main UK mobile networks all use carrier-grade NAT, where a large number of cellular devices share a relatively small number of public IP addresses.

As cellular IP addresses make up only 5% of our database IP addresses, and only 2% of our visits, we will not analyse this data any further.

4.6 Other IP Addresses

Our database also contained 2,315 other types of IP addresses, including businesses, education, government, and a number which were of unknown type.

We did not analyse this data in any detail but note that hosting proxies within these network types would suggest a serious security violation for some of the organisations involved.

4.7 Shared IP Addresses

To conclude our analysis, we looked at how IP addresses are shared across VPN vendors. We found that:

- 3 IP addresses were shared across 9 VPN vendors.
- 12 IP addresses were shared across 8 VPN vendors.
- 83 IP addresses were shared across 7 VPN vendors.
- 166 IP addresses were shared across 6 VPN vendors.
- 419 IP addresses were shared across 5 VPN vendors.

Of these IP addresses, 86% are residential IPs and a further 8% are cellular (the remainder have various classifications).

In total, 42,606 IPs were shared across more than one VPN vendor. Table 4-10 gives some examples of shared IP addresses:

Observed IP	Type	ISP	Visits by VPN	
xxx.xxx.100.241	Residential	TalkTalk	992x IPVanish 6x StrongVPN 4x HideIPVPN 2x VPNHub 2x NordVPN	11x WindScribe 6x MonVPN 3x InternetShieldVPN 2x Privado
xxx.xxx.164.69	Residential	Sky UK Limited	308x IPVanish 9x PureVPN 4x VPNShazam 2x StrongVPN 1x Privado	34x Ivacy 6x MonVPN 4x NordVPN 2x HideIPVPN
xxx.xxx.180.156	Cellular	Three	10x Ivacy 2x VPNShazam 2x MonVPN	5x Privado 2x PureVPN 2x HideIPVPN

			1x NordVPN 1x BolehVPN	1x IWASEL
xxx.xxx.232.2	Residential	Sky UK Limited	686x IPVanish 4x MonVPN 3x HideIPVPN 1x Privado	17x StrongVPN 3x NordVPN 1x VPNHub 1x InternetShieldVPN
xxx.xxx.201.173	Cellular	Three	239x IPVanish 4x Privado 3x VPNHub 1x Surfshark	9x NordVPN 4x MonVPN 3x StrongVPN 1x HideIPVPN

Table 4-10 Example IPs Shared Across VPN Vendors

Sky UK Limited confirmed that the IP address xxx.xxx.164.69 in the table above was indeed a Sky UK residential customer IP address during the time of the test.

Table 4-11 shows an extract from visit activity for the first two IPs above:

Observed IP	Date/Time of Visit	VPN Visiting
xxx.xxx.100.241	2022-07-15 01:04:06 2022-07-15 01:15:09 2022-07-15 01:15:09 2022-07-15 01:15:09 .... 2022-07-15 02:48:27 2022-07-15 02:48:27 2022-07-15 06:25:04 2022-07-15 06:25:04 2022-07-15 06:25:04 2022-07-15 06:25:04 2022-07-15 12:40:32 2022-07-15 12:40:33 2022-07-15 13:01:09 2022-07-15 13:29:00 .... 2022-07-15 14:27:00 2022-07-15 14:27:00 2022-07-15 18:21:24 2022-07-15 18:21:24 2022-07-15 18:26:42 2022-07-15 18:26:42 2022-07-15 18:26:42 2022-07-15 18:26:42 2022-07-15 19:04:03	IPVanish IPVanish IPVanish IPVanish .... IPVanish IPVanish WindScribe WindScribe WindScribe WindScribe VPNHub VPNHub IPVanish IPVanish .... IPVanish IPVanish WindScribe WindScribe WindScribe WindScribe WindScribe WindScribe MonVPN
xxx.xxx.164.69	2022-07-21 00:41:36 2022-07-21 00:42:04 2022-07-21 00:43:52 2022-07-21 01:46:52 2022-07-21 03:09:57 2022-07-21 04:41:26 2022-07-21 04:41:26 2022-07-21 04:45:35 2022-07-21 04:47:00 2022-07-21 06:53:29	PureVPN PureVPN Ivacy Ivacy Ivacy PureVPN PureVPN Ivacy Ivacy VPNShazam

	2022-07-21 06:53:29	VPNShazam
	2022-07-21 08:43:43	Ivacy
	2022-07-21 09:44:29	Ivacy
	2022-07-21 12:59:52	VPNShazam
	2022-07-21 13:37:55	Ivacy
	2022-07-21 13:47:49	Ivacy
	…	…
	2022-07-21 15:43:02	Ivacy
	2022-07-21 15:48:09	Ivacy
	2022-07-21 15:57:11	VPNShazam
	2022-07-21 19:46:22	Ivacy
	2022-07-21 19:46:22	Ivacy
	2022-07-21 19:48:59	Ivacy
	2022-07-21 23:39:13	MonVPN

Table 4-11 IP Address Activity Over Time

The first IP address was visited by IPVanish, WindScribe, VPNHub and MonVPN on the same day.

The second IP address was visited by PureVPN, Ivacy, VPNShazam and MonVPN on the same day.

Although it is possible that these IP addresses are hosting multiple proxies, we believe that it is more likely that multiple VPN vendors are using the services of a common proxy network. A single proxy installation in a home can therefore serve several different VPN vendors.

4.8 Conclusion

We have seen that VPN vendors are using a variety of solutions to route OTT service traffic:

- Data centre-hosted servers
- AWS-hosted servers
- Residential proxies

Residential proxies are now in widespread use across a number of VPN vendors. For targeted OTT services, we have observed that most of the traffic is presented using residential proxies. These proxies are installed in tens of thousands of homes across the UK. Many of these proxies appear to be shared across VPN vendors, indicating that third-party proxy network suppliers are used, or that VPN vendors within the same conglomerate[3] are sharing a proxy network built and operated internally.

5 Technology Deep-Dive

In this section we explore how VPN vendors fit all the components together.

5.1 Traffic Routing using DNS

All OTT services are built from a variety of sub-domains which are visited as a user navigates a service. Some OTT services have only a few sub-domains, while others have many. As an example, let's imagine an OTT service `www.myottservice.com` which is actually built from several subdomains:

- `www.myottservice.com` – Main service entry point.
- `auth.myottservice.com` – Provides login/authentication services.
- `navigation.myottservice.com` – Provides service navigation services: browse, search, etc.
- `playout.myottservice.com` – Provides content playout services.

[3] https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/

- `ads.myottservice.com` – Provides advertising services.
- `cdn.myottservice.com` - Provides content delivery.

In most services, only a subset of these sub-domains will perform geo-location/VPN detection checks. If the service does not perform these geo-checks on a sub-domain, then those sub-domains need not be routed through proxy servers.

VPN vendors have different strategies around this, but it is clear that at least some VPN vendors carefully analyse the target OTT service and only route the minimal amount of traffic through proxies.

Here are two examples of real services (we've changed the domain names to anonymise the service).

5.1.1 OTT Service #1

Several sub-domains are used by this service, as listed in Table 5-1.

Domain	Usage	Geo-Check on Domain?	DNS Override?		
			ExpressVPN	NordVPN	Surfshark
`service.com`	Top Level	No	No	Yes	Yes
`service.tv`	Top Level	No	No	No	Yes
`metadata-feed.service.com`	Metadata	No	No	No	Yes
`metadata-api.service.com`	Metadata	No	No	No	Yes
`user-data.service.com`	User Management	No	No	No	Yes
`user-api.service.com`	User Management	No	No	No	Yes
`config.service.com`	Service Config/DRM	Yes	Yes	Yes	Yes
`apps.service.com`	Application Hosting	No	No	No	Yes
`ads.service.com`	Ads	No	No	No	Yes
`images.service.com`	Images	No	No	No	Yes
`thumbnails.service.com`	Images	No	No	No	Yes
`log.service.com`	Service Telemetry	No	No	No	No
`ondemand-cdn.service.com`	CDN	No	No	Yes	Yes
`live-cdn.service.com`	CDN	No	No	Yes	No

Table 5-1 DNS Manipulation of OTT Service #1

The service provider performs geo-restriction and VPN detection only on the domain `config.service.com`.

ExpressVPN has chosen to reroute only the domain `config.service.com`, as this is the only service that performs geo-checking. NordVPN chooses to reroute CDN traffic too, and Surfshark reroutes almost all traffic.

The domain `config.service.com` is significant here. This domain appears to be used to download service configuration data and DRM licenses only. This is very low-volume traffic and relatively insensitive to latency. This makes life easy for the VPN vendor – their proxy network need only re-route a very small amount of traffic, and their standard VPN servers can take all the high-volume traffic.

When only a subset of domains is re-routed, an OTT service provider will observe a single device presenting different IP addresses across different service domains. For example, `config.service.com` may present a residential IP address, but `log.service.com` may present a VPN server IP address.

5.1.2 OTT Service #2

Another OTT service we have reviewed also has a wide range of domains within its service. However, one domain is of specific interest:

```
geo-location.geo-vendor.com
```

This is not a domain owned by the OTT service but is a domain owned by one of the OTT service vendors (the domain name has been changed to anonymise the vendor). The browser itself queries this vendor domain to obtain the geo-location of the device (country, city, etc).

It is not good practice for client-side applications to perform geo-location checks, but it is interesting to observe that NordVPN and Surfshark are targeting this domain with proxies. Clearly, VPN vendors are not only targeting OTT services, but also some of their technology suppliers too.

Table 5-2 shows how these VPN vendors are targeting this geo-location vendor domain across a range of countries. This careful targeting will disrupt geo-location activities for a variety of web applications, not just OTT streaming services.

Target Country	DNS Override?	
	NordVPN	Surfshark
United Kingdom	Yes, 192.0.0.57	Yes, 92.249.37.82
United States	Yes, 192.0.0.108	Yes, 92.249.37.52
Spain	Yes, 192.0.0.54	Yes, 92.249.37.25
Netherlands	Yes, 192.0.0.56	Yes, 92.249.37.48
Italy	Yes, 192.0.0.96	Yes, 92.249.37.218
Canada	Yes, 198.18.1.201	Yes, 92.249.37.84/92.249.37.24
Ireland	Yes, 198.18.1.180	Yes, 92.249.37.13
France	–	Yes, 92.249.37.5
Germany	–	Yes, 92.249.37.23

Table 5-2 DNS Manipulation of a Geo-location Vendor

Both NordVPN and Surfshark have deployed country-specific proxy servers to re-route this geo-location traffic.

The IP addresses used by NordVPN (192.xxx.xxx.xxx and 198.18.xxx.xxx) are reserved IP addresses and not publicly routable. NordVPN must therefore be using a private network to route this traffic.

Surfshark is taking a different approach. The 92.249.37.xxx IP addresses are hosted in a data centre in the British Virgin Islands.

5.2 Proxy Types

Our study has found evidence of the following types of IP address:

- Data centres
- AWS
- Residential homes

It is likely that residential homes are being reached in many cases by utilising third-party services such as Oxylabs, Smartproxy, EarthWeb, IPBurger, SOAX and GeoSurf. These, and many other similar businesses, have been supporting the web industry for several years. They provide a range of services including access to residential proxy networks. These companies acquire these residential proxies through a variety of means, although reputable companies strive to do so using ethical means.

Oxylabs has a handbook describing residential proxy sourcing which may be of interest to the reader:

https://oxylabs.io/Oxylabs_Residential_Proxy_Acquisition_Handbook.pdf

The major questions around sourcing residential proxies are around user awareness and user consent. We will not explore these issues further in this whitepaper; suffice to note that residential users who share their bandwidth are opening their homes to many risks:

- Malware/ransomware infection
- Data loss/private data theft/blackmail
- Use of bandwidth for illegal activity

Proxy network services can be costly to use. Although VPN vendors almost certainly negotiate customised deals with proxy network operators, publicly available pricing gives some insight into the prices involved. Smartproxy and Oxylabs offer a range of pricing options, but typically charge a monthly fee of between $0 and $5,000, then charge between $4 and $12 per Gigabyte of data (higher monthly fees bring down data fees).

A two-hour Ultra HD movie on Netflix is around 13 Gbytes. It is hard to see how routing an Ultra HD movie using these proxy products makes economic sense. We suspect that VPN vendors are relying on routing high-volume traffic such as video content via data centre proxies only and routing as little traffic as possible through residential proxies. Only then does it make economic sense. In addition, the larger VPN vendors may be exploring options for building their own proxy networks to reduce costs.

5.3 Proxy Routing

Take the following example to CyberGhost DNS resolution for two major UK OTT services:

- www.service1.com 10.0.0.243
- www.service2.com 10.0.0.243

The proxy server will receive traffic for both those services but must forward traffic to the correct target server. Almost all OTT service traffic today is HTTPS. HTTPS requires the browser and the OTT server to negotiate a secure TLS connection, which authenticates the server's certificate and negotiates encryption configuration. A major concern is that these proxy networks are intercepting and decrypting HTTPS traffic, which would be a security nightmare. We will show that these proxy servers act as a simple IP router only, and the security of HTTPS is not compromised when traffic is routed via proxies.

Proxy server technology will vary across VPN vendors, but a proxy server could be set up to operate as follows:

- For proxy servers routing a single target domain, all traffic (HTTP or HTTPS) can simply be forwarded to the target domain.
- For proxy servers routing multiple domains, the server needs to work out where the traffic should be sent. A little more work is therefore required:
    - For HTTP traffic, the proxy server can inspect the traffic it receives as it is not encrypted. The proxy can easily identify the server that the client wishes to connect with and forward the request as required.
    - For HTTPS traffic, the proxy server can snoop on the TLS handshake and extract the Subject Name Indication (SNI) field from the TLS ClientHello message. The SNI field is sent by the client before the TLS starts encrypting the traffic and contains the server's name that the client wishes to connect with. By inspecting the SNI field, the proxy server knows the target server and can then proceed to route the rest of the TLS handshake traffic and all the subsequent encrypted data to the correct server. Critically, the SNI snooping does not interfere with the security of the HTTPS connection in any way. These types of proxies are often termed SNI proxies.

Using these techniques, the proxy server will always know where to route traffic, without impacting the network traffic security.

Once the target server is known, the VPN vendor may wish to further route traffic via an AWS-hosted proxy or a residential proxy network. If so, the traffic will typically be forwarded using SOCKS (short for SOCKet Secure). A SOCKS proxy is a very simple IP-level packet router which receives IP traffic, then forwards it to the target server. SOCKS5 proxies (the latest version) can route any type of traffic, can be easily installed on an AWS server or on a consumer device, and can be a very efficient method for routing large amounts of traffic. Other methods are available for

routing traffic through residential homes, but SOCKS5 proxies are a popular method for anonymising traffic on the Internet[4].

The VPN vendor therefore has two opportunities to decide how to route a client connection:

- Manipulate DNS entries to route traffic from traditional VPN servers to proxy servers.
- Use HTTP or HTTPS/SNI inspection within the proxy server to make further routing decisions.

As we have seen, the VPN vendors can ultimately decide to route traffic:

- Via the VPN server.
- Via a data centre-hosted proxy server.
- Via an AWS-hosted proxy server.
- Via a residential proxy network.

At each step, the VPN vendor can make traffic routing decisions based on the domain name of the service they are targeting. There is no inspection of user data in this process, and the security of HTTPS is preserved.

5.4 Illustrated Proxy Network

Figure 5-1 illustrates a proxy architecture which may be deployed by a VPN vendor. Architectures will vary across VPN vendors, but this illustration allows us to understand how a theoretical VPN vendor could optimise its proxy network to avoid detection and balance operational costs.

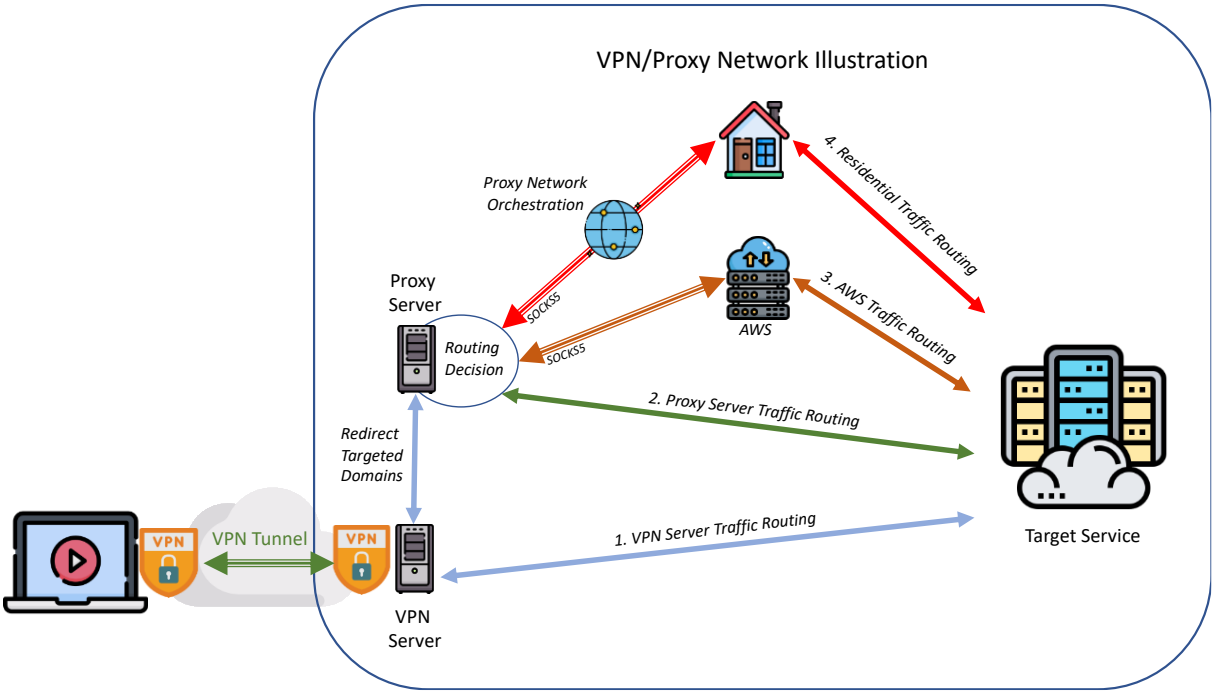

Figure 5-1 Illustrated Proxy Network Architecture

The proxy server in the illustration identifies the target domain for a request (see Section 5.3) and decides how best to route that traffic.

Overall, there are four possible methods to route traffic, as listed in Table 5-3:

Server Type	Observations
1. VPN Server	Cheapest option for VPN vendors, as servers are shared across all services and optimised for high bandwidth.

[4] For some insight into the darker side of residential SOCKS proxy services, we recommend reading some recent articles from Brian Krebs, including: https://krebsonsecurity.com/2022/08/no-socks-no-shoes-no-malware-proxy-services

	Easiest for VPN detection vendors to spot. Default routing option for VPN vendors if traffic is not blocked by OTT services.
2. Proxy Server	Used by VPN vendors if their VPN servers are blocked. Higher operational cost for VPN vendors as servers may not be shared and server load may be higher due to traffic inspection and routing decisions. Preferred option for VPN vendors if VPN servers are blocked by OTT services.
3. AWS Proxy	This option is not heavily used by VPN vendors but remains available when the OTT services are not blocking AWS IP addresses.
4. Residential Proxy	Used by VPN vendors if all other options are blocked. Highest operational cost for VPN vendors. Only economic if the volume of traffic can be minimised to specific domains only.

Table 5-3 Illustrated Proxy Network Routing

The VPN vendors will be continuously monitoring OTT services to ensure their VPN service continues to provide access to the OTT services. Any updates to the OTT service will have to be reflected in the configuration of the proxy network.

A level of automation is likely. For example, a VPN vendor may continuously monitor geo-checked APIs in the OTT service to detect blocking. If the OTT service starts to block a proxy server IP address, automated processes could re-configure the proxy server to present a different IP address without any manual intervention.

6 Recommendations

As we have seen in this whitepaper, many VPN vendors are using a variety of methods to route OTT service traffic:

- Hosted VPN servers
- Hosted proxies
- AWS-hosted proxies
- Residential home proxies

The use of residential home proxies is widespread and growing. This presents two challenges for OTT service providers. First, detecting residential proxies is difficult as traffic from these IP addresses may be indistinguishable from genuine user traffic. Second, blocking residential proxies can be problematic as it can lead to unintentional blocking of genuine users (who may not even be aware they are hosting a proxy).

Since blocking residential IPs can have a detrimental impact on genuine users, it is important to ask the question: “If I spot a residential IP address suspected of hosting a proxy, what do I do about it?”. This will determine your response a great deal.

We recommend four possible responses:

Defend

The aim here is to make your OTT service as challenging as possible for a VPN vendor to target with residential proxies. We aim to target their weakest links – they rely on DNS to target services, and routing high-volume services via proxies is expensive.

- Do all geo-checks server-side. Never use client logic to make geo decisions.
- Ensure geo-checks are present on all important service endpoints in your service.
- Ensure that geo-checks exist on your CDN and make sure checks are performed throughout streaming. VPN checks on the CDN force the VPN vendors to route video traffic via proxies.
- Consider tying authentication tokens to IP addresses so that a single streaming session can only be consumed from a single IP address. This could have a detrimental impact on users if they legitimately change their IP address during a streaming session (for example, a network change or cellular device-based

streaming) but this does force the VPN vendor to route all traffic via the same IP address. This could be useful if applied to CDN authentication tokens. Your service API can perform geo-checks on an IP address, then issue a CDN authentication token which ties the media delivery to that IP address only.

- Review the domains in use in your service to make it harder for a VPN vendor to detect specific traffic via DNS. As an extreme example, if your service is entirely routed to a top-level domain such as `www.service.com`, then the VPN vendor is required to route everything via proxies.

Note that technologies such as DoH (DNS-over-HTTPS) or DoT (DNS-over-TLS) may disrupt the ability for VPN vendors to manipulate DNS. This may be an area of future exploration.

Understand

The aim here is to make sure your service is setup to gather information that is useful for detecting VPN activity.

- Make an API available to extract IP address information from your service. Make sure this API is on a geo-checked domain.
- Ensure that you log IP address information along with your other service telemetry. This can be used to spot suspicious activity which may warrant further investigation:
    - Users hopping between multiple IPs when navigating your service during a single session.
    - Large numbers of users connecting from a single IP.
    - Users connecting from unexpected IP ranges – AWS or hosting data centres.
    - Users moving location in impossible times.
- Regularly review the VPN market for vendors claiming to avoid detection by your service. Web searches for "Top VPNs for Streaming" or "Best VPN for *Your Service*" will give insight into those vendors targeting you.

Respond

The aim here is to increase the blocking rates on your service.

Note: Measures to increase blocking rates can be very effective but can have a detrimental impact on genuine users. Caution is required.

- Select and integrate a reputable VPN detection vendor. Ensure that any downloaded databases are kept up to date by updating at least daily.
- If you block a connection, provide clear messaging to the user, and give an escalation route for them to report issues. Mistakes can happen.
- Consider blocking hosting providers suspected of hosting VPN servers as well as IP addresses of known VPN servers. Some VPN detection vendors have this functionality.
- Consider blocking AWS IPs (and other cloud providers). There is little reason for a genuine user to use these services to route traffic.
- Consider blocking all hosting providers. This carries a real risk of blocking genuine users, so this option requires an escalation route for users to report issues.

Finally, consider your response to residential (or cellular) IPs suspected of hosting proxies:

- Since the IP address of a residential home can change at any time, how confident are you that this decision is correct? Further, if the ISP is using carrier-grade NAT (many cellular networks do), can you know anything at all?
- Do you need to take further validation steps before taking action? What are those steps?
- Should you report the issue to the user in some way, or block them?
- If reporting the issue to the user, are you aiming to raise awareness of a possible issue, or do you want the user to take action? What actions?

Educate

More generally, the OTT industry should play some part in the education of consumers regarding the risks involved in hosting proxy servers. Many will not even be aware that they are doing this.

Ask yourself a simple question: Is my home hosting a proxy server?

Kingsmead Security Ltd

Web: www.kingsmeadsecurity.com

Email: contact@kingsmeadsecurity.com

Conclusion

This whitepaper has given some real insight into the technologies used by VPN vendors to avoid detection. Using residential homes and cellular devices to route traffic is a game-changer for the industry which must react to the challenge this brings. Our analysis showed that tens of thousands of residential homes are integrated into vast proxy networks, which are used by multiple VPN vendors.

Simply blocking these IP addresses is unlikely to be an acceptable answer for OTT service operators. Hundreds of thousands of genuine users could be denied service if this step was taken.

Our recommendations (in Section 6) provide some options for OTT service operators. Actions aimed at making life more challenging for the VPN vendors and actions aimed at data gathering are strongly recommended. Actions for increasing levels of service blocking are available, but some need careful impact analysis.

We remain concerned about the impact of these services on the individuals hosting these proxies in their home. Many will not be aware that they are routing traffic for anyone, anywhere who seeks to conceal their activity. We believe that user awareness should be part of the industry strategy going forward.

For independent advice on protecting your OTT service, please contact Kingsmead Security at contact@kingsmeadsecurity.com or visit www.kingsmeadsecurity.com.

Kingsmead Security Ltd is an independent content security consultancy serving the TV and film industry. We support content owners, service providers and technology vendors to protect movie, sports and other premium content.