Design advantages of the ZTNA model: Architectural Evolution for More Secure and Efficient Remote Access

MSc Research Project
MSc in Cybersecurity

Lorenzo Lombardi
Student ID: x22198024

School of Computing
National College of Ireland

Supervisor: Dr. Ross Spelman

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Lorenzo Lombardi……………………………………………………………………………………

Student ID: x22198024……………………………………………………………………………………..……

Programme: MSc in Cybersecurity……………………………… **Year:** 2023-2024……

Module: MSc Research Project…………………….……………………………………….………

Supervisor: Dr.Ross Spelman…………………………………………………………………………………

Submission Due Date: 2024/08/12……………………………………………………………………………….……

Project Title: Design advantages of the ZTNA model: Architectural Evolution for More Secure and Efficient Remote Access

Word Count: ……………………………………… **Page Count**…………………………………………….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ………………………………………………………………………………………………………

Date: 2024/08/11……………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Design advantages of the ZTNA model: Architectural Evolution for More Secure and Efficient Remote Access

Lorenzo Lombardi
x22198024

Abstract

In recent years, several companies have faced major changes in their network due to new challenges regarding network security. Most of these companies massively increased their number of remote workers due the Covid-19 pandemic. If the remote access was a plus in the past, nowadays it is a required benefit for all those employees that look for a better work life balance. Since workers are the weakest link in the cybersecurity chain, the remote access makes these challenges even harder than ever. It's a common thought, and widely demonstrated, that social engineering is still one of the worst threats in cybersecurity landscape because either of the unpredictable behaviour of human beings and the most sophisticated attack techniques that can take advantage of the modern Artificial Intelligence capabilities too. Because of this, security connectivity between remote users and companies has important implications. Even if remote access solutions have been largely used for years, it's now a critical point more than ever since it is now available not only for technical personnel but for all those ones that just need to access to the company resources stored in a private datacentre or in a public cloud.

Several kinds of solutions have been developed during the years, and among the most used there are the remote access tools like VPN. Some of them are reliable providing good performance but it's time to consider that further precautions are needed and maybe upgrade those solutions following new security standards.

The legacy approach is called also "Castle-and-moat". Once the user gets the network access can reach several destinations on the same network segment.

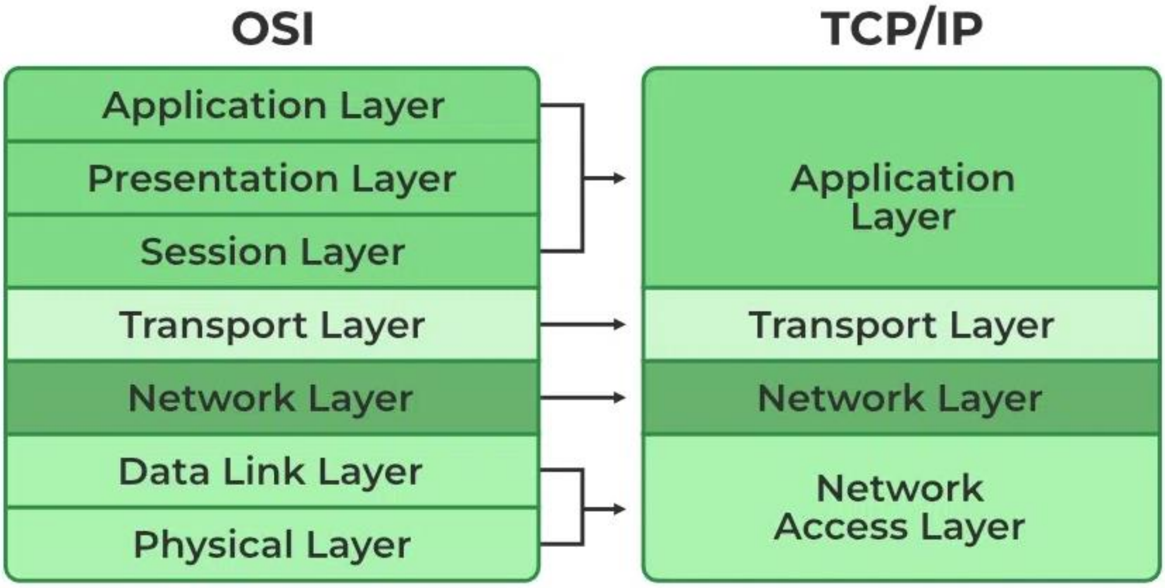
On the other hand, the new approach starts from the assumption that everybody and everything can be potentially a threat, regardless of the source place. You must consider the refinement of technical solutions in the field of cyber threats, the possibility of exploiting systems vulnerabilities, the ease of careless action of the user opening a phishing-type email. You need to be aware that a device or account breach could be absolutely hidden for a long time before it is discovered.

Starting from this awareness, a new approach is not just a choice but it's a needed action to stay competitive against the cybersecurity threats, and it may be an opportunity to seize advantages of the new model: the Zero Trust Network Access (ZTNA).

***Keywords**: Cyber Threats, VPN, ZTNA, Network Design, New Security Model.*

1 Introduction

Concerning remote access solutions, the Virtual Private Network (VPN) is certainly one of the greatest and most widespread examples. VPN is a technology that allows remote access by taking advantage of its network architecture features. This kind of solutions are a virtual overlay on lower layer and provide a private environment over another one. Contrary to popular belief, VPNs do not provide security features by default [1]. For instance, there is not confidentiality in L2TP, MPLS, IPSEC without ESP (Authentication Header only), but they need to work in synergy with further protocols and algorithms that make the VPN secure. Over a public network, the internet, a VPN can be configured between two specific endpoints by encapsulating data at some point of the ISO/OSI or TCP/IP model hiding the underlying: it connects, or it merges private networks physically separated. The most popular VPNs work at network level (like the IPSEC VPN) or at application layer (like the SSL VPN).



[2]

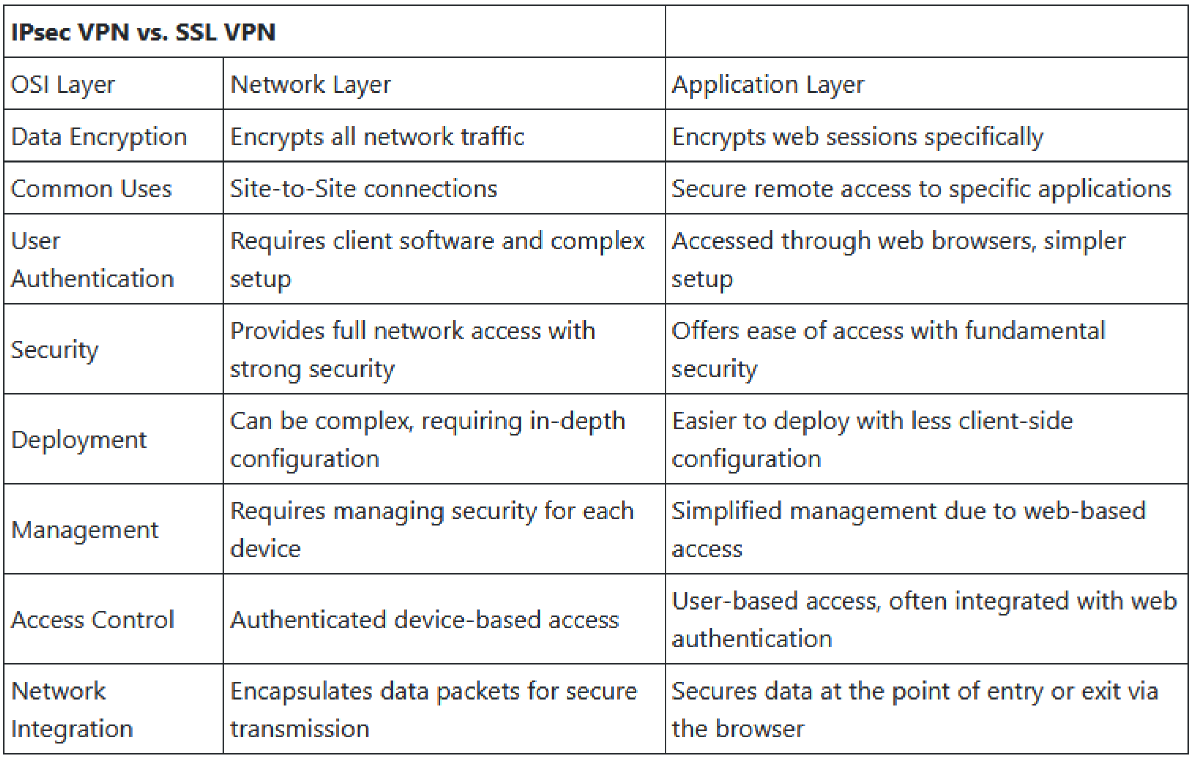
SSL VPN: it works at the application layer. It’s used for remote access only and it’s vendor specific. Initially it was web browser native, but then most important network security vendor, like Cisco and Juniper, applied this technology for a complete tunnelling solution [3].

IPSEC VPN: it works at the network layer. It’s vendor agnostic and it can be configured both for remote access and site to site purposes. High performance, more complicated to configure. They are massively used to establish connection between sites and companies.

Both can be configured to work with the following configuration:

- *FULL TUNNELING*: all the traffic is encapsulated into the tunnel. In the remote access case, the user traffic can be monitored because all his traffic is passing through the company firewall, but this causes a high level of usage of the company internet bandwidth.

- *SPLIT TUNNELING*: only the chosen networks are exchanged via tunnel to forward the interested traffic, the other traffic follows the default route.



IPsec VPN vs. SSL VPN		
OSI Layer	Network Layer	Application Layer
Data Encryption	Encrypts all network traffic	Encrypts web sessions specifically
Common Uses	Site-to-Site connections	Secure remote access to specific applications
User Authentication	Requires client software and complex setup	Accessed through web browsers, simpler setup
Security	Provides full network access with strong security	Offers ease of access with fundamental security
Deployment	Can be complex, requiring in-depth configuration	Easier to deploy with less client-side configuration
Management	Requires managing security for each device	Simplified management due to web-based access
Access Control	Authenticated device-based access	User-based access, often integrated with web authentication
Network Integration	Encapsulates data packets for secure transmission	Secures data at the point of entry or exit via the browser

[4]

These solutions have worked for a long time and still work well for most companies. The SSL VPN is more focused on the remote access side while the IPSEC are the standard de-facto of the site-to-site scenario. Focusing on the remote access, new security models have emerged today, and it is time to rethink remote access security by considering a new paradigm. Looking at the legacy VPNs, a network technology thought to create communications eventually become even secure, the new standard starts from the concept that nothing and nobody can be trusted on principle but, after rigorous and continuous checks, it can be allowed to access only those things are supposed to be allowed. This approach adds several security elements that must work together to guarantee a holistic view of the network infrastructure but at the same time provide a chance to optimize some solutions that have been the result of years of development and continuous addition.
Here the ZTNA approach starts.

How can the ZTNA model enhance security, improve resilience and optimize network performance?

2 Related Work

Looking for the ZTNA principles and implementation examples among Vendors and research papers [5] [6] it comes out that in the legacy network infrastructure, your place in the network gave you and defined the permission to access to specific resources. Conversely, the ZTNA transcends network position. This big change allows the network architects to deploy new solution, based on the identity, that can be flexible and adaptive because they are free from any network logic.
There are several articles that compare legacy VPN solutions and ZTNA. Looking at them, it’s quite clear that the ZTNA approach could be applied to the VPN solutions as well. The ZTNA is a new concept that aims to guide and resolve the new security challenges that companies must face, not just by adding a further overlay but changing the starting point of the new security network design. The main advantage is that nowadays we already have several tested and reliable tools and protocols that are useful to reach specific goals to accomplish new security needs. Now it’s possible to rethinking all of them working together with the best optimization trying to eliminate overlaps that in the legacy infrastructure had to be per design constraints.

Looking at the biggest players in the world, below some interpretation of the ZTNA concepts.

Google defines three of the most important elements of ZTNA [7]:

- Assume all network traffic is a threat, at all times
- Enforce least-privileged access
- Always monitor

On the other hand, Microsoft focus the ZTNA revolution on the identity and the authentication effectiveness [8]:

- The foundation of Zero Trust security is the identity. Both users and devices.

The ZTNA is not a condition, it’s more a trip towards a new model. Just a new network infrastructure build from scratch could reach a complete level of ZT.
In this regard, Fortinet introduces a hybrid model that guides migration from legacy VPN to the ZTNA approach [9][10].

I think that comparing VPN and ZTNA is not fair just because the first one is a technology, and the second one is a model. It does not make sense to me comparing their features because, for instance, it’s possible to implement ZT logic within a VPN implementation. There could be several elements of the ZTNA in a VPN solution such as:

- continuous monitoring
- posture checking
- session-based rules
- least privileges
- micro segmentation and horizontal firewall
- Single Sign On
- Multi-Factor Authentication
- Endpoint Detection & response

ZTNA it’s not just a model but it is something about awareness of security risk, sooner or later it must be adopted.
And it’s even more: it’s a *Game Changer*.
I aim to highlight those key aspects of ZTNA that can be interesting from a design point of view: they can justify the migration to this model, and they could be applicable to most of the legacy infrastructures.
Because of this, I’m going to analyse those specific characteristics that make the ZTNA a game changer for the security infrastructures. I mean those native peculiarities that are not applicable in the old scenario that might go unnoticed or secondary but could be a real improvement of the new approach.
Finally, it’s important to consider that overlying structures and complex implementations can weigh down the chosen solution and make it less performant. A new challenge is also finding a design that provides the strongest security and a safe approach, and at the same time, improving the user overall experience.

3 Research Methodology

Since ZTNA is not a technology or a simple protocol, neither a recognized standard (not yet at least) the first thing to do is to identify the common pillars among the security Vendors and the definitions of the most authoritative frameworks. I started from the NIST SP 800-207 [11] and then I had a look at the most important Vendors interpretation of this new model. As often happens in IT, a new technology is unlikely to arise from scratch.
Often the Vendors Sales talk about a new revolutionary solution that has just came out, when it is mainly the optimization of several previous technologies that eventually can work together in synergy. For example, let's take in consideration the SD-WAN: it's revolutionary and incredibly cost-effective but in the end it's the standardization of older technologies like Dynamic IPSEC VPN, policy routing, probing and traffic steering. In the past you could build something similar on your own with a huge effort and likely with a low level of resilience. The standardization and the simplification of older technologies can bring to new technical solutions.
The interesting things about ZTNA is that this is just the beginning of a new model, but several considerations are already carried out.

From NIST definition, the main principles are:

- Everything, potentially, is a threat.
- All data sources and services are considered resources
- Every communication must be secured, regardless the network location
- Access is allowed per-session basis
- The enterprise is aware and monitors the integrity and security of all assets (owned and guest/BYOD)
- Continuous monitoring and verification
- Authentication and authorization are required before any access is allowed.
- Least privileges principle applies to all the resources.
- Micro segmentation

My research is focused on a specific but very common situation, where a corporate network needs to provide access to sensitive services that could be hosted on-premises or in cloud.
I Looked for some vendor solutions and how they are implemented.

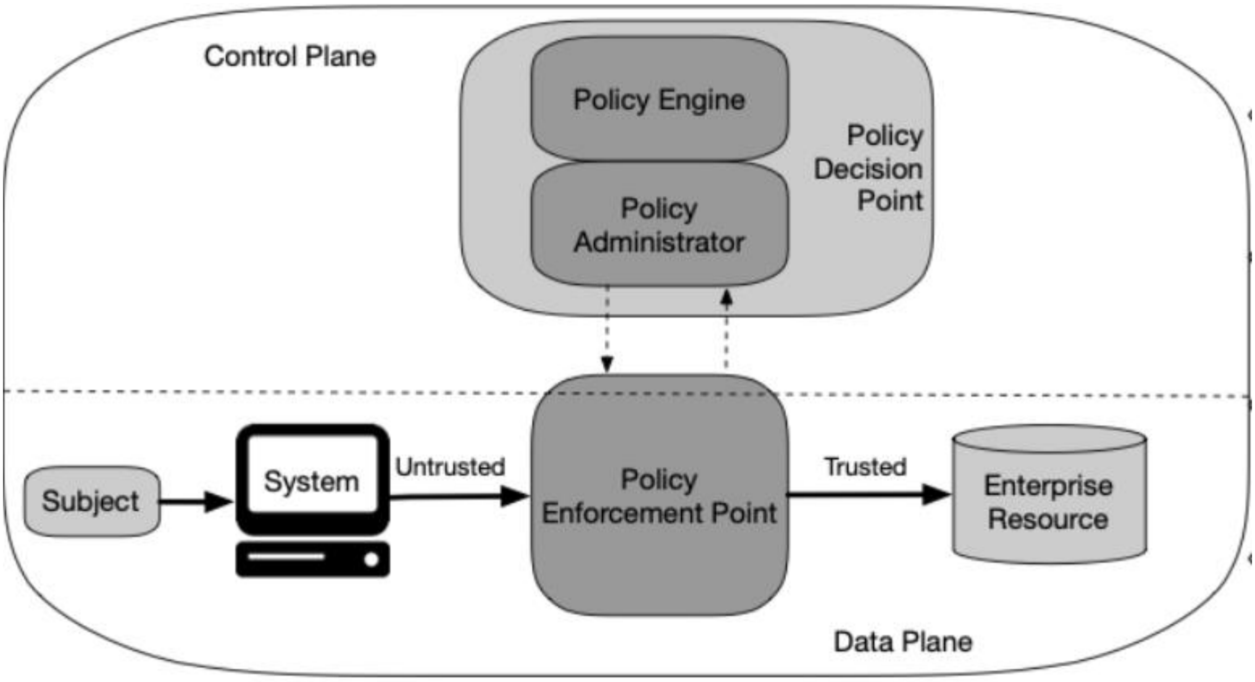
- Akamai: Enterprises Application Access (EAA): reverse proxy and Content Delivery Network (CDN) a GSLB [12].
- Cloudflare Access and Cloudflare Gateway Application firewall [13]
- Citrix: ZTNA with Citrix Secure Private Access [14]
- F5 Networks [15]
- Zscaler [16] [17]
- Fortinet: ZTNA [18]
- Cisco: Secure Access by Duo and Umbrella [19]

ZTNA implementation is still vendor specific even there are some examples of interoperability. There are vendors like Palo Alto and Akamai that relieves on the cloud capabilities to provide ZTNA features while other companies like Fortinet allows you to create a whole ZTNA infrastructure entirely on-premises.

4 Design Specification

According to the NIST, the following ones are key components that Enterprises need to manage to have a full ZTNA solution:

- PEP: policy enforcement point, it’s likely the perimetral firewall that works at data plane level and permit or deny sessions.
- Endpoint ZTNA agent: this software installed on the endpoint owned by the company is the element that make the PDP aware of the endpoint status.
- PDP: Policy Decision Point (it can be split in 2 elements: policy engine (PE) and policy administration (AP). This is a critical element that can connect to the endpoint for telemetry purpose and it’s a sort of brain of the data plane flow.
- Enterprise public key infrastructure (PKI): the infrastructure needs to have a certificate chain to authenticate devices by using private and public keys.
- Multi Factor Authentication (MFA): it is a required element to increase the security of authentication. Something you know, something you have, or you are.
- Domain Name Server (DNS) and GSLB (Global Server Load Balancing)
- Reverse Proxy: This functionality allows the Firewall (PEP) to expose a TCP service hosted internally. The firewall can both break the SSL connection in 2 parts or simply forward it to the internal resource.
- Security information and event management (SIEM): this solution can correlate suspicious events that occur in the network infrastructure to help detect threats in advance.



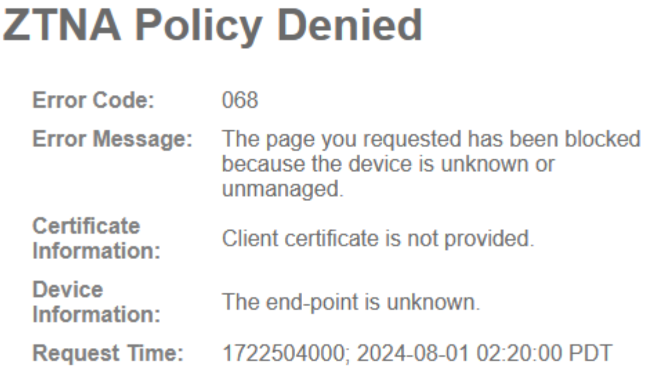
5 Implementation

Looking for the key factors of the new paradigm of the ZTNA model, I found very interesting the following statement from the NIST:

Network Requirements to Support ZTA:

8.Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first

Looking for some network solution that could accomplish this statement, it seems that the Reverse Proxy could be the answer. The Reverse Proxy is an old and proven technique to expose public services, and it seems to be a common factor of ZTNA design of several vendors both for cloud and on-premises scenarios: this solution allows the firewall to expose internal services and possibly split the communications in two different parts.
It can manage the external HTTPS connections with specific certificates in a trusted chain (PKI).
The certificate on the device (remote or local) enforces and makes stronger the authentication phase by adding a further after the checks of Username, Password and MFA.
Below an example of an exposed web page when ZTNA does not allow you. Before attempting a login with MFA or SSO, the device needs to be recognized, authenticated and authorized to access the page, thanks to the unique certificates installed by the Enterprise.

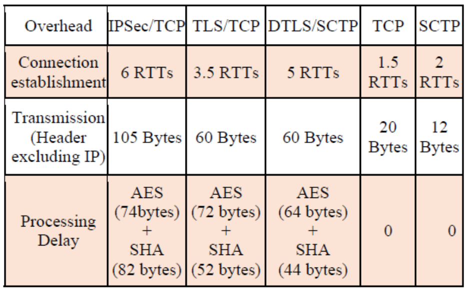


ZTNA Policy Denied

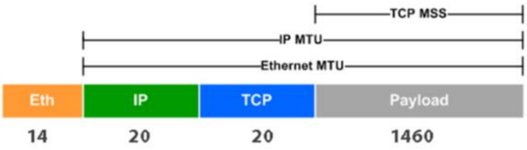
Error Code:	068
Error Message:	The page you requested has been blocked because the device is unknown or unmanaged.
Certificate Information:	Client certificate is not provided.
Device Information:	The end-point is unknown.
Request Time:	1722504000; 2024-08-01 02:20:00 PDT

6 Evaluation

If the cybersecurity professionals were waiting for a ZTNA model it is also true that the ZTNA is also a vendor marketing phenomenon that aim to migrate toward this new model.
In the end, ZTNA gathers and brings all the security precautions that make this model much more robust, but as said those new things can be implemented, at least partially, even in a legacy solution. Looking for detailed information telling why the ZTNA model should bring advantage in terms of network performance, I could not find specific reasons among research papers and vendors statements. Security vendors show clearly why the security enhancement is reached, but they claim better performance without providing specific reasons or proven metrics. It’s all about optimization. In the legacy environment, it’s quite common see HTTPS connections encapsulated in the VPN tunnel. This is expected because the old infrastructure has not been developed by considering one general design.
In order to be compliant with the security audit, SSL encrypted connections need to be enforced to all the sensitive systems.
Considering the SSL VPN, there could be about 5% of overhead for each established secured session, depending on the MTU size [20]. The table below refers to 1500 MTU, AES128 and SHA1. More secure AES256GCM and SHA384 generate a slightly higher overhead.

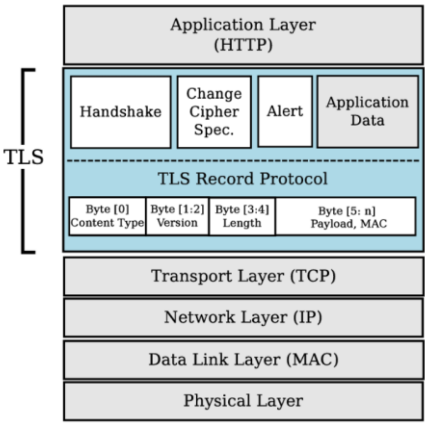


Overhead	IPSec/TCP	TLS/TCP	DTLS/SCTP	TCP	SCTP
Connection establishment	6 RTTs	3.5 RTTs	5 RTTs	1.5 RTTs	2 RTTs
Transmission (Header excluding IP)	105 Bytes	60 Bytes	60 Bytes	20 Bytes	12 Bytes
Processing Delay	AES (74bytes) + SHA (82 bytes)	AES (72 bytes) + SHA (52 bytes)	AES (64 bytes) + SHA (44 bytes)	0	0



It becomes a security overlap when HTTPS is encapsulated in an SSL/TLS VPN Tunnel that potentially could be saved by adopting the ZTNA with reverse proxy feature.

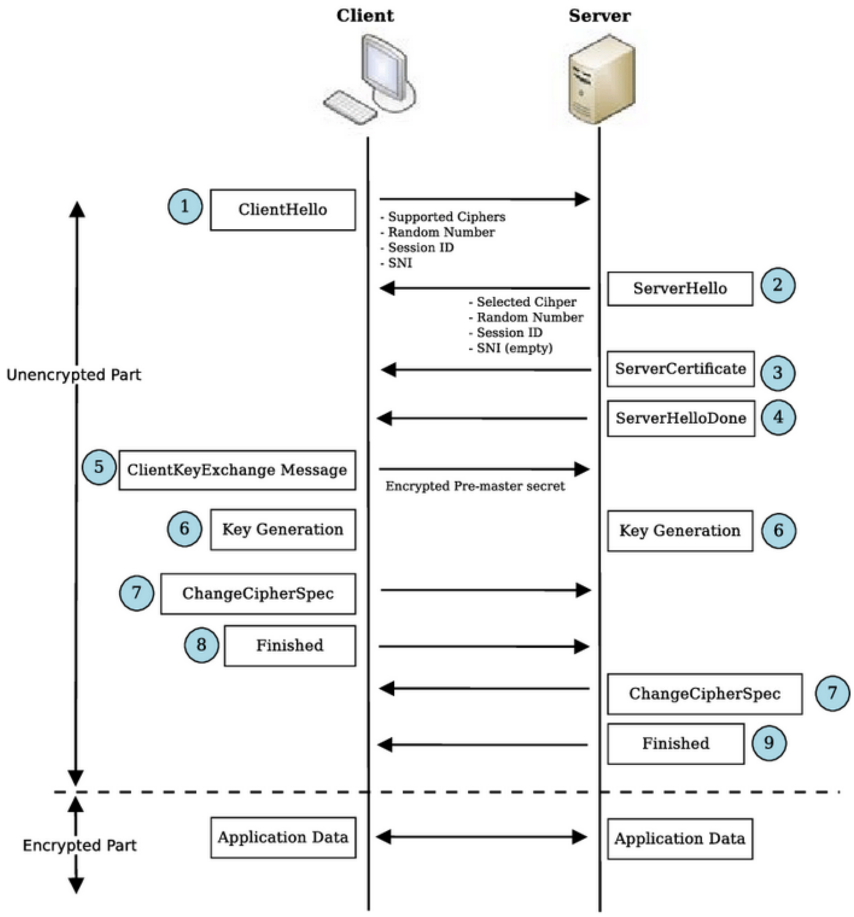
Despite a small improvement, there are big benefits in daily operations and simplification in troubleshooting because there are effectively fewer components interacting with less overlap.
Avoid the HTTPS services encapsulated in VPN Tunnel brings another advantage: the Maximum Segment Size (MSS) is preserved, and it mitigates problems with packets fragmentation [21]. These problems can be tricky to troubleshoot and provide bad performance with those protocols sensitive to latency [22] [23].



[24]

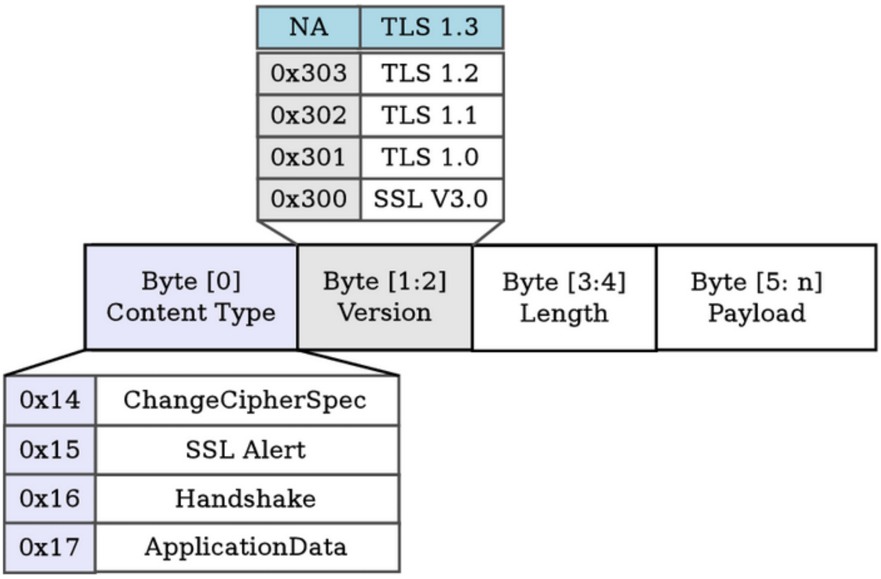
The SSL protocol includes 2 main subprotocols:

- SSL Handshake Protocol [25]: this protocol happens after the TCP Handshake (Syn – SynAck – Ack) but before a connection is encrypted between a Client and a Server starting from the “ClientHello” message. In this phase the security algorithms and connection configuration are negotiated between the client and the server such as: protocol version, cipher suite, certificates checks, symmetric key generation.



[26]

- SSL Record Protocol: is used to secure unsecure protocol like HTTTP -> HTTPS, FTP->FTPS and it also create secure tunnels in the SSL VPN. It manages the: Data encapsulation, Compression, Encryption, Integrity, Sequence.

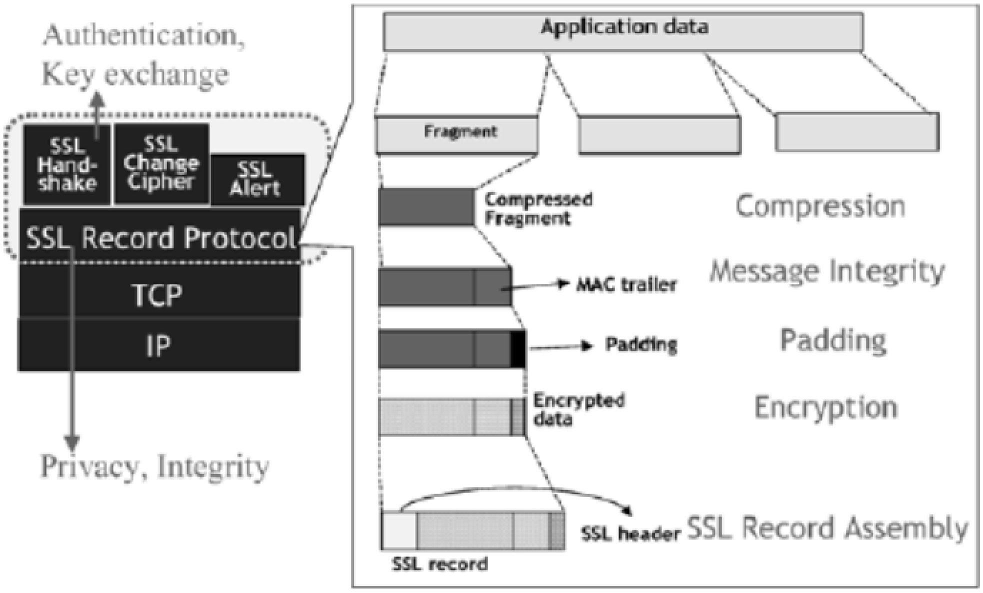


NA	TLS 1.3
0x303	TLS 1.2
0x302	TLS 1.1
0x301	TLS 1.0
0x300	SSL V3.0

Byte [0] Content Type	Byte [1:2] Version	Byte [3:4] Length	Byte [5: n] Payload

0x14	ChangeCipherSpec
0x15	SSL Alert
0x16	Handshake
0x17	ApplicationData

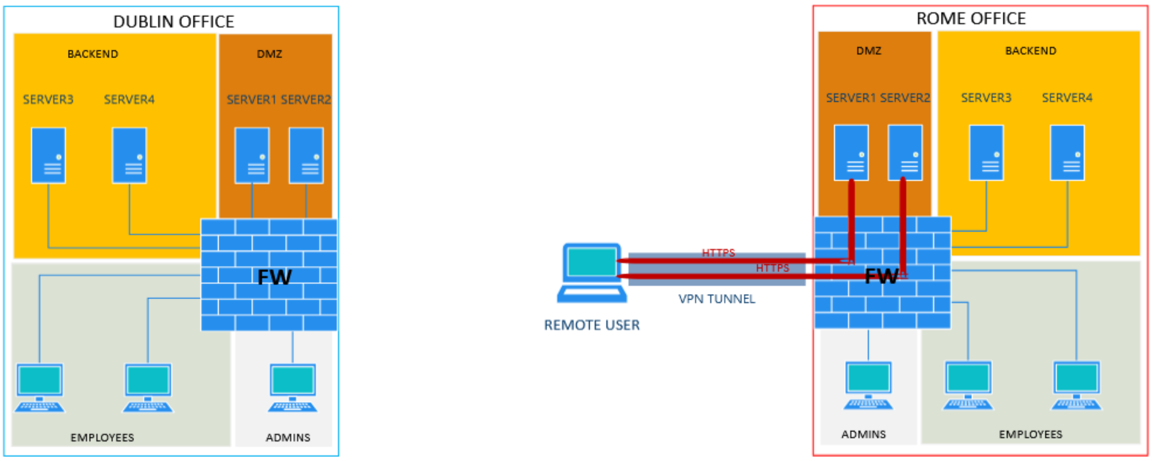
[27]



[28]

6.1 Case Study 1 – Legacy VPN

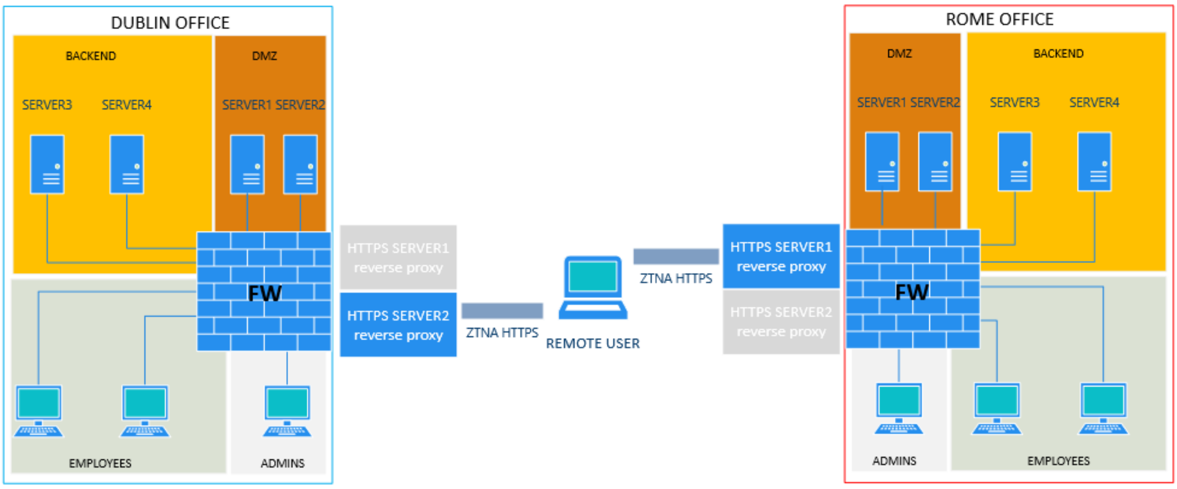
Let’s consider a classical enterprise topology where some remote users need to access sensitive company resources that are stored on premise and are managed by internal webservers. Those resources must be available and secured.
This design could be partially hosted in a public cloud infrastructure, the logic remains the same.



A company having two or more physical offices need to provide several services for the day-by-day operations via HTTPS.
To make these sites work from office and remotely, in a legacy environment, you need a Remote Access VPN service available on the frontend firewall, or on a VPN concentrator just behind the perimetral firewall.
You can provide some kind of redundancy by creating a local cluster (2 devices acting as a single logic unit) or it’s possible to implement something more structured like a geographical redundancy infrastructure. In this case you can have two VPN servers on both sides working with two different public IP addresses. For instance, Dublin could have 1.1.1.1 while Rome 2.2.2.1.
A common configuration allows to take advantage of both VPN servers by using the same domain to resolve both public IP addresses. Even if you connect by using a URL that can resolve different IP like “vpn.myoffice.com” (1.1.1.1 Dublin or 2.2.2.1 Rome) you are stuck to that specific VPN server. If some services of that office are not available, you cannot simply establish a further tunnel since just one tunnel per time is allowed [29].
After the VPN is established, a further tunnel encapsulated into the SSLVPN tunnel will let you connect to the internal servers. The servers should be in DMZ if accessible from untrusted networks, but it could be behind a backend firewall as well. Because security audit, the admin and user access must be secured. It means that only HTTPS is allowed.
As already said, this overhead, the tunnel SSL encapsulated into another tunnel SSL, is something you don’t want [30]. A robust set of algorithms is enough to protect your connection. These two tunnels create a 5% of overhead depending on the algorithms. Furthermore, it’s important to consider that this kind of encapsulation lower the connectivity performance due to the lower MSS size.

6.2 Case Study 2 – Reverse Proxy

Since securing a connection with SSL/TLS protocol with robust algorithms is enough to guarantee authentication, confidentiality and integrity for several years let’s have a look at the simpler Reverse Proxy solution.



Let’s assume that these resources are hosted on the servers and directly exposed on internet via the reverse proxy technique. Internally, they are reachable directly by using their private IP address.
Likely, Rome and Dublin are connected via IPSEC tunnel and/or a MPLS link to replicate and sync the servers hosting the services.

Below a map of the internal and external IP addresses:

Site	Dublin Office		Rome Office	
Service	HTTPS SERVICE 1	HTTPS SERVICE 2	HTTPS SERVICE 1	HTTPS SERVICE 2
Corporate IP address	192.168.10.1	192.168.10.2	192.168.20.1	192.168.20.2
Public IP address	1.1.1.1	1.1.1.2	2.2.2.1	2.2.2.2
URLs	Service1.myoffice.com	Service2.myoffice.com	Service1.myoffice.com	Service2.myoffice.com

Dublin Office:

HTTPS SERVICE 1:

- From internal network:

it can be reached via 192.168.10.1 or by using internal DNS resolving *service1.myoffice.com*

- From public network:

it can be reached via 1.1.1.1 or by resolving via public DNS this URL: *service1.myoffice.com*

HTTPS SERVICE 2:

- From internal network:

it can be reached via 192.168.10.2 or by using internal DNS resolving *service2.myoffice.com*

- From public network:

it can be reached via 1.1.1.2 or by resolving via public DNS this URL: *service2.myoffice.com*

Rome Office:

HTTPS SERVICE 1:

- From internal network:

it can be reached via 192.168.20.1 or by using internal DNS resolving *service1.myoffice.com*

- From public network:

it can be reached via 1.1.1.1 or by resolving via public DNS this URL: *service1.myoffice.com*

HTTPS SERVICE 2

- From internal network:

it can be reached via 192.168.20.2 or by using internal DNS resolving *service2.myoffice.com*

- From public network:

it can be reached via 1.1.1.2 or by resolving via public DNS this URL: *service2.myoffice.com*

When an employee is physically connected in Dublin office, his local DNS server will resolve the two public URLs by returning the private IP hosted in Dublin. Same story for Rome employees, the only difference will be the different private IP resolved.

From public network, the same URLs will be resolving the public IP because the split-horizons DNS.

There could be some DNS load balancing logic to resolve one URL with the Dublin or Rome office IP or prefer one over the other one depending on several conditions, including some kind of persistence features. Global Server Load Balancing (GSLB)[31][32] features can help to monitor the service with specific HTTPS probe that query the hosted service in order to be aware of their health status. There could be the case that *server1.myoffice.com* resolves Dublin public IP (1.1.1.1) while *server2.myoffice.com* resolves the Rome public IP (2.2.2.2). This way there is a transparent load balancing among the Rome and Dublin offices. This balancing improves the overall services availability and optimizes the network utilization of both offices. It’s crucial to have it when performing maintenance activities on one site because it can easily move the active services on the other site without having any impact on the production.

To make those services securely accessible from internet, employees need to have an endpoint agent managing device certificates (PKI public/private) installed on their corporate computers. That is required for the authentication and authorization and further security checks like User, Password and OTP can be implemented to provide a full MFA.

From outside, an employee connecting to one URL is just making a HTTPS connections that would not been allowed to external user or untrusted devices because the ZTNA check (based on the device certificate).

7 Conclusion and Future Work

Using a VPN tunnel is certainly still a valid solution but there are limitations that should be raised clearly.
Comparing the two solutions, the followings advantages can be noted:

Remote Access VPN advantages:

- Proven and reliable solution
- Admin access is easier (full network access)
- Easier implementation (compared to the full ZTNA with EndPoint Agent and PDP)

ZTNA Reverse Proxy advantages:

- By design just one port/service is allowed. No need to check further constraints.
- HTTPS overlap is avoided, 5% of exchanged data saved for each single secured session.
- MSS is maximized, better latency performance and less packets exchanged.
- Fragmentation problem mitigated
- Tunnels can have different level of security and different algorithms depending on the criticality of the exposed service.
- There are not tunnels hanging when services are not used. HTTPS Tunnels are quickly down when not used saving bandwidth and resources.
- Modular system, further destination can be added or removed without impacting the split-tunnel. These actions can be done in a transparent way for the remote users.
- Greater flexibility in implementations. By using GLSB services it’s possible to expose the same services in another site (cloud included) in a transparent way. This improves the performance and the service resiliency.
- Distributed system. There is not a unique point of failure but many exposed services.
- No network routed into the tunnel, no information about internal network addresses and no risk of any overlap with other internal network if the use is working from another office.
- ZTNA principles are applied to on-premises users too

The new network paradigm, that is applicable thanks to the ZTNA model, can enhance all the security triad principles: confidentiality, integrity and availability. The ZTNA features can improve confidentiality and integrity, thanks to their enforced checks and continuous monitoring even in a legacy VPN environment. But it turns out that a real native ZTNA model, with the reverse proxy solution, can optimize the resources and provide an enhanced overall availability of the critical services.

The optimization of the tunnels turns into a higher availability of services during high level traffic period. The ability to redirect a service hosted on one site to another site, transparently for remote users, provides a wider variety of possible actions by making the network structure more flexible and helping technicians in its management and maintenance.

VPN and ZTNA should not be considered as alternatives to each other, but they can coexist together.

Most critical and used services should be under ZTNA, while the company can keep on migrating the other services from the legacy solution to the new model. Furthermore, it must be considered that ZTNA provides services through HTTPS only: there are a number of protocols that are not supported to be incapsulated in HTTPS so the legacy VPN solution will be still required for those.

Looking for ZTNA benefits and advantages respect to the legacy VPN solution, I discovered that likely all the specifics characteristics could be added to the legacy VPN. Vendors like Fortinet encourage a hybrid model where a remote access VPN can be enhanced by adding all the elements that characterize the zero-trust model that have been mentioned in this paper.

In my Lab, I could not implement a real zero-trust model that is something really complicated that only a security Vendor can provide; I was focused on a specific NIST statement that advice to expose services on the physical network perimeter. It looks like several vendor applied this principle by taking advantage of the reverse proxy implementation and this is what I tried to test, comparing it to the legacy tunnel solution. Honestly, I didn't really like the reverse proxy functionality at first, because it opens the ports of the external firewall and allows anyone to open sockets at least at the network level. Then I realized that it simplifies the flow and provides better service availability because it reduces encryption overhead, optimizing network bandwidth, and helps to have a more flexible and modular infrastructure.

In my LAB I blocked listening ports on my public IP address by implementing inbound rules that could filter the reverse proxy by checking the source IP address based on a dynamic DNS resolution.

It would be interesting measure the overall performance on a large-scale network, where hundreds of employees connect remotely, to see what the real benefits are in an enterprise scenario. It would be interesting comparing ZTNA with another secure approach: the Software Defined Perimeter (SDP).

References

[1] Editor, C.C.*Virtual Private Network (VPN) - glossary: CSRC, CSRC Content Editor*. Available at: https://csrc.nist.gov/glossary/term/virtual_private_network

[2] *Tcp.pptx* (2023) *SlideShare*.
Available at: https://www.slideshare.net/slideshow/tcppptx-259464522/259464522

[3] *OpenVPN and the SSL VPN Revolution - Giac Certifications*.
Available at: https://www.giac.org/paper/gsec/3985/openvpn-ssl-vpn-revolution/106391

[4] *SSL VPN vs. IPSec: What are the differences? Palo Alto Networks*.
Available at: https://www.paloaltonetworks.com/cyberpedia/ipsec-vs-ssl-vpn

[5] E.B. Fernandez, A. Brazhuk *A critical analysis of zero trust architecture (ZTA).*
Available at:

https://www.researchgate.net/publication/363306732_A_Critical_Analysis_of_Zero_Trust_Architecture_Zta

[6] S.R.Pokhrel, G.Li, R.Doss, S.Nepal *Towards decentralized operationalization of Zero Trust architecture*.
Available at:
https://www.techrxiv.org/articles/preprint/Towards_Decentralized_Operationalization_of_Zero_Trust_Architecture/19127090

[7] *What is Zero trust? | google cloud. Google*.
Available at: https://cloud.google.com/learn/what-is-zero-trust

[8] *Zero trust model - modern security architecture: Microsoft security. Zero Trust Model - Modern Security Architecture | Microsoft Security*.
Available at: https://www.microsoft.com/en-us/security/business/zero-trust

[9] Newton, P. (2023) *ZTNA over VPN can be a good place to start your zero trust journey, Fortinet Blog*.
Available at: https://www.fortinet.com/blog/industry-trends/ztna-over-vpn-to-start-zero-trust-journey

[10] *Ztna over VPN Tunnels*.
Available at: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-ztna-vpn-tunnels.pdf

[11] Rose, S. *et al.* (2020) *Zero trust architecture, CSRC*.
Available at: https://csrc.nist.gov/pubs/sp/800/207/final

[12] *Moving beyond perimeter security*.
Available at: https://www.akamai.com/site/en/documents/white-paper/akamai-moving-beyond-perimeter-security.pdf

[13] Tuber, D. *et al.* (2024) *Cloudflare access is the fastest zero trust proxy, The Cloudflare Blog*.
Available at: https://blog.cloudflare.com/network-performance-update-security-week-2023

[14] *Why ZTNA is superior to vpns - Citrix.com*.
Available at: https://www.citrix.com/platform/citrix-secure-private-access/

[15] *Zero trust in an application-centric world. F5, Inc.*
Available at: https://www.f5.com/resources/solution-guides/zero-trust-in-an-application-centric-world

[16] *What is Zero trust network access? Zscaler*.
Available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-access

[17] *What is a reverse proxy? Core Concepts and Definition*.
Available at: https://www.zscaler.com/resources/security-terms-glossary/what-is-reverse-proxy

[18] *Architecture Guide - Zero Trust Network Access. Fortinet.*
Available at: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/09f71ecd-6817-11ec-bdf2-fa163e15d75b/Zero_Trust_Network_Access-7.0-Architecture_Guide.pdf

[19] *Solutions - cisco secure access service edge (SASE) and Security Service Edge (SSE) architecture guide* (2024) *Cisco*.
Available at: https://www.cisco.com/c/en/us/solutions/collateral/enterprise/design-zone-security/sase-sse-ag.html

[20] *Hussein, A. et al. Securing diameter: Comparing TLS, DTLS, and IPSec: IEEE Conference Available at: https://ieeexplore.ieee.org/document/7777417*

[21] *RFC 791: Internet protocol IETF Datatracker*.
Available at: https://datatracker.ietf.org/doc/html/rfc791

[22] *IP fragmentation in detail*, *Packet Pushers*.
Available at: https://packetpushers.net/blog/ip-fragmentation-in-detail/

[23] GeeksforGeeks (2022) *How mtu and MSS affect networks?*, *GeeksforGeeks*.
Available at: https://www.geeksforgeeks.org/how-mtu-and-mss-affect-networks/

[24] *The TLS layers and sub-protocols | download scientific diagram*.
Available at: https://www.researchgate.net/figure/The-TLS-layers-and-sub-protocols_fig4_321347130

[25] *How an SSL connection is established*. *IBM*.
Available at: https://www.ibm.com/docs/en/cics-tg-zos/9.3.0?topic=ssl-how-connection-is-established

[26] *The TLS handshake protocol messages sequence*.
Available at: https://www.researchgate.net/figure/The-TLS-handshake-protocol-messages-sequence_fig5_321347130

[27] *TLS record format | scientific diagram*.
Available at: https://www.researchgate.net/figure/TLS-record-format_fig7_321347130

[28] *SSL record protocol working principle | scientific diagram*.
Available at: https://www.researchgate.net/figure/SSL-protocol-with-an-expanded-view-of-the-SSL-record-protocol_fig2_224230457

[29] Kirvan, P. (2021) *How to use two VPN connections at the same time*, *Networking*. Available at: https://www.techtarget.com/searchnetworking/answer/Can-you-have-two-VPN-connections-to-the-same-machine-simultaneously

[30] Roy, W. by: S. (2023) *SSL overhead: What it is and how to reduce it?*, *Baeldung on Computer Science*.
Available at: https://www.baeldung.com/cs/ssl-overhead-causes-countermeasures

[31] *Global server load balancing. F5 Networks.*
Available at: https://techdocs.f5.com/en-us/bigip-15-0-0/big-ip-dns-load-balancing/global-server-load-balancing.html

[32] Barney, D. (2024) *Global server load balancing - why it is necessary*, *Kemp*.
Available at: https://kemptechnologies.com/blog/global-server-load-balancing-why-it-is-necessary