5thmountain

The Case for “Blameless” TLS/SSL Inspection In A Regulated Environment

Introduction

A lot more attention is being paid to cybersecurity because of the various breaches that have happened over the last few years. There's much more boardroom pressure to make sure all angles are covered.

No one wants to be the C-level executive that's speaking to the press about what happened. Executives want to know: “Are we spending the right kind of money on security? Is it integrated into everything we're doing? Are we covered?”

These are very simple questions, but they point to a number of factors that force you to integrate privacy and security into what you're doing rather than try to tack it on as an afterthought.

The authors believe that this document should be of interest to:

- CEOs
- CIOs
- CISOs
- CFOs
- IT Security Department
- IT Networking Department
- IT Architecture Department
- Risk Management/Audit Department
- Any other associated disciplines
- In particular the corporate representatives for the furtherance of POPIA.

The Encryption Issue

It is common cause now, that data traversing the Public internet (and private networks as a follow on), is becoming ever encrypted. The reasons for this are driven by security concerns as transactions are more and more Cloud based.

The transactions include E-commerce, online trading, investments and any and every detail of an individuals identity. Indeed an individual is constantly amazed at the level of information leak as to our own interests as detected by where and what we do on the Web.

The proliferation of mobile devices is feeding this behaviour with more and more transactions happening in the palm of your hand.

The fact that most business interaction is now encapsulated via web browsers (as opposed to a stand alone dedicated applications) has led to ongoing browser development, and competition to be the most acclaimed and chosen browser is keen.

85 +% OF TRAFFIC NOT SEEN

The differentiator of the highest levels of security, balanced against user friendliness, speed and attractiveness of the browser, is accelerating feature sets that include built in anonymity.

The fact is that global politics and events pull on freedom of speech policies, and these policies are divided and often juxtaposed by sovereign country, in terms of control and censorship, are drivers of this anonymity.

The seamless automation and background behaviour of negotiating a “secure, trusted and safe” session is at the forefront of this browser competition.

This need for privacy has been showcased in the recent USA elections and it is not just limited to web browsing but e-mail leaks as well. Cyber-threats are increasing steadily (see the recent debacles below).

Transnet Cyber Attack

SA Space Agency hit by Data Breach

Department of Justice hit with Ransomware Attack

Hackers breach South Africa’s courts — systems crippled and people's banking details compromised

This technical ability to wrap a user in an iron clad armour of protection stands at odds with a government's need for access to information, such as that defined in the South African PROMOTION OF ACCESS TO INFORMATION ACT 2 OF 2000, while simultaneously also supporting the PROTECTION OF PERSONAL INFORMATION ACT.

The sovereignty of transactions is a major point of concern and interest.

The need for businesses to comply, and at least to pay more than "Lip Service" to these pieces of legislation, is actually in the best interest of the businesses as evidenced by actual damage caused by Cyber-Crime.

The Content Control Issue

The idea that controlling where users can tread in regard to internet sites for the purpose of protecting the business from cyber-threats and general malware, including unsavoury content and bandwidth being used for personal non-work related activities (cyber-slacking), has resonance with the vast majority of businesses and even a percentage of parents (parental-control).

Traditional methods of controlling internet usage turns largely on the rating of web sites (threats and content) and databases of these destinations are made available as free and commercial offerings of various degrees of effectiveness, depending on the source of this data and often linked to subscription or licensing costs.

The Centralised Control Issue

Databases are used to create whitelists/blacklists that are often associated with web proxy servers (that force the users to access the internet via a central corporate controlled proxy) as opposed to an end to end and per site basis.

This "back-hauling" of data, for this centralised control, is both extremely inefficient and actually is less secure (through anonymity) than applying content controls as close to the users as possible.

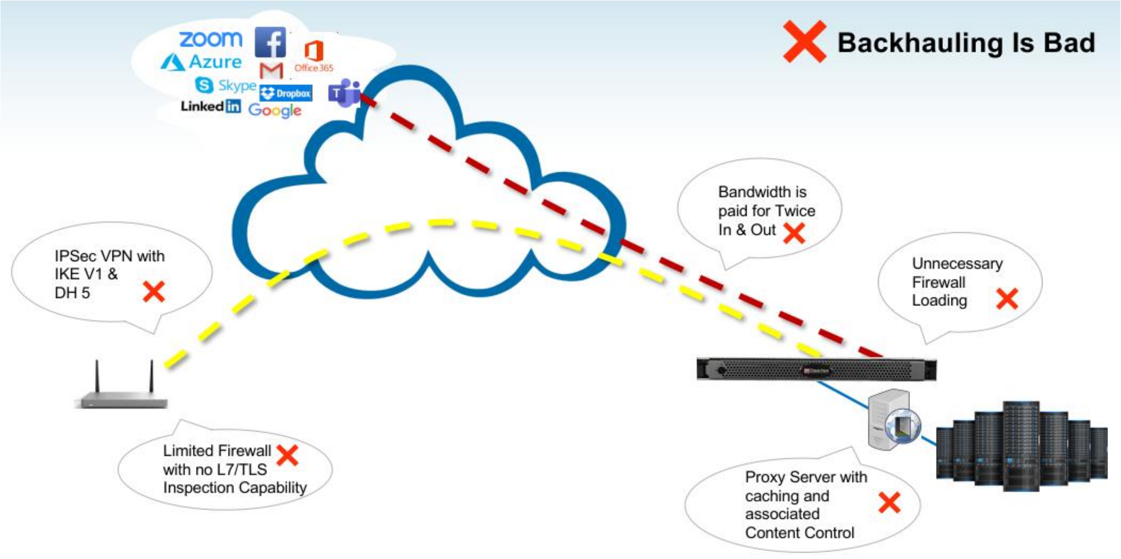
The surface area of internet Access Proxy Servers is relatively large and an easy target for cyber-attacks. The fact that the bandwidth used by the proxy is quite "fat" compared to the "narrow" non-proxy (split tunnel) access clients, makes it an ideal target for Denial Of Service Attacks (DDOS). Even if the corporate firewall/s are successful at blocking such threats, there is a resource (performance) hit to the firewalls.

"In the pre-cloud Dark Ages of just a few years ago, the standard model for supporting branch offices was to use a wide-area network, typically MPLS from a telecom carrier, to carry all traffic to and from a data center, where security was managed centrally.

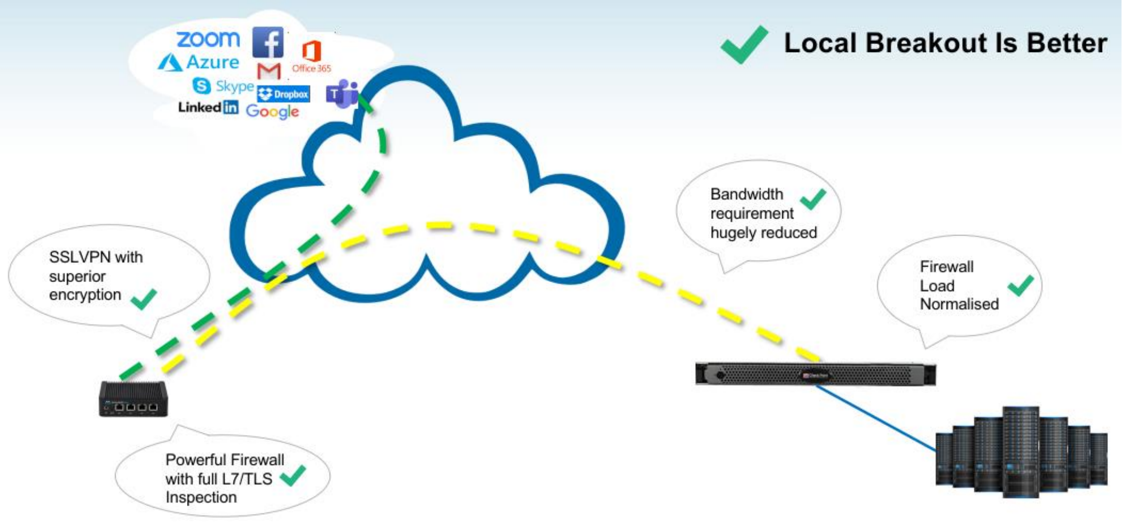
This was essentially "the worst of all worlds", according to Naveen Zutshi, Chief Information Officer at Palo Alto Networks. "In the branch offices, you had a lot of hardware to manage and maintain and, because you were back-hauling everything to the data center, you often had performance and latency issues. Plus, the bandwidth was expensive.

Even if that model were efficient and inexpensive - which it isn’t - it would no longer be feasible in the cloud era, when branch offices and remote users are increasingly bypassing centralised IT and going directly to the cloud.”

SD-WAN Implementation with a legacy MPLS like Backhaul Topology


✗ Backhauling Is Bad
zoom
Azure
Skype
LinkedIn
Office 365
Dropbox
Google
Bandwidth is paid for Twice In & Out ✗
Unnecessary Firewall Loading ✗
IPSec VPN with IKE V1 & DH 5 ✗
Limited Firewall ✗ with no L7/TLS Inspection Capability
Proxy Server with caching and associated Content Control ✗

SD-WAN Implementation with Cloud Centricity and Distributed Local Control


✓ Local Breakout Is Better
zoom
Azure
Skype
LinkedIn
Office 365
Dropbox
Google
Bandwidth requirement hugely reduced ✓
Firewall Load Normalised ✓
SSLVPN with superior encryption ✓
Powerful Firewall with full L7/TLS ✓ Inspection

Other methods of internet access control include Domain Name Server Blocking (DNS blocking) - Firewalls are configured to send DNS requests to service providers such as WebTitan, OpenDNS (Cisco Umbrella), SafeDNS and many others. Access to the intended site/s is tested during the IP address resolution against (again similar if not the very same white-list/black-list mentioned above) databases.

Both techniques of blocking, whether used in isolation or in combination, are becoming less and less effective due to the ever increasing encryption of data in transit, including DNS lookups over HTTPS (the systems simply have no visibility of the sessions) and as a result more and more false positives or entire misses are occurring.

Recent statistics show that the DNS blockers, as an example, have dropped to an effectiveness of around 10% whereas 5 years ago the % was circa 80%.

The poor performance of these systems leads to frustration for the users and network administrators alike as everyday activities are being blocked. The cost of system solutions currently in place is simply a waste of money, and the effectiveness of human resources needed to administer the users' report incidents, ongoing is concerning.

The fact that DNS lookups are ever increasingly occurring over HTTPS (invisible) is rendering these systems increasingly ineffective.

The inability of systems to have visibility of more than around 15% of what is going on, and who is talking to whom, makes the control of bandwidth usage a complete hit and miss affair.

The fact that software updating is exponentially growing, as more and more APPS are needed for cloud based activities, is leading to an upward spiral for more bandwidth per user. The increasing reliance on virtual meeting sessions (Zoom/Teams etc.) is driving this need for faster and faster clock speeds.

Of course the first response by business to avoid this spend, is often causing a “witch-hunt” to find and censure the bandwidth abusers.

The Falsely Accused User Issue

Users are often identified as internet facility abusers by the network and security teams, while the user is completely unaware that his device of choice is doing activities in the background.

Some of these activities include;

- Synchronisation of devices (laptop to phone etc.)
- Backups to cloud drive space (Google Drive, One Drive etc.)
- Software updates such as Apple devices to iTunes, Android OS and APP updates.

The Special Case Of Microsoft Updates Issue

As per the author's measurements, Windows updates, as a bandwidth and session %, are by far the largest, followed by Apple Devices and Android.

The issue regarding Microsoft's updating strategy, is not so much in the update coming down off the internet towards the user device, but a default setting that causes the users' devices to leverage Microsoft's version of bittorrent technology (publicly unnamed by MS) to "seed" chunks of update cached data towards any number of other Windows users (leechers) anywhere in the world, who have no connection or relationship whatsoever with the unaware user.

It is possible to override the Windows updates default settings to prevent this behaviour but it requires an advanced, per device configuration or a push of a "Group Policy Script" to set the devices. This is often not possible, because users may be the actual owners of the devices (BYOD) and do not fall within such corporate policy controls.

The frustration in communicating this issue is compounded by an attitude of ("we have got this covered"), and dismissed, by IT and network personnel.

The "We have got this covered" Issue

The truth is that this is not covered at all. The support teams continue to view updates in a down from the cloud towards user (inbound simplex) and not an outbound session (duplex) activity, that Microsoft average's users bandwidth (MS's explanation is that by leveraging an updating community it is for the benefit of all of the update community). In fact Microsoft would have to lay on huge amounts of bandwidth, and servers to serve all the Windows machines out there in the world.

The network team will tell you that using local update Windows Server Update Services (WSUS) obviates this issue. In fact running WSUS servers (if not on the actual user's Local Area Network simply moves the bottleneck upstream) and does not solve the uplink issue at all as the "seeding" of the Rest Of World issue is completely disconnected from the user's own updating downloading process.

So as long as a Windows machine is connected to the internet, and the default update settings are in use, these machines will continue to participate in the updating community for all the Rest Of World users.

With the update sessions being encrypted, the standard content control systems simply know nothing of these connections, and application aware controls do not block these update sessions as they are not identified as applications such as uTorrent etc.

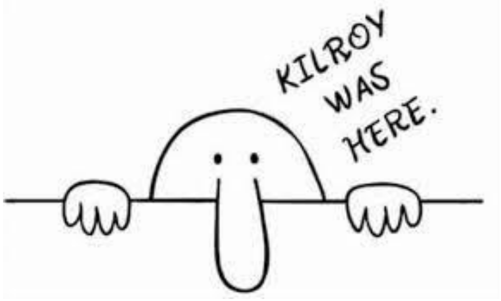
The systems, that are able to loosely identify these sessions as “bittorrent” and not as Windows updates, simply cause the unfortunate users to be blamed for “bittorrent” as if it is illegal (bittorrent as a protocol is not in itself illegal). These update sessions are not bittorrents as in downloading from ”The Pirate Bay” etc. and the unfortunate users (and their co-workers) are either data-capped or restricted in actual available speed by association. Now by far the users are simply trying to do their work.

It is the authors’ experience that these Windows updates are mostly wrongly identified (even as PlayStation sessions) as the update peers are free to negotiate any convenient IP ports to communicate through.

Out of frustration, the exasperated users simply bypass the corporate network (to get on with their work) and connect to the internet via tethering of “hotspots” or other routers. The bypass of the company network causes serious security vulnerability and can cause the corporate firewalls to shut down sessions due to the re-entrant “man-in-the middle” that the user has created (unwittingly).

The “Top Talkers” Issue

Reliance on “top talker” statistics, while not having visibility of the majority of the usage detail (encrypted data), is a very poor position to rely on for decision making.



Let’s take an example of a top 10 report. It is default assumed that the “top talker” must be an “abuser” of the resources, when in fact he may well be a “top producer” and his traffic count is representative of the fact that he has a large network of connections for his business.

In fact, if one were to lump the miscellaneous or unclassified data, as a single user (let’s call him Kilroy) that top talker would by far exceed the usage of the total number of the identified top talkers.

The issue here is that the current systems are reporting top talkers within a 10% visibility limitation and the 90% “Kilroy Was Here” is simply ignored and categorised as ‘miscellaneous’ or generic TCP data.

The “Throwing Bandwidth At It” Issue

The authors, when investigating the perception of not sufficient bandwidth, discovered a direct causal link to uninspected or encrypted data and due to the inability to filter the data adequately defaults to a “more bandwidth needed” reaction.

The problem with this method, is that by simply upgrading bandwidth, serves a wider and wider audience and will consume updates and uploads on an ever-increasing host count on a % of nominal bandwidth basis.

This bandwidth escalation suites the ISPs perfectly, as this is how they are able to invoice more and more from their captive clients. ISPs will never interrogate a client as to why he believes he needs more bandwidth, and will be more than happy to “upgrade” you. To this extent the ISPs often engage in offering “more bandwidth at current cost” (specials) at the price of resetting (extending) the clients contract dates to avoid network churn.

The South African Issue with Bandwidth

Most South African service providers have not created their services (bandwidth oversubscription syndication) to accommodate this upload behaviour and the constant low level of uploading update data damages the ISP’s sharing of bandwidth model (both commercially and as a technical service). Throttling of bandwidth penalties may be triggered and the whole user experience slows down. The knee-jerk reaction is to “throw bandwidth” at the problem.

Enter SSL/TLS Inspection and the Question Of The Legality of Payload Decryption

“Since more than 80% of traffic is encrypted these days, according to Security Boulevard, a performance hit like that forces organisations to choose between experience – meeting the throughput needs of end-users and the business — and security.

It’s estimated that around 70% of attacks use encryption to evade detection, which is alarming when you consider that SSL inspection can’t be enabled for all traffic. Certain regulations prioritise user privacy over security, which has led to only one option for security practitioners: accept this as a business risk.”...

The authors contend that the risk mentioned above should not just be accepted as alternate methods to mitigate the risk do exist - **See the conclusion at the end of the document.**

The IDS/IPS Defeated Issue

Intrusion Detection Systems (IDS for short) does analyse network traffic. But as more and more network traffic is becoming encrypted, the IDS solution encounters more and more difficulties in demonstrating any value.

Security = Privacy / Privacy = Security

The balance between the protection of privacy, and high security protection, varies from country to country based on geopolitical sensitivities and human rights sensitivities.

Congress Needs To Start Caring About Our Privacy As Much As China Does

The Reasonable Expectation Of End-To-End Communication Sessions - The Geopolitical Influence

USA

The USA is obsessed with data being seen in the light of a battlefield resource and currently places security before privacy as a priority.

“Data security is a critical first step before privacy or consumer protection priorities are legislatively or practically possible. Security of the collection, storage and movement of consumer data logically underpins the development of meaningful privacy rights over consumer data. Making data secure is the prerequisite to vesting privacy rights, if for no other reason than to ensure an individual’s right to omit, correct or review any such data. Privacy is almost impossible without a market-wide reasonable expectation of who has rightful access to specific data.”

The authors’ view is that systems and products produced in the USA (big brand names), including Gartner positioning, prioritise the aspect of data security over privacy and use techniques that may offend the regulations of another sovereign country. The comparison with Europe and South Africa, and indeed even China now, is that data is seen as an extremely important currency that encourages end-to-end business-to-business dealings. The emphasis should be on end-to-end communications with a high degree of protection against manipulation of the actual data.

Europe

GDPR stresses the importance of encryption, but does not include decryption in its recommendations, because the data sessions are intended to be encrypted end-to-end and this excludes eavesdropping by default as it is incongruous with the concept of privacy. USA security product vendors are largely playing to the emphasis on security at all costs.

South Africa

POPIA is, inter-alia, the South African implementation of the principles ensconced in GDPR and as such it is the authors’ view that the institutionalisation of the big brand products (The, **“We’ve got this covered, because we are an “XYZ... shop”**, narrative) by corporate South Africa will actually undermine the privacy goals of POPIA.

South Africa has three cornerstone legislations acting in a high degree of balance i.e.

- POPIA (Act No. 4 of 2013: Protection of Personal Information Act, 2013)
- PAIA (Act No. 2, 2000 Promotion Of Access to Information Act, 2000)
- Cyber Crimes Act (Act No. 19 of 2020: Cyber Crimes Act, 2020)

All three legislative legs fall within the jurisdiction of the Department of Justice and Law Enforcement.

The concept of “Access to Information” encompasses the concept of “lawful intercept” which is only administered by law enforcement agents mandated through the courts.

It is the authors’ concern that corporate deployment of tools or devices, including software that facilitate such intercept, could constitute potential unlawfulness or at minimum could embroil the corporate organisation if a data breach should occur.

The penalties can be severe and could also include civil damages claims over and above the criminal aspect (South African Law of Delict).

The POPIA is founded on the Bill of Rights and Chapter Two of the Constitution of South Africa contains the Bill of Rights, a human rights charter that protects the civil, political and socio-economic rights of all people in South Africa. The rights in the Bill apply to all law, including the common law, and bind all branches of the government, including the national executive, Parliament, the judiciary, provincial governments and municipal councils. Some provisions, such as those prohibiting unfair discrimination, also apply to the actions of private persons.

The seriousness of the impact of POPIA is reflected in the recent determination by our Apex Court on 4 February 2021:

LRC welcomes Constitutional Court ruling in RICA case

LRC welcomes Constitutional Court ruling in RICA case

Johannesburg — The Legal Resources Centre welcomes the Constitutional Court ruling this morning that specific provisions of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) are invalid.

“This judgment reaffirms the importance of the constitutional right to privacy and the need to protect everyone’s right not to have the privacy of their communications infringed. It further protects everyone from security agencies and abuses of power. It is also a step in the right direction in strengthening our democracy.”

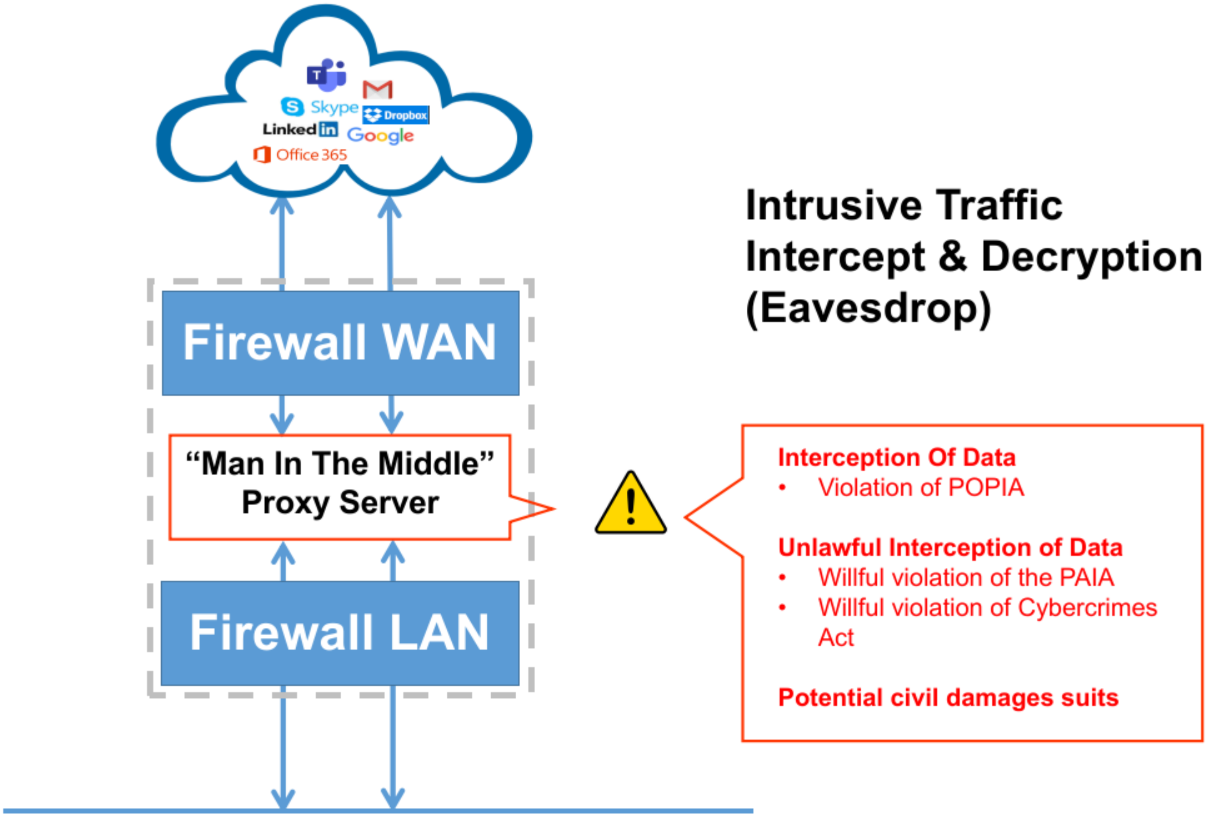
The authors urge that businesses take the responsibility of being a “Responsible Corporate Citizen” to heart with regard to the matter of privacy.

Amazon GDPR fine signals expansion of regulatory focus

Corporate citizenship: Your company's role in society

Governments continue to eye data privacy, forcing CIOs to adapt

Legal Implications Of Payload Decryption by Man-In-The-Middle Interception Of Data



Intrusive Traffic Intercept & Decryption (Eavesdrop)

Interception Of Data

- Violation of POPIA

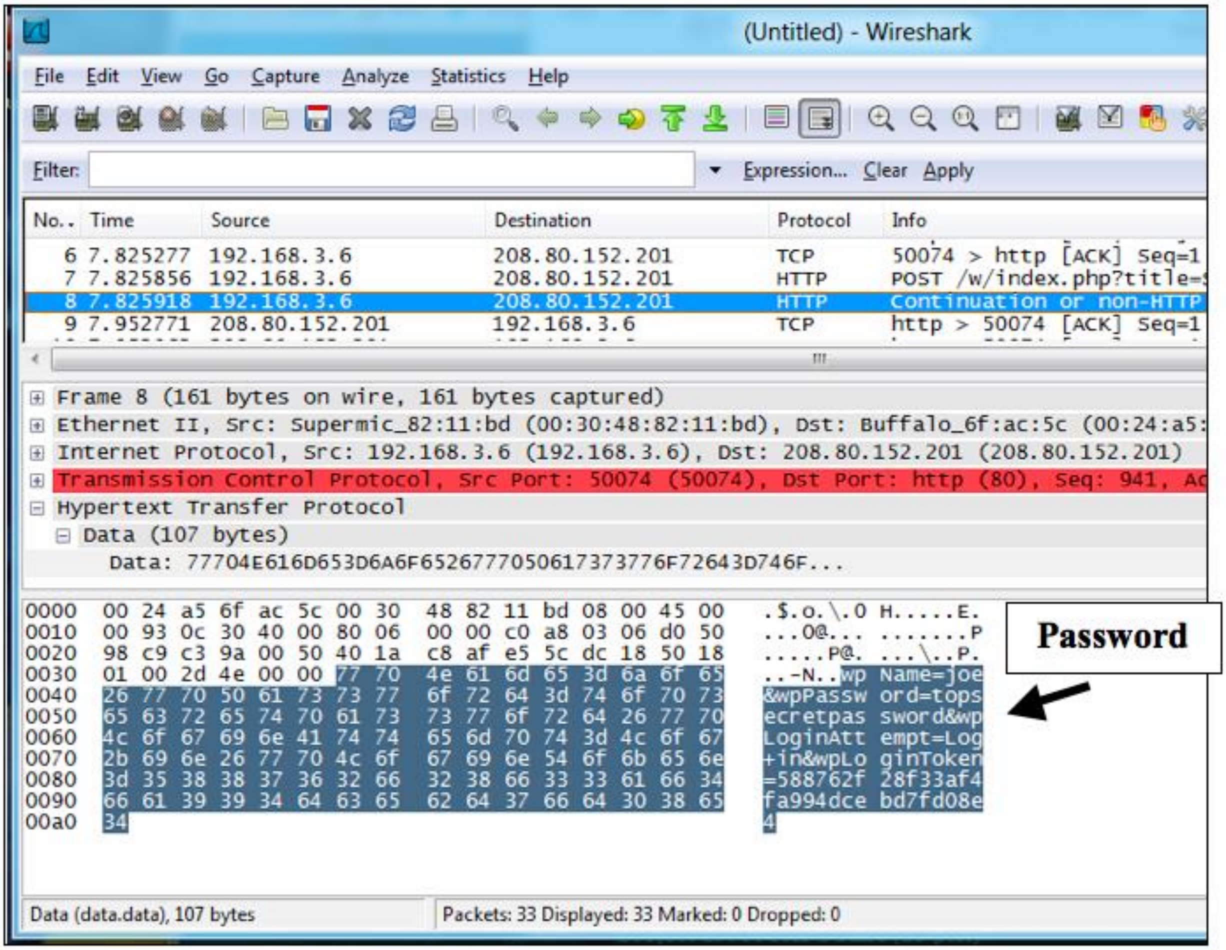
Unlawful Interception of Data

- Willful violation of the PAIA
- Willful violation of Cybercrimes Act

Potential civil damages suits

The method above, can **expose user data in clear text,** and details such as user names, passwords, bank account details etc. are, in the authors’ opinion, a violation of the POPIA.

The willful abuse of such method would constitute, in the authors’ opinion, violation of either or both the PAIA/Cybercrimes Acts.



(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No..  Time      Source          Destination     Protocol  Info
   6 7.825277  192.168.3.6     208.80.152.201  TCP       50074 > http [ACK] Seq=1
   7 7.825856  192.168.3.6     208.80.152.201  HTTP      POST /w/index.php?title=
   8 7.825918  192.168.3.6     208.80.152.201  HTTP      Continuation or non-HTTP
   9 7.952771  208.80.152.201  192.168.3.6     TCP       http > 50074 [ACK] Seq=1

⊞ Frame 8 (161 bytes on wire, 161 bytes captured)
⊞ Ethernet II, Src: Supermic_82:11:bd (00:30:48:82:11:bd), Dst: Buffalo_6f:ac:5c (00:24:a5:
⊞ Internet Protocol, Src: 192.168.3.6 (192.168.3.6), Dst: 208.80.152.201 (208.80.152.201)
⊞ Transmission Control Protocol, Src Port: 50074 (50074), Dst Port: http (80), Seq: 941, Ac
⊟ Hypertext Transfer Protocol
  ⊟ Data (107 bytes)
      Data: 77704E616D653D6A6F65267770506173776F72643D746F...

0000   00 24 a5 6f ac 5c 00 30  48 82 11 bd 08 00 45 00   .$.o.\.0 H.....E.
0010   00 93 0c 30 40 00 80 06  00 00 c0 a8 03 06 d0 50   ...0@... .......P
0020   98 c9 c3 9a 00 50 40 1a  c8 af e5 5c dc 18 50 18   .....P@. ...\..P.
0030   01 00 2d 4e 00 00 77 70  4e 61 6d 65 3d 6a 6f 65   ..-N..wp Name=joe
0040   26 77 70 50 61 73 73 77  6f 72 64 3d 74 6f 70 73   &wpPassw ord=tops
0050   65 63 72 65 74 70 61 73  73 77 6f 72 64 26 77 70   ecretpas sword&wp
0060   4c 6f 67 69 6e 41 74 74  65 6d 70 74 3d 4c 6f 67   LoginAtt empt=Log
0070   2b 69 6e 26 77 70 4c 6f  67 69 6e 54 6f 6b 65 6e   +in&wpLo ginToken
0080   3d 35 38 38 37 36 32 66  32 38 66 33 33 61 66 34   =588762f 28f33af4
0090   66 61 39 39 34 64 63 65  62 64 37 66 64 30 38 65   fa994dce bd7fd08e
00a0   34                                                 4
```

Password

Data (data.data), 107 bytes | Packets: 33 Displayed: 33 Marked: 0 Dropped: 0

See evidence below

Palo Alto Networks - How to Decrypt SSL using Chrome or Firefox and Wireshark in Windows

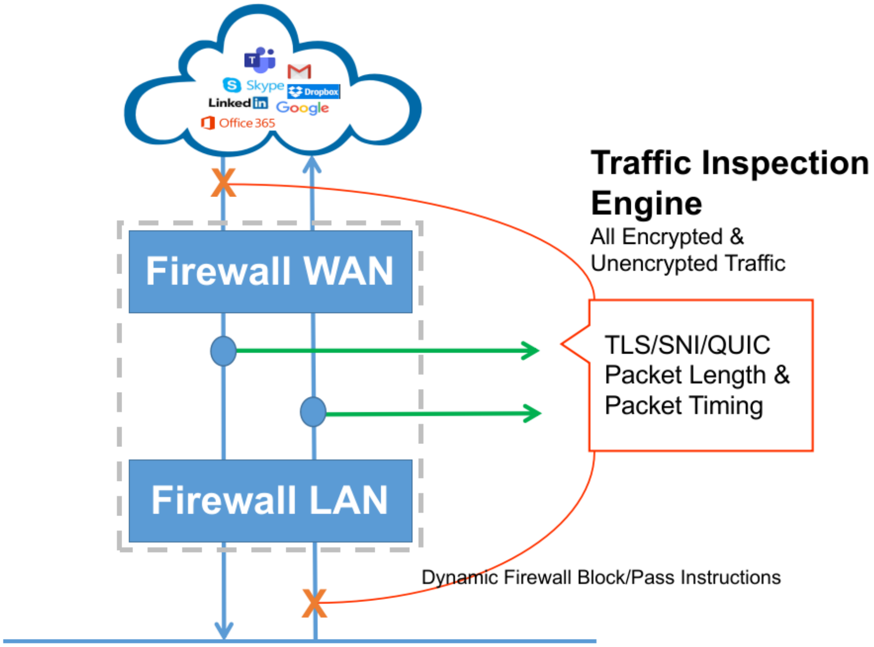
Palo Alto - Wireshark Tutorial: Decrypting HTTPS Traffic

Fortinet SSL Decryption

Fortinet SSL Inspection

So, is it possible to implement a solution that is highly effective in securing data in transit while avoiding unlawful interception?

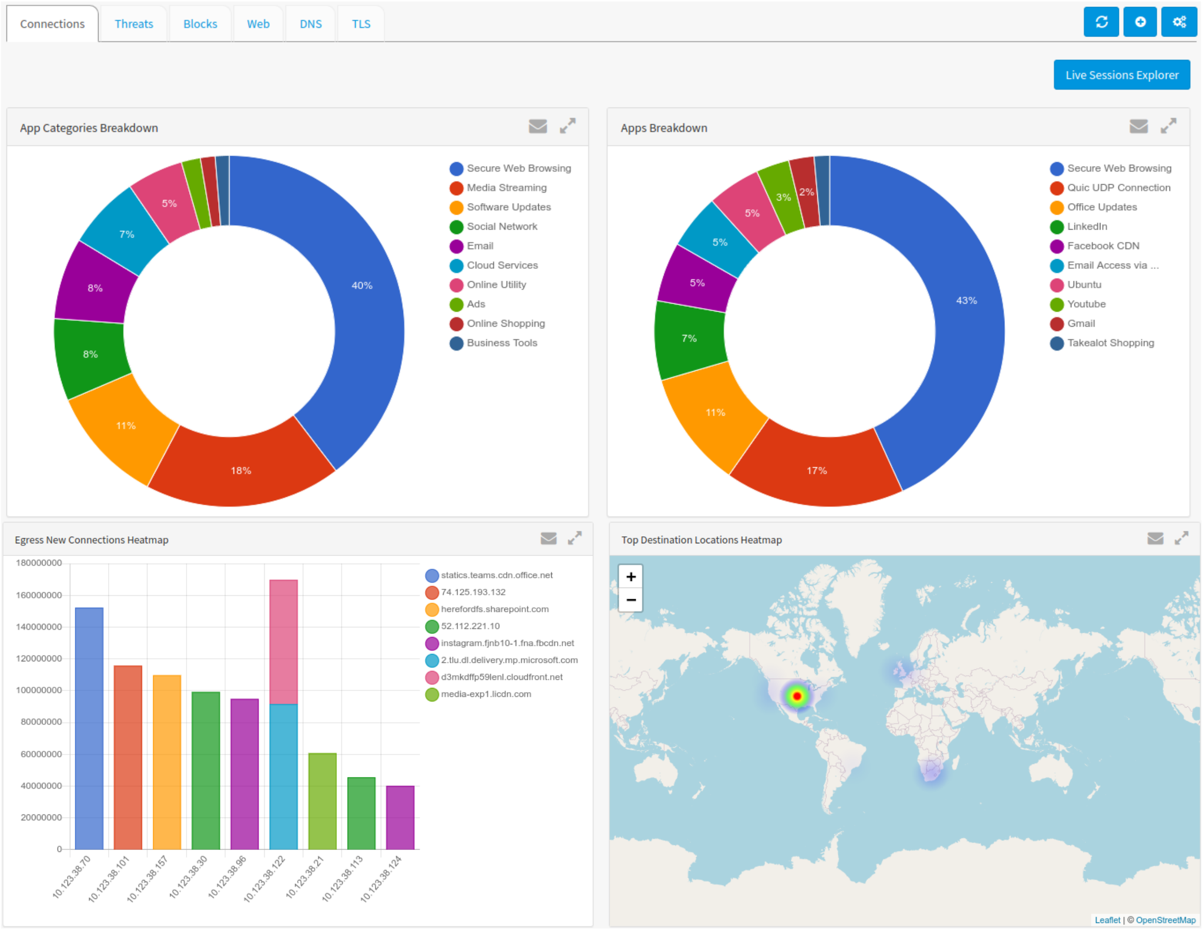
Lawful Non-Intrusive Traffic Inspection (No Payload Decryption)

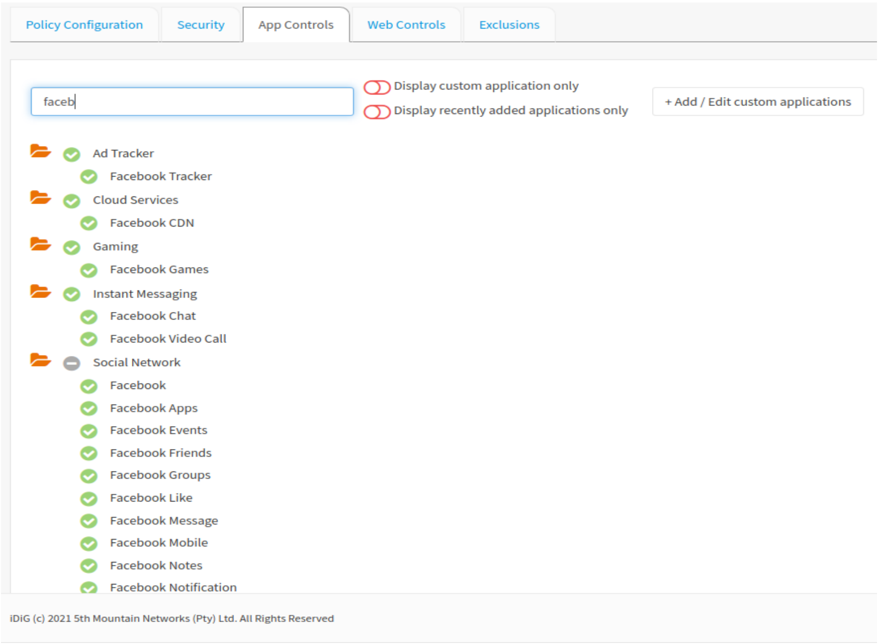

Skype
Dropbox
LinkedIn
Google
Office 365
Traffic Inspection Engine
All Encrypted & Unencrypted Traffic
Firewall WAN
TLS/SNI/QUIC
Packet Length &
Packet Timing
Firewall LAN
Dynamic Firewall Block/Pass Instructions

The authors are able to provide a solution based on inspection of TLS/QUIC and SNI while not decrypting payload data.

Algorithms acting on the data extracted through the three data sources listed above are able to provide a high degree of confidence in categorising the applications, the integrity of the sessions and ensuring that no in-session impersonation is underway. Further detail involving statistical packet lengths and inter-packet timing resulting from the inspection enable the solution to feature:

- Application Control
- Web Filtering and Security
- Advanced Network Analytics
- Real-time Cloud Threat Intelligence based blocking
- Cloud Centralised management & reporting
- User-based Filtering and Reporting
- Active Directory Integration
- Policy based filtering and QoS
- Application / Web category based Traffic Shaping and Prioritisation





faceb

○ Display custom application only

○ Display recently added applications only

- ✓ Ad Tracker
  - ✓ Facebook Tracker
- ✓ Cloud Services
  - ✓ Facebook CDN
- ✓ Gaming
  - ✓ Facebook Games
- ✓ Instant Messaging
  - ✓ Facebook Chat
  - ✓ Facebook Video Call
- ⊖ Social Network
  - ✓ Facebook
  - ✓ Facebook Apps
  - ✓ Facebook Events
  - ✓ Facebook Friends
  - ✓ Facebook Groups
  - ✓ Facebook Like
  - ✓ Facebook Message
  - ✓ Facebook Mobile
  - ✓ Facebook Notes
  - ✓ Facebook Notification

iDiG (c) 2021 5th Mountain Networks (Pty) Ltd. All Rights Reserved

Cost Comparisons

An indicative industry response that seeks to augment typical SD-WAN solutions with enhanced security capability is captured below:

The inclusion of other vendor derived pricing in the table below is for illustrative purposes only. The authors do not endorse or deem these systems mentioned to be POPIA compliant.

The associated link was re-published on IT-Web recently.

Pricing for Big Name Brand A is per site whereas pricing for Big Name Brand B and 5th Mountain is per user/device. Three examples are shown below based on different numbers of sites and users. Per customer pricing would however have to be calculated depending on number of sites and users for the specific customer.

It is clear that the 5th Mountain solution is a fraction of the cost in all cases. Please note that although we have made every effort in ensuring that the prices quoted are correct at this time, the pricing is indicative and should not be accepted as an official quote. Prices may also change without notice. (all vendors)

Big Name Brand A	Big Name Brand B	Halo Managed Secure SD-WAN
Security at the edge	Security in the cloud (IPSec)	Security at the edge
No SSL Inspection	Full in-line SSL inspection	Full in-line SSL/TLS inspection
Limitation of edge resources (CPU etc)	Unlimited cloud resources	No limitation - service based - not hardware
No DLP	Optional DLP	Packet level inspection DLP
No Sandbox	Optional Sandbox	No Sandbox
No ATP	Optional ATP	Comprehensive ATP
Remote Worker security (VPN only)	Full in-line mobile user security enforcement	Full MFA and SSL VPN for every user
	(Windows, Mac, IOS, Android)	(Windows, Mac, IOS, Android, Linux)
Edge Cost	**User Cost**	**User Cost**
$ 300 Annual License	$ 17 / user Annually	$ 5.35 - $ 10.69 / user Annually
	5 User Branch / $ 85 Annually	5 User Branch / $ 26.75 Annually
	10 User Branch / $ 170 Annually	10 User Branch / $ 64.10 Annually
	20 User Branch / $ 340 Annually	20 User Branch / $ 213.80 Annually
Big Name Brand A	**Big Name Brand B**	**Halo Managed Secure SD-WAN**
Business Case 1	**Business Case 1**	**Business Case 1**
Sites 500	Sites 500	Sites 500
Users 5	Users 5	Users 5
UTM = $ 300 * 500 = $ 150,000 (Annually)	**$ 17 * 5 * 500 = $ 42,500 (Annually)**	**$ 5.35 * 5 * 500 = $ 13,375 (Annually)**
(Excludes H/A)	(Includes H/A)	(Optional H/A + 50%)
Business Case 2	**Business Case 2**	**Business Case 2**
Sites 50	Sites 50	Sites 50
Users 15	Users 15	Users 15
UTM = $ 300 * 50 = $ 15,000 (Annually)	**$ 17 * 15 * 50 = $ 12,750 (Annually)**	**$ 6.41 * 15 * 50 = $ 4,807.50 (Annually)**
(Excludes H/A)	(Includes H/A)	(Optional H/A + 50%)
Business Case 3	**Business Case 3**	**Business Case 3**
Sites 5	Sites 5	Sites 5
Users 30	Users 30	Users 30
UTM = $ 300 * 5 = $ 1,500 (Annually)	**$ 17 * 30 * 5 = $ 2,550 (Annually)**	**$ 9.72 * 5 * 30 = $ 1,458 (Annually)**
(Excludes H/A)	(Includes H/A)	(Optional H/A + 50%)
(Excludes possible larger device required)		(No larger devices required)

Supporting Inclusion

The authors take this opportunity to include what we believe to be a substantial and meaningful article written by a person/s not connected in any way with 5th Mountain Networks of which we believe the substance supports our own view of the above.

Our privacy vs. their security: What's wrong with SSL/TLS Man-In-The-Middle, Anyway?

Ron Williams - Chief Technology Officer at InfoSec Global

Expectation vs. Reality

Our common expectation when using SSL/TLS (https) to connect to a web site is that our communication with that site are encrypted and therefore private. This is true only when both parties, client & server, are authenticated to one another using Public Key Certificates. However, the vast majority of websites that use SSL/TLS use single-sided authentication. They don't use SSL Client authentication and certificates. If you only use a Client Certificate with corresponding private key to connect to SSL/TLS enabled web sites - the following isn't relevant to you. However,

Transparently or otherwise, it is likely that at least some of your SSL/TLS sessions have been, or continue to be, read by a third party. For a sizable proportion of us, MITM monitoring falls completely within bounds of our employment contracts, whether we remember it or not.

In the employment case, SSL/TLS MITM is often described as the equivalent of having a security guard rifle through your backpack, purse, or briefcase before you leave the building. Security is simply enforcing company policy, looking for and 'blocking' assets that the employee is not authorized to carry off premise. When MITM is used in the employment or 'secure' facility case - it is the network equivalent of the security inspection before leaving the work.

What is SSL/TLS Man-in-the-middle?

SSL/TLS MITM is not about 'breaking' encryption, as no encryption is broken. It is about the man in the middle, or proxy acting as server to client, and as client to server.

If you think you've connected with Bank of Freedonia, and it looks and smells like Bank of Freedonia, and you 'know' that SSL/TLS is about encryption - it's understandable that you believe your communication is confidential. But is it?

SSL/TLS, based on public key cryptography, provides two basic capabilities - authentication and confidentiality. It provides for mutual authentication, each party authenticated to the other, and for server only authentication, where the server is authenticated to the client, but the client is not authenticated to the server - hence, single-sided.

Single-sided Authentication is by far the most common web server deployment, the server is authenticated to the client, but the client is not authenticated (via SSL) to the server. Enter the Man-in-the-Middle.

In a MITM scenario, a middleman (or proxy) represents itself to the server as a client, and to the client as the server. Instead of one connection directly between client and server, there are two connections established: the client user to the proxy, and the proxy to the Server. The proxy can see all the traffic in-between.

How to impersonate a legitimate site

The way the proxy represents itself to the client is as the legitimate server. It crafts a PKI Certificate that the client will accept as trusted. Among the ways a client might trust a certificate is by:

1. The user deliberately installing a 'MITM' certificate in their browser, keychain, or certificate store and marking as trusted

2. The client's organization installing a MITM certificate on the employee's machine via endpoint management and marking the certificate as trusted

3. A proxy forging a legitimate site certificate, signed by a Certificate Authority that has been granted 'Root' status. In this case the forged certificate is in the trust chain of a trusted root, and will be automatically installed in the client's 'Root Certificates' through operating system update, managed endpoint installation, or otherwise obtaining the current 'Global Roots.'

In the first two cases, this can be made completely transparent to the user. If I'm an employee, I know that my company requires such ability; there's no need such monitoring be hidden. I see the security inspection before I leave the building.

In the last case - forging certificates by means of a trusted Root or Intermediate CA - not only can the MITM do so opaquely (to the end user), but they do so by introducing serious vulnerabilities into the entire PKI infrastructure.

Why do you think this case introduces serious vulnerabilities? Legitimate vendors provide this for their legitimate customers!

Few legitimate MITM vendors use the Intermediate Trusted CA in their implementations.

They understand the risks the the public key infrastructure. Remember DigiNotar?

In order to craft a 'forged' certificate that will not cause an alert in the client's browser, the proxy must

1. Create a certificate with the destination Server's URL, to match the one requested by the client;

2. Sign the certificate with a private key corresponding to the trusted Root or Intermediate CA's certificate.

If the proxy creates the server certificate 'on-the-fly,' it must have access to a private key corresponding to the trusted Root or Intermediate Certificate. Anyone with access to the proxy can conceivably obtain the private key and generate 'trusted' certs ad nauseum.

Alternatively, a proxy vendor owning a Root or Intermediate Certificate could pre-forge popular site's server certificates and populate them into it's proxy, although there are technical challenges if the legitimate certificate binds the server's IP address to it's URL. In this case the forging will likely occur at the proxy, as the client's browser 'sees' the proxy's IP address as the servers.

The missing counter-party

You may have observed that outside of forging their certificates, I've made little mention of the expectation of the Web Service whose certificates are being forged. Like users, Web Services usually have an expectation that their SSL/TLS enabled service provides for confidential exchange of information between themselves and their users. Or do they?

Countering MITM

Web Service Providers are increasingly using techniques like Certificate Pinning and http strict transport security (HSTS) to mitigate MITM techniques. At the same time, MITM vendors (and attackers) are researching new ways to circumvent these techniques.

Conclusion

SSL/TLS MITM may have legitimate use cases in which all parties agree, Employer and Employees for example. Legitimate vendors provide this service in a way that is transparent to all parties. Such use may reflect genuine business need while respecting employee privacy by white-listing (no-inspection) financial, healthcare, or other user sensitive sites.

SSL/TLS MITM if institutionalized by allowing vendors to use trusted Root or Intermediate CA's to forge legitimate certificates, will continue to erode the security and reliability of the SSL/TLS PKI infrastructure.

Compromise of a MITM proxy that uses Root or Intermediate CA certificates techniques may provide an attacker with either the MITM CA's private key, or a pre-forged collection of otherwise legitimate certificates enabling them to do likewise, anywhere.

In order to distinguish itself from illegitimate or criminal exploitation, legitimate use of MITM should be accompanied by full disclosure and agreement of all parties.

5th Mountain’s Conclusion

“If you think you've connected with Bank of Freedonia, and it looks and smells like Bank of Freedonia, and you 'know' that SSL/TLS is about encryption - it's understandable that you believe your communication is confidential. But is it?”

It is the authors’ contention that every person has a reasonable and rightful expectation that his communication is end-to-end and secure.

It is further our contention that POPIA’s goals expect exactly that. The concept of eavesdropping cannot be contemplated in the protection of personal information.

It is also our position that by procuring large brand name products does not in itself make an organisation compliant with requirements that are sovereign and we urge South African based organisations, as responsible corporate citizens, to not institutionalise such systems as this will ultimately undermine the greater security of the internet through excessive whitelisting of websites to somehow comply with the regulations.

We also contend that by using a **“Think Global - Act Local”** strategy that it is possible to build a **“Blameless Networking Solution”** and that such a solution can outperform systems that are developed in and for largely their own sovereign entities who have unique and different geo-political purposes to the Republic of South Africa.

It is also our pleasure to present such a competitive (no-compromise) and blameless solution that makes commercial sense in an RoE limited environment.

In The News!

Justice dept cyber attack spills over to Info Regulator - 14 September 2021

[Justice dept cyber attack spills over to Info Regulator]

Advocate Pansy Tlakula, chairperson of the IR, says: “It is very unfortunate that this breach has occurred. As the regulator, we are concerned about the high number of security breaches in SA.”

“In August alone, 38 responsible parties suffered, and reported, security breaches.

Responsible parties are reminded of their obligation under POPIA to secure the integrity and confidentiality of personal information of data subjects by taking appropriate, reasonable, technical and organisational measures to prevent unlawful access to, or processing of, personal information. It is our role to ensure personal information is processed safely and securely. Failure to do so has legal consequences.”

5th Mountain Networks (Pty) Ltd
12th Floor, Bedford Centre
Cnr Smith & Van Der Linde Roads
Bedfordview, 2007
South Africa

+27 10 100 3639

info@5thmountain.co.za

5thmountain.co.za

5thmountain

5th Mountain Networks name and logo are trademarks of 5th Mountain Networks (Pty) Ltd. All other brand names, product names, or trademarks belong to their respective owners.

5thmountain.co.za