Network security procedures

By :Mohamed Firas Faisal

# Contents

[**Contents 2**](#_83vo1vvd65q5)

[**Introduction 3**](#_641uc3280051)

[**INVU 4**](#_k8ggora7auzi)

[**Company infrastructure 5**](#_rr2o3fndm3cr)

[Main Infrastructure 5](#_76nkkkd4d9aj)

[Flagged features of the company 5](#_mgqom1mvi959)

[**Improvements to be made to infrastructure 6**](#_h3n708v3wies)

[Ping monitoring 7](#_wrlvag9wes5f)

[Log file monitoring 7](#_mqqpt0aeqvl0)

[SNMP monitoring 7](#_xdkldge6p2c0)

[NetFlow monitoring 8](#_kh57ops01s6k)

[SQL query monitoring 8](#_rgov5fidlbh5)

[Other monitoring procedures 8](#_zezlcw3xwg5i)

[**More Pointers On Security 9**](#_998vhrutcat4)

[Audit and intrusion detection systems: 9](#_mx8jwuhiaq9q)

[Router Safety 9](#_q1hohwb2gdx5)

[Have a more robust security protocol for your networks 10](#_1ms2f2bu1di0)

[Reliable VPNs to use for your company 10](#_7sn5opl6dmyn)

[Physical Security measures 11](#_9s04mx96brx4)

[**Conclusion 12**](#_l5zv99ndyqyk)

[**References 13**](#_mgqsek5m7ei7)

# Introduction

In today's interconnected world, network security has become a paramount concern for individuals, organisations, and governments alike. As our reliance on digital information and communication grows, so does the potential for cyberattacks and data breaches. Network security encompasses the strategies, tools, and practices employed to protect the integrity, confidentiality, and availability of data and resources within a network. It aims to safeguard against unauthorised access, malicious attacks, and accidental disruptions, ensuring the secure and reliable operation of networks. This is a documentation about the network security of the company INVU. This documentation will be assessing and addressing the network security issued faces in the company and will give suggestions to improve accordingly.

# INVU

INVU is a leading data storage company that was founded on March 9 2008. INVU offers a comprehensive suite of secure and reliable data storage solutions for individuals, businesses, and organisations of all sizes.

INVU offers:

* On-Premises Solutions: Tailored physical and virtual storage solutions for organisations requiring data sovereignty and customised infrastructure.
* Hybrid Data Storage: Combine the flexibility of the cloud with the control of on-premises storage for a solution that caters to your unique needs.

As the company handles data it guarantees that you will get:

* User-Friendly Interface: Our intuitive and user-friendly interface simplifies data management and streamlines workflows for a seamless user experience.
* Dedicated Customer Support: Our team of experts is available 24/7 to provide comprehensive support and answer any questions you may have.

# Company infrastructure

## Main Infrastructure

INVU has state of the art server technology for speed and efficiency of storage of clients data. Uses multiple Hard Disk Drives for its servers. Users can store their data on the cloud using their website and application. Employees that work at the company have to follow a guideline imposed by the company. They audit their servers but not so regularly. The company has a small team of people that analyse the risk to data security. The network security they use is not up to date. They have very little security features and this is something that they have to improve on.

## Flagged features of the company

Frequent data loss: The company experiences frequent data loss events, leading to lost or corrupted files. Mainly due to the lack of a firewall. This can have devastating consequences for businesses that rely on their data for operations.

Inadequate data backup: The company fails to maintain adequate data backups, making it impossible to recover lost data. This can cause significant financial losses and reputational damage.

Poor data security: The company's data storage systems are poorly secured, making them vulnerable to cyberattacks. This can result in data breaches and expose sensitive information to unauthorised individuals. So far five cases of poor data protection have been reported. (viruses and hackers)

Poor physical security: The company is run in a small building with minimal security to their servers. This makes the servers vulnerable to physical attacks and natural disasters.

Inexperienced network security team: They audit the data regularly and find errors in their systems but do not know how to fix them

# Improvements to be made to infrastructure

For data Loss: For the frequent loss of data ensure that the system used has data protection features and that the connection between the servers and the clients (through the internet) is optimal for file transfer. Improve the connection quality from your ISP so that when your servers receive the data it won't get lost or corrupted.

Inadequate data backup: Add more storage space to your infrastructure and have Cloud backups of your clients data in another region or so. Use a secure connection such as a reliable VPN for the data transfer over the network to the offshore data backup storage. A VPN will make sure that your connection is secure from others trying to get into your network.

Poor data security: Use firewalls to monitor incoming and outgoing traffic in the network. When your employees are working make sure they are connected to a proxy server. A proxy server is a server application that acts as an intermediary between a client requesting a resource and the server providing that resource. It improves privacy, security, and performance in the process. Imbed IPSec (IP security) protocols in your servers. Have a good encryption method to your clients data so in a case of a breach the privacy will be ensured. Use anti hacking softwares to protect your clients data. Anti hacking software prevents hackers from intercepting the data in the first place.

Poor Physical security: Move your infrastructure to a better secured place. If not able to have a good physical security system in place in your current building.

Network Monitoring: Monitoring your network is crucial for the security of your clients data. Here are some Network monitoring techniques:

## Ping monitoring

Network pings are one of the oldest monitoring techniques, but it is still widely used by NPMs today. The monitoring tool sends a packet (or multiple packets) to a node or device, expecting to receive a response back. If the target node sends back an “all-clear” message, the monitor knows the node is up-and-running. However, if no response is received, it sends out more pings to get the node’s attention. If these pings still turn up nothing, the monitoring tool alerts the user.

## Log file monitoring

Typically, devices on a network will generate log files as they operate. These log files provide basic information that the device can report on, including any errors. While it isn’t as sophisticated as other techniques, some tools monitor log files to look for device-reported troubles. Log files are simple text files that might contain keywords such as “error” or “critical” that signal a problem with the node. Monitoring tools look for these keywords and report on anything unusual. The security team can use these logs in their audits.

## SNMP monitoring

SNMP is a device protocol that provides monitoring tools and nodes a common language to communicate with each other. The system relies on agents inside devices to provide information to network managers and monitoring tools. An SNMP manager sends out polls to devices to inquire about their current status, and devices can send traps when significant network events occur. NPMs that include SNMP monitoring have a common framework to talk to each other, centralising and simplifying monitoring capabilities.

## NetFlow monitoring

NetFlow systems use packet traps to examine traffic that passes through a part of the network. The NetFlow probes capture traffic data and then sends it to a monitoring tool for analysis. The analysis examines network traffic flow and volume to determine how data moves through the network. Flow-based monitoring systems, including NetFlow, analyse the conversations between devices and ensure that data and information is travelling along the network path smoothly.

## SQL query monitoring

To monitor databases connected to a network, monitors can utilise SQL queries. These queries ask the database to provide information on the number of data requests, transmissions, etc. Using this information, a monitor can determine if the database is performing adequately or not. Ideally, the database should be sending data across a network to accommodate for every request it receives; if the database is performing slowly, the monitoring tool can detect it and inform the network team. (Hein)

## Other monitoring procedures

Regularly check your network logs every month or even more frequently. Check for any unusual activity in the network. Audit the whole infrastructure every year or so. Do weekly or monthly checkups on your network logs

# 

# More Pointers On Security

## Audit and intrusion detection systems:

Use IPS. IPS stands for “intrusion prevention system” and it does what it says on the tin—it prevents intruders from accessing your network and causing irreparable and expensive harm through financial losses and data breaches.

It’s a network security system that analyses network traffic flows to detect, flag, isolate, and prevent malicious activity and code from harming networks. Often situated behind a firewall, IPS provides an additional, in-depth layer of analysis that further inspects web traffic—often performing a deep dive into IP packets and signatures to find any anomalies. Anything deemed malicious is isolated, resolved, and flagged with IT teams for further inspection. Some solutions also come with the ability to detect any vulnerabilities within the network, which can also be highlighted for admins to investigate. (Lightfoot)

## Router Safety

Schedule routine reboots to clear the system memory and refresh all connections. Rebooting the router may disrupt any potential malware that may have been implanted.

Disable remote access management, if possible, to prevent unauthorised people from remotely accessing your router and tampering with it.

Disable Simple Network Management Protocol (SNMP) to reduce risk of threat actors collecting basic system configuration information about your network.

Set up each router administrator with their own login username, unique password and appropriate privilege level. If event logging is enabled, then the login information will be important for auditing and incident investigation purposes.

Use Media Access Control (MAC) filtering to choose which trusted devices connect to your network.

Enable port filtering. (“Routers cyber security best practices - ITSAP.80.019”)

## Have a more robust security protocol for your networks

* Audit the network and check security controls.
* Revisit and communicate security policies.
* Update antimalware software regularly or as needed
* Set appropriate access controls and employ multi factor authentication
* Establish and communicate a security governance structure
* Educate end users
* Have a maintenance system for security infrastructure.

(Larsen)

## Reliable VPNs to use for your company

1. [Perimeter 81](https://www.comparitech.com/go/perimeter-81/l/list/) Our #1 choice VPN for business. Servers are capable of fast and stable connections that can handle all kinds of network traffic including SSH, RDP, VNC, and Telnet. You can even set up site-to-site VPNs.
2. [NordLayer](https://www.comparitech.com/go/nordlayer-business-vpn/l/list/) Specialist business VPN popular with small and medium sized organisations.
3. [Twingate](https://www.comparitech.com/go/twingate-business-vpn/l/list/) Business VPN which caters to remote teams with SSO support, split tunnelling, zero-trust access, and private gateways.
4. [Windscribe](https://www.comparitech.com/go/windscribevpn-business-vpn-list/) Budget business VPN option with top security features, easy to use apps and centralised billing option. Good documentation but lacks 24/7 support.
5. [CyberGhost](https://www.comparitech.com/go/cyberghost-business-vpn/l/list/) Great value service with secure apps that are easy to install and get started. Some of the fastest servers we have tested.
6. [IPVanish](https://www.comparitech.com/go/ipvanish-business-vpn/l/list/) Fast servers with secure and reliable connections. User friendly apps. Would prefer 24hr support.
7. [ExpressVPN](https://www.comparitech.com/go/expressvpn-business-vpn/l/list/) Extensive network of fast servers. High-grade encryption and even works great in China and the UAE. Not the cheapest option on this list.

(“7 Best VPNs for Business in 2023 and some to Avoid”)

## Physical Security measures

* Monitoring and Surveillance
* Keep the Network Devices in the Secured Room
* Use Rack-Mount Servers for added Physical Protection
* Keep a Check on the Work Space Security
* Use Case Locks
* Protect the Portable Equipment
* Save the Backups
* Disable the Ports
* Protect Your Output

(“10 Physical Security Measures Every Organization Should Take”)

# Conclusion

INVU is a decent data storing company. With the improvements mentioned above the company will have greater reliability and a much wider customer base. The most important thing is to ensure your networks are safe. Ensure that they are safe from hackers and viruses and malware and such.

# References

Works Cited

firas, editor. *network security notes*. 2023.

Hein, Daniel. “5 Network Monitoring Techniques Your Enterprise Needs to Use.” *Solutions Review*, 26 March 2019, https://solutionsreview.com/network-monitoring/5-network-monitoring-techniques-your-enterprise-needs-to-use/. Accessed 28 November 2023.

Larsen, Amy. “The top 10 network security best practices to implement today.” *TechTarget*, 15 November 2019, https://www.techtarget.com/searchnetworking/tip/The-top-10-network-security-best-practices-to-implement-today. Accessed 27 November 2023.

Lightfoot, Lottie. “The Top 10 Intrusion Prevention System Solutions.” *Expert Insights*, 3 May 2023, https://expertinsights.com/insights/top-10-intrusion-prevention-systems/. Accessed 27 November 2023.

“Routers cyber security best practices - ITSAP.80.019.” *Canadian Centre for Cyber Security*, 4 October 2022, https://www.cyber.gc.ca/en/guidance/routers-cyber-security-best-practices-itsap80019. Accessed 27 November 2023.

“7 Best VPNs for Business in 2023 and some to Avoid.” *Comparitech*, 17 October 2023, https://www.comparitech.com/blog/vpn-privacy/business-vpn/. Accessed 27 November 2023.

“10 Physical Security Measures Every Organization Should Take.” *DMAC Security*, https://dmacstrategic.com/10-physical-security-measures-every-organization-should-take/. Accessed 27 November 2023.