NetAbstraction™

Network Privacy and Its Impact on Security – Frequently Asked Questions (FAQ)

1. What is the difference between privacy and security?

Most people have a general understanding that security means protection. For organizations, security demands the protection of customer information and an organization's intellectual property from unauthorized or illegal attempts to access, steal, or corrupt the data.

Privacy on the other hand, can be interpreted several ways and is often misinterpreted as being interchangeable with security. Generally, privacy assures that personal information and corporate confidential information are collected, used, protected and destroyed legally and fairly. Privacy policies include processes that define what data can be collected, what are the permissible uses, with whom might it be shared and how long the data should be retained.

It is possible to have security without privacy, but impossible to have privacy without security.

2. What's the difference between personal and network privacy?

Personal privacy refers to a person's right to control their personal information and define how it is used and where it may be distributed. Personal privacy includes both the data and the owner's identity.

Network privacy is a newer and often overlooked concept of an organization's right and need to protect their identity, intellectual property and customer data while doing business over the Internet. NetAbstraction's network privacy solution never alters data, but rather the pathways that transport the data to protect both the data and the organization's identity. Network privacy becomes an additional layer of protection that significantly increases a would-be attacker's efforts to initially locate the desired data. If they can't find you…they can't attack you.

3. Why is network privacy important?

With a significant migration to the cloud and subsequent need for network risk management, network privacy has become a significant issue. Risk management involves three aspects: information governance, data privacy and security issues. Security is about the safeguarding of data, whereas privacy is about the safeguarding of user identity and related data. Privacy is integral to a truly secure network because it prevents exposure of the identity of the network user. If they can't find you…they can't attack you.

Networks are subject to attacks from malicious sources. Attacks fall into two categories: Passive, when a network intruder intercepts data traveling through the network, and Active, when an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

It is crucial that information security, privacy and data protection be addressed comprehensively at the design phase. Network privacy solutions need to be **proactively** implemented.

Barbara M. Hunt
CEO and Founder
bhunt@netabstraction.com
703-244-3938

4. How does NetAbstraction use "Privacy" to improve your network security?

The NetAbstraction service's operational design is based on using intermediaries (cutouts or surrogates) to acquire the commercial infrastructure used to implement the network. None of the infrastructure has been acquired in the name of NetAbstraction (to reduce possible targeting of publically known services). We protect our identity and also your's.

With "privacy" incorporated into our network design, we increase the security of your network in the following ways:

- We disguise your network communications pathways – if they can't find you, they can't target you!
- We dynamically shift your network – it is hard to identify or hit a moving target. We shift our customer's communications path on a regular basis or dynamically in response to a perceived cyber threat.
- We use a new tunneling protocol that is misidentified as normal TCP traffic, enabling the tunnels to privately hide (become lost) within the traffic of the commercial provider networks.
- We use multiple providers/technologies and geographic locations to disperse and layer any points of possible attack.
- By controlling the routing through our network, we are able to protect our customer's identity and location, optimize the path and improve overall performance.
- We protect your network and Internet access identity by providing alternate subscriber information, which is exposed in commercial providers' databases.
- We protect your network and Internet access identity which is exposed in commercial providers' databases, by providing alternate subscriber information. We also regulary rotate and exchange the infrastructure that we use to establish our physical infrastructure, to maintain overall privacy and avoid being a static point of attack.
- We logically isolate each customer's communications within our physical infrastructure, hiding the customer network topology from any external scrutiny, while also providing privacy and secure separation from other users.
- By creating a virtualized network, we decouple the logical network from the commercial provider's physical network. The logical decoupling of virtual servers from the physical network reduces the opportunity for attackers to reach resources connected to the network. It also isolates the logical network from vulnerabilities inherent in the physical network infrastructure.

Cloud infrastructure is acquired using identity management and protection domain expertise that NetAbstraction leadership gained through our extensive background in the U.S. Intelligence Community. We are cloud agnostic and always implement our network communications pathways across at least two different cloud provider networks.

Our patented ability to control the network routing increases network privacy and security, enhances performance and creates isolated channels of communications. If they can't find you…they can't attack you.

Barbara M. Hunt
CEO and Founder
bhunt@netabstraction.com
703-244-3938