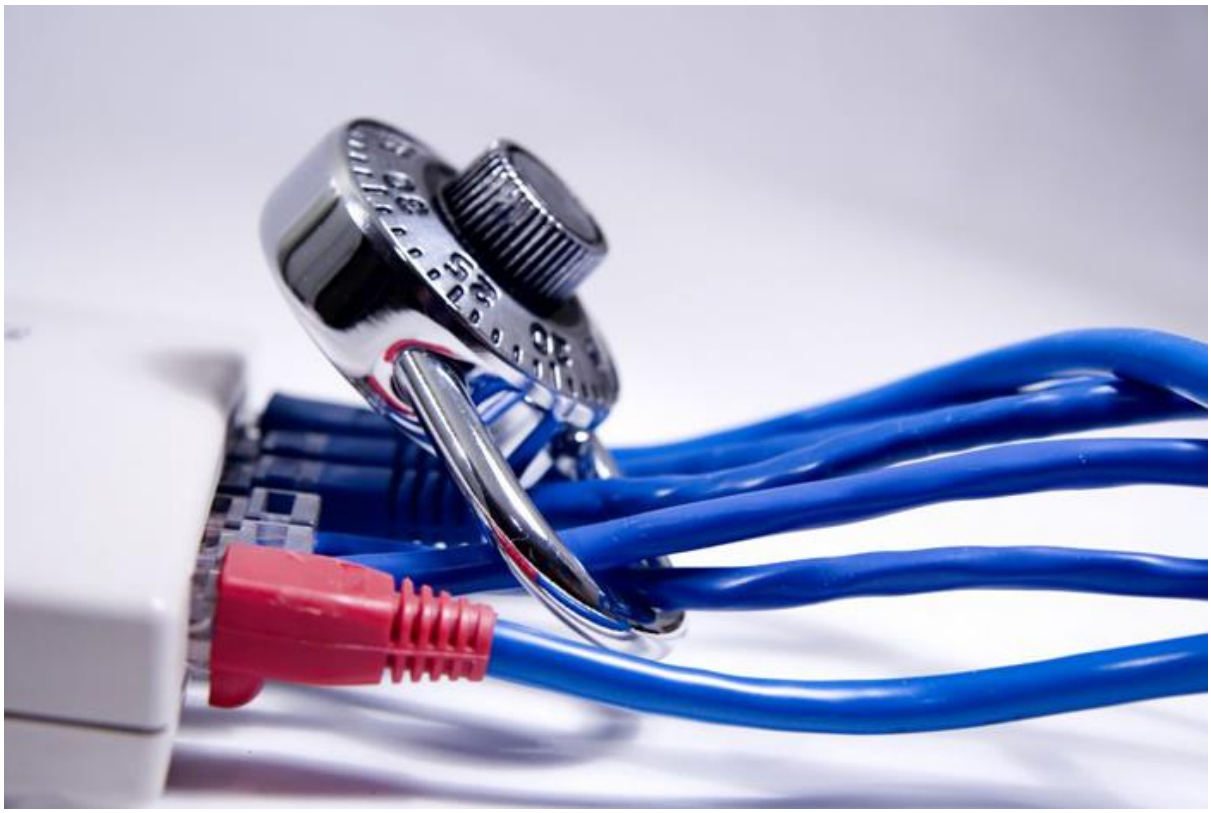
Why VPNs are not secure enough for hybrid networks?

Vijay Rangayyan, Instasafe



Virtual private networks, or VPNs, were created with the aim of providing secure connectivity between multiple people and devices over public networks like the internet. By setting up a point-to-point tunnel, consisting of a secure encrypted link between the user's device and the server of the VPN service provider, a VPN was seen as extending a private network over the public network. The main application of VPNs was seen to be the secure transfer of data, including corporate and financial data. The encryption and anonymity provided by the technology led to its adoption to protect data in transit across hybrid networks, protecting information from industrial espionage, government surveillance and criminals looking for valuable information that they can harvest and peddle. VPNs are of various types, depending on their topography, the security protocol that is used, or the tunnel's termination points. One of the more popular VPNs is the Secure Sockets Layer VPN, which uses the SSL protocol and can be used from a browser without client software.

VPNs often use old, insecure encryption:

However, research published in early 2016 suggested that 90 percent of SSL VPNs used insecure or outdated encryption. High-Tech Bridge, a provider of web and mobile application security testing as a service, reported in February, 2016 that it had scanned non-intrusively randomly selected, publicly available SSL VPN servers, and found that 77 percent of the tested SSL VPNs still use insecure SSLv3, with a few dozens still using SSLv2.

The survey also found other security gaps including the widespread use of untrusted SSL certificates and the use of insecure SHA-1 signatures, and the even older MD5. Browser vendors have discussed phasing out SHA-1 because of its security limitations, including potentially allowing the forging of a certificate, impersonating a server and intercepting critical data, according to the report. The serious gaps in the security of VPNs that have been discovered are a red alert for organizations who have placed their faith in these encrypted tunnels for their data in transit. The core of the technology is encryption and if that is seen to have holes then that would break the basic premise around which VPNs have been created. "DMZs and legacy VPNs were designed for the networks of the 1990s and have become obsolete because they lack the agility needed to protect digital businesses," Gartner analysts wrote in a report titled "It's Time to Isolate Your Services From the Internet Cesspool", of September 30, 2016. The report also said that network designs that expose services and accept unsolicited connections present too much risk. "Security leaders can reduce risks using software-defined perimeters and other techniques that isolate applications from the internet," it added.

VPNs offer only all-or-nothing access:

VPNs did a fine job by providing remote users with network access as if they were still on the corporate network but it all worked well, using multi-factor authentication, as long as the network perimeter was well-defined and there were static user and server resources, according to the SDP Working Group of the Cloud Security Alliance. That scenario has changed dramatically as mobile workers access the corporate network from multiple and dispersed locations using a variety of devices. VPNs do not also allow for fine-tuned, multiple-level access to resources on the organization's network as they operate on an "all-or-nothing" principle for access to the assigned network, meaning that all

users have full network access to the entire VLAN, according to the Cloud Security Alliance study. VPNs also do not provide security to on-premise users, requiring organizations to have a different set of technologies and policies to control access by on-premises users.

Software-defined perimeter:

The Cloud Security Alliance backs the Software-Defined Perimeter, a new strategy for controlling remote access to the network. Key to this approach is the authentication and authorization of the person and the device before allowing even a packet to reach the target server, which means that cloud resources are kept hidden to unauthorized users. The upfront authentication and authorization of remote users and their devices also allows organizations to give access to their networks selectively and with granularity, so that some users, for example, would be able to access only a corporate application or part if it. This strategy helps overcome the all-or-nothing access found to be a major drawback on VPNs.

SDP and the ‘black-cloud’

In today’s diversified IT environment consisting of mobile devices, hybrid clouds and public clouds, the SDP allows organization to blacken the cloud to all but trusted devices. As the number and variety of devices in an organization can only potentially increase — if one considers the large number of mobile devices and internet of things sensors likely to want access to IT infrastructure — organizations are going to have to darken parts of the internet, so that access is closed until a device is properly authenticated. SDP therefore moves to a system of least privilege and zero trust rather than access by default. Access is provided only once full authentication and trust is established. The Cloud Security Alliance’s concept of the black-cloud is not new and was first mooted by the U.S. Defense Information Systems agency. The advantages of SDP is that it supports a variety of devices beyond laptops and PCs and links device and user identity, providing an additional level of security. Policies are also based on the user rather than the IP address, making true and secure mobility a reality.

Challenges for organizations:

SDP offers strong authentication up-and-down the stack, said research firm Enterprise Strategy Group. Besides defining a number of connection types such as client-to-gateway, client-to-server, server-to-server, and private cloud-to-public cloud, the architecture requires strong authentication from layer 2 or 3 up to layer 7, and numerous technologies for authentication such as biometrics, tokens, smart cards, encryption key management like key generation, key distribution, key rotation, etc., and certificate management, and PKI, according to ESG. “Few

civilian organizations have thought through the ramifications of authenticating every transaction and encrypting every network session," ESG analyst Jon Oltsik wrote in a blog post. "This must be done strategically or it becomes an operations nightmare and IT risk," he added. Although SDP offers tremendous potential security and data protection benefits to organizations adopting the standard, they have to be careful about how quickly and which parts of their infrastructure they transition first to SDP. Don't junk your VPNs, at least not yet. Some parts of the organization data and applications may be still fine traveling through only a VPN for now.