International Journal of Grid Distribution Computing
Vol. 8, No.6, (2015), pp.41-48
http://dx.doi.org/10.14257/ijgdc.2015.8.6.05

Carrier-Class VPN to Cloud Evolution

Kire Jakimoski, Vladimir Bogoevski and Dejan Kochov

FON University, Faculty of Informatics, Skopje, Republic of Macedonia
kire.jakimoski@fon.edu.mk

Abstract

This paper analyzes the technology of cloud computing and the challenges that occur when connection is established through the Internet and public devices. Devices used for connection to the secured network very often don't meet the security levels of the network that they connect to. To ensure that the connection is secured even from a public device and through the Internet major role is played by older technology, VPN. Therefore, we will present the security measures taken to secure the remote connection and the challenges faced to meet such a level, benefits, reliability, performance and latency of an enterprise network. These issues must be solved appropriately to ensure the confidentiality and integrity of data and information, as well as overall corporate network security. Obtained analysis in this work also presents the evolution of the cloud related to VPN, addressing the general security risks associated when using devices via VPN to access to an enterprise internal network. Furthermore, we analyze SSL VPN security risks in this context.

Keywords: *attacks, cloud, enterprises, secure network, secure remote access, SSL*

1. Introduction

There have been very few changes in the Virtual Private Network (VPN) business network area over the past few years, while there have been many improvements in other IT sectors such as processing, storage, and consumer networking. The evolution in networking introduced cloud services, but new security threats have arisen, and there is increased number of people working remotely on the devices they are using [1].

The improvements that are done in past few years put a challenge on the traditional VPN networking approach, making space for a new way for networks in the cloud. There isn't any sense for remote workers to establish a remote connection to their office to access the servers, files or applications that are in the cloud [2]. People increasingly work remotely and they need LAN-like access to their work network from where they are and on the device they are using. The VPN hardware is natively less unnecessary than today's cloud services and the VPN hardware and configuration requirements make the solution not scalable and inflexible.

Now every business is able to afford enterprise-class applications, data storage and computing which is provided with the changes in the IT infrastructure made by the cloud. It is important to note here that virtualization is a key feature to cloud computing. [3].

In recent years, various virtual private network (VPN) technologies have been widely used to provide secure site-to-site connectivity and remote access [4]. There are many reasons for such overwhelming adoption and business success. Two major factors are total ownership cost savings and productivity enhancements. The total ownership cost can be considered as the initial deployment cost plus the cost of user training, support, and facility maintenance over time. Productivity enhancements can be measured in terms of tool effectiveness, user time savings, usability improvements, and user satisfaction.

Secure Sockets Layer (SSL) VPN is an emerging technology that provides remote-access VPN capability, using the SSL function that is already built into a modern web

ISSN: 2005-4262 IJGDC

browser [4]. SSL VPN allows users from any Internet-enabled location to launch a web browser to establish remote-access VPN connections, thus promising productivity enhancements and improved availability, as well as further IT cost reduction for VPN client software and support.

In Section 2 we cover the differences how the VPN was used in the past and how it all started, and the role that VPN plays today in cloud technologies.

Section 3 is about the evolution of VPN to the cloud, and improving the security while eliminating threats. It goes in-depth about network to network and point to point VPN's, security models, security issues that are related to VPN and addressing the risk that might come up with it.

Section 4 covers the performance, latency, reliability of the cloud network and SSL VPN connection and configurations that are made to improve them.

2. VPN: In the Past and Now

With the start of the globalization, businesses had a rough time with connecting business branches geographically. The internet, besides comparatively cheap connectivity, was an opening for the businesses to build private networks on the public internet infrastructure, and for the first time access networks from remote locations [5]. That was the start of VPN networking.

With the start of the VPN used infrastructure was simpler and cheaper for installation and implementation of the technologies used before. With the cheaper and simpler infrastructure VPN provided an easier way to create geographically dispersed business networks even for midsized level businesses. The demand for VPN products was extremely huge, and was represented by some of the leading equipment vendors in the world. The VPN hardware based solutions with the need of ongoing management time, ongoing support contracts, required installation time and complexity, and the upfront costs caused stagnation and hardly followed the new IT technologies.

Just as the cloud technology caused enterprise-class applications, computing, and storage available and affordable to every business, cloud networking has the potential to do the same for networking. The achieved goal with cloud VPN is describing the connectivity component of the cloud networking, allowing networks to be built without cost, complexity and limitations of hardware based VPN. Cloud networking concept is simple. All of network core functions are moved to the cloud, so the need for configurations and local hardware is eliminated. The benefits with cloud network are the same as other cloud based IT services that are faster deployment time, easing the administration of the network, no need to replace the hardware, no software updates or maintenance, built-in scalability and redundancy, accessing the network from an internet connection [6].

3. VPN to Cloud Evolution

Network-to-network VPN itself has many security threats. Hacking through the encrypted tunnel undetected is almost impossible. This provides the attacker with the capability to use many services on many hosts in order to gain access and control of cloud computing data. The network-to-network offers network transparency and management that enables analysis of the traffic after the point of decoding, but it does not take care of the data payload end-to-end. If any part of the cloud is jeopardized, all parts associated to that cloud via network-to-network VPN technology have to be treated like endangered. This can be problem that occurs when high secure network is associated to a security weaker network, so the secured part is equally threatened to the exposures that aren't secured in the weaker network. Because of the cloud computing design, clients not always know when part of the network is added to another, likely weaker ensured network.

Second type of VPN is point-to-point VPN, granting encrypted connection from customer to host for numerous services. Considering these associations, much like network-to-network association, appear at layer 3, and most of the equal assurance concerns found in the network-to-network VPN happen here as well. Luckily, almost all cloud computing service providers choose to use the service-to-host design through SSH, SSL or other dedicated service. There are faults in the service-to-host form, but if there are limitations on the size of the access area, the security footmark will be reduced, so monitoring and securing will be more manageable. This kind of form is providing surveillance on the overall session. To increase the security on the process, cloud service provider can insert logging forms and security controls, and this depends on the service provider`s security models. Components like logging and event surveillance are demanded by the enterprises compliance software, so there are recommendations that clients have to define processes and actions related to auditing, logging and noting. Connectivity infrastructure of enterprise networks, corporate or a small office depends on the predictions on the performance and latency of the provided network intended to be of highest carrier-class. Such networks use different methods of virtualization to achieve the advantages of network efficiency and resource integration. The virtualization of network can be at a link, device and service level such as with layer 2 multiprotocol label switching and layer 3 VPNs. Multiprotocol label switching based VPNs are easy to carry out, security level is undoubted, providing scalability and high performance with low latency. Enterprise clients now look for an entire IT solution to ensure their business agility and they need it at lower costs. In order to build global VPNs business needs to rent virtual private links and network resources. With the expanding virtualized data centers and the inexpensive availability of the infrastructure, and Software as a Service (SaaS), clients are more interested for hybrid cloud solutions. Crucial part of the infrastructure of the overall hybrid cloud solution is dependent on the network. In the present, company customers need to exit the VPN and use public Internet so they can connect to a public cloud provider. Sometimes, the public cloud provider can loan network resources from various service providers to connect a huge enterprise`s private clouds to its public cloud status, building hybrid cloud environments. Different solutions pose probable concerns in some fields [7, 8].

3.1. Threats and Security

Clients may not be able to choose to create or control the security protocols for their traffic flow in the public cloud or control the level of isolation of their applications from other tenants. Common security solutions can’t see into the traffic of the virtual machine (VM) within the cloud, nor do they have the ability to extent it, restricting them from addressing the security needs to the basic network, and thereby exposing security risk. As long as users work remotely, using different devices with different operating system with applications connected on various network types, they also provide more chances for intruder attacks. These options make managing and securing the cloud VPN much harder for the corporate administrators. The devices themselves are a source of concern. Is the device owned by the corporation, if not, how can the company secure configuration and patching? If the corporation has regulated specific remote access VPN users like Cisco Systems VPN client or Barracuda Network SSL VPN agent, what if vendor’s software is not applicable on various platforms and devices? This can be avoided by limiting the access to network resources like email, to specific services based on the security control level of the device. In practice it`s hard to deny the access to email on devices like smartphone, particularly when its seen as standing in the way of progress on the company. Creating a basic standard to define what establishes decent security for devices owned by the company would ensure safe remote access through the cloud. Company`s devices that not meet the basic standards can be blocked from accessing the cloud or can be only allowed to use low-sensitivity information or services. Other alternative is enterprises to

create a set of allowed and supported devices that are configured to correspond with the company policy and used according to the acceptable usage plans. Recommended functionalities that devices should have are antimalware software support, file system level encryption, VPN customer support and set password secured boot.

Risks and threats that might occur with remote connection via Internet and through public or unsecure devices are:

Risk related to user's authorization - The VPN is providing simple way to access enterprise network and shared data, easily from the Internet. The security of the VPN is determined and leveled from the methods that are required from the users or devices to gain authorization to access the secure corporate network. If the authorization methods are simple, like static password may be exposed to attacks like passwords cracks, snooping or social engineering attacks. Authorization that is requiring input of something that user has and something that knows is a basic requirement for secure remote access to the enterprise network. There are cases where three factor authorizations are needed. This requires biometric identification like fingerprint, eye scan *etc*.

Spread of malwares, viruses and other threats from user computer to the enterprise network - The remote access poses a threat to the network security. The remote computers that haven't met corporate security and gained access to the network, potentially can forward viruses, malwares to the corporate network. To evade such a risk to the corporate network, updated antivirus software is a must on the remote computer used to connect to the network.

Split tunneling - Split tunneling comes in position whenever a computer on the remote end of a VPN tunnel at the same exchanges network traffic with both networks shared and the internal network without initially placing all network traffic in the VPN tunnel. This case opens a door for the intruders on the shared network to bypass the security of the remote computer and use it to gain authorization on the internal network of the corporation. Efficient way to improve security from network based attack is to have host based firewall.

Host security software it`s not required on public devices - Connecting with SSL VPN from wherever via Internet to the enterprise internal network is very easy and comfortable to use. But there is an inconvenience when for establishing a connection through SSL VPN public devices are used, because it can lack appropriate maintained antivirus software or very likely it can be without installed host based firewall. These devices are big risk when used for secure connection, like SSL VPN. Such devices can be an excellent way for viruses, malwares, Trojans and other malicious software to be spread on the entire network, compromising the security authentication used to defend the network. This can be a case if the device is hijacked by an attacker and used as a back door to use a live session to compromise the internal resources with malicious software.

Physical access to shared device - If a device remotely connected to the corporate network is left by the user with online session, network becomes opened to anyone who may have access with that device. Because the device is opened for everyone physically there is a threat of compromising the internal network. Such a risk is enlarged by SSL VPN because the connection can be made from any device connected to the Internet.

Keystroke loggers - Devices used with SSL VPN connection are much more exposed and weaker to keystroke loggers, as a result of establishing the secure connection on public devices. Such a device probably doesn't have the required security standards of the secure enterprise network and might be threatened and software like keystroke logger may allow leaks on classified data, user authorization and other sensitive information. This and other kinds of malicious codes are best to be detected before establishing connection with secure network. There are kinds of products with these security options that can easily detect key loggers before connection is attempted. The success and performances are variable depending on the vendor`s offer.

Man in the middle attack - In this kind of attacks, intruder cuts off the client connection and gains sensitive and secure data. After gaining the authorization data the intruder can use this data to connect to the secured network. At the time of the attack the intruder uses gateway that is shown as a false SSL VPN site to the client, so the gateway bypasses any authorization that client is entering on the real site. Through the malicious gateway and the technologies it have, there can be multiply actions that the intruder can take upon the secure network. The client connection can be ended with phony message that connection can't be realized or something similar. In this kind of attacks, client hasn't checked precisely if the communication is with the real SSL VPN website.

Security policies and secure access through strong user authentication - SSL VPN deployment and clients of SSL VPN should conform to the remote access and VPN security strategies in the organization. Strong client authentication is a top need; several decisions are available to accomplish this purpose. Commonly, one begins by executing two-factor validation procedures. Examples for this issue are incorporate hardware tokens, digital certificates (as a form of client authentication), and smart cards. In addition, our association ought to clearly state what sort of host security requirements must be met, (such as individual firewall, antivirus, hot fixes, or security patches). Different choices should include whether the organization permits split tunneling.

Host identity verification - There is a distinction between trusting a client (after passing strong client authentication) and trusting the client's computer. A Trojan-loaded PC defeats strong user authentication. A "company computer", which commonly supported and managed as indicated by corporate security policies, typically deserves more trust then a "non-company computer". A protected SSL VPN infrastructure should permit us to verify a remote host's identity by checking on predefined end device parameters. Examples include registry entries, special records in a predefined location, or digital certificates (as a form of device authentication). The host identity data can be utilized to make our access permission decisions.

Secure desktop – What do you do if a remote PC does not meet your thorough corporate security policies and benchmarks? A noteworthy SSL VPN business advantage is to allow clients to "VPN in" from any Internet-based PC. A hefty portion of them are non-company assets that typically would not meet your security arrangements and guidelines. To settle this issue, some recent VPN SSL products give the ability to create a protected "sandbox" or "secure desktop" on remote computer. This safe desktop is commonly protected from other processes on the computer and has an "on-the-fly" encrypted file system. Malicious code, regardless if it's present on the computer, will not be able to access the content in the protected desktop. This sort of usage additionally guarantees that information will be deleted in a safe way at the end of the session.

4. Performance and Latency

Channeling in-cloud traffic to a foreign firewall may lead to bigger latency and delay, which could affect the cloud performance and the use of tunneling through the Internet can reduce the bandwidth availability. Internet latency can be very unstable as there are not SLA (Service-Level Agreement) guarantees. Access to the services of the public cloud can be acceptable for business applications that are not critical, while the usual enterprise customer cannot work with unpredictable bandwidth availability and latency and need to have a good level of application performance for the business-critical applications.

To improve security and performance on the network there have been changes to traditional VPN IP security into SSL VPN, backup data into data protection and network tunneling into application tunneling.

SSL VPN has many advantages in comparison to some other known VPN technologies. For providing a secure connection between remote users and private

network resources, SSL VPN uses SSL protocol and its successor, Transport Layer Security (TLS). Nowadays this SSL/TLS function is found in almost every modern web browser. Contrary to traditional IP Security (IPsec) technology, where installation of IPsec client software is required on a client machine before a connection can be made, that is not the case with SSL VPN where users are not required to install client software. Because of this the SSL VPN is also known as "clientless VPN" or "Web VPN". SSL VPN has many great features; one of them is the user-friendly interface. Different IPsec VPN merchants can have various implementation and configurations requirements, while SSL VPN only needs a modern web browser. End users are able to use their favorite web browser without being restricted by the operating system. Another SSL VPN advantage for clients is in the field of outbound connection security. In many situations, outbound Secure HTTP (HTTPS) traffic, which is also based on SSL, is not blocked.

There is a difference between a full VPN tunnel and an SSL-enabled proxy server. The latter is an application door that supports a certain type of applications. A complete SSL VPN, on the other hand is a VPN that gives all VPN qualities and local LAN client experience (in terms of network access). In the event that application access requirements are modest, SSL VPN does not require additional client software to be installed on the endpoint machine. For more extensive application access, a dynamically downloadable tunneling client is commonly delivered when expected to the customer device to support such full SSL VPN capabilities [9].

Required data protection is most important for improving the security to the network, but there must be changes with the enabling remote connections to the network. Traditional backups requires more performance and it`s not cost effective and practical anymore. This may be solved with many software products for backups, opening many alternatives to the old disk based backup. Making data protected as it is created can be done with continuous data protection, and with assurance that backups would not create an operational dangerous impeding access to the remote access VPN.

4.1. Reliability

Businesses need to always have access to applications with reliable network availability so they can run critical applications in the public cloud, very much alike to that accessible with carrier-grade enterprise VPNs. The business firms need to work with multiple vendors to set up hybrid cloud solutions. Among the countless available cloud solutions, mostly middle sized businesses are likely to use myriad of cloud solutions. The communication supplier can assist into integration to the cloud services chain, through providing a protected and trustworthy cloud connection to numerous public cloud providers. This integration also influences on weak isolation and recovery in the case of weaknesses along the service string.

Cloud computing framework is constituted of host, servers and network transit. The assortment of devices, transportation and abstracted management and expectations demand organizations to divide their security on layers completely to ensure that relations and data are well secured. Using one service VPN for accessing the cloud is known to be the most secure and can decrease the risk to compromise both the client and the server [10]. The user must still stay aware of the cloud server design and need to enhance as much as possible his security form into the cloud.

5. Conclusion

Because the demands by the enterprises need improving the mobility of their workers, changes in the infrastructure of the network are necessary. Some improvements were done in the past few years that put a challenge on the traditional VPN networking, making room for a different way of networking in the cloud. For improving the security of the network VPN plays main role, establishing secure access to the network from the Internet.

There is great need for remote workers to establish a remote connection to their office to access the servers, files or applications that are in the cloud.

Security risks comes with the usage of remote connection from devices that may not meet the security criteria of the corporate network and lack of knowledge of the workers to check all the security measures before attempt to connect to the secured network. Education on workers for that matter and accurate configuration of the SSL VPN makes the connecting easy to use, reliable and secure.

References

[1] G. Shroff, "Enterprise cloud computing: technology, architecture, applications", Cambridge university press, **(2010)**.
[2] J. Bond, "The enterprise cloud", **(2015)**.
[3] U. Gurav and R. Shaikh, "Virtualization: a key feature of cloud computing", Proceedings of the International Conference and Workshop on Emerging Trends in Technology, ACM **(2010)**, pp. 227-229.
[4] P. J. Kaur, and S. Kaushal, "Security concerns in cloud computing", InHigh Performance Architecture and Grid Computing, Springer Berlin Heidelberg **(2011)**, pp. 103-112.
[5] R. Venkateswaran, "Virtual private networks", Potentials, IEEE, 20(1), **(2001)**, 11-15.
[6] T. Velte, A. Velte, and R. Elsenpeter, "Cloud computing, a practical approach", McGraw-Hill, Inc. **(2009)**.
[7] H. Zhang, G. Jiang, K. Yoshihira, H. Chen, and A. Saxena, "Intelligent workload factoring for a hybrid cloud computing model", World Conference on Services-I, IEEE, **(2009)**, pp. 701-708.
[8] J. Qiu, J. Ekanayake, T. Gunarathne, J. Y. Choi, S. H. Bae, H. Li, and G. Fox, "Hybrid cloud and cluster computing paradigms for life science applications", BMC bioinformatics, 11(Suppl 12), S3, **(2010)**.
[9] S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "Guide to SSL VPNs", NIST Special Publication, 800, 113 **(2008)**.
[10] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud security and privacy: an enterprise perspective on risks and compliance", O'Reilly Media, Inc. **(2009)**.

Authors

Kire Jakimoski received his B.Sc. degree in the field of Telecommunications from the Military Academy "Mihailo Apostolski" in Skopje, R. Macedonia in 2002, M.Sc. degree in Electrical Engineering in the field of Telecommunications from the Ss. Cyril and Methodius University in Skopje, R. Macedonia in 2007, and Ph.D. in technical sciences from the Ss. Cyril and Methodius University in Skopje, R. Macedonia in 2013. From 2002 to 2006 he works as an Officer for Telecommunications in the Ministry of Defense in the Republic of Macedonia. From January, 2006 to March, 2012 he works as an adviser for information security in the Directorate for Security of Classified Information in the Republic of Macedonia. From March, 2012 he is with Faculty of Informatics, FON University in Skopje. Also, he is an author/co-author of around 30 published research papers and one book. He is an Assistant Professor at the Faculty of Informatics, FON University in Skopje, Macedonia. His research interests include Information and Communication Technologies, Wireless and Mobile Networks, Heterogeneous Wireless Networks, Information Security.

Vladimir Bogoevski and **Dejan Kochov** are students at the Faculty of Informatics, FON University, Skopje, Republic of Macedonia.