VPN Security Considerations for Financial Institutions Migrating to the Cloud

Síofra O'Neill

M.Sc. (Software Design & Development)

National University of Ireland, Galway

Discipline of Information Technology

College of Engineering & Informatics

23 August 2013

Head of Discipline:

Dr. Michael Madden

Supervisor:

Dr. Michael Schukat

Abstract

In a financial institution, IT risk management is driven by the need to adhere to industry and legislative regulation, hence data security is paramount. For this reason, financial institutions should stress test for potential vulnerabilities before migrating services to the public cloud.

This research paper focuses on one particular attack vector in cloud technology, the Virtual Private Network (VPN). The VPN is a gateway to an institution's private network. Malicious exploitation of this gateway could have potentially devastating effects on an institution's reputation and business.

The purpose of this thesis is to demonstrate a number of ways in which IPsec VPNs can be exploited. The practical experiments detailed in this study illustrate vulnerabilities in VPN technology, and highlight why financial institutions should adopt private cloud instead of public cloud solutions. These experiments are performed using freely available security tools, and are designed for use by any IT professional; not just security experts.

Table of Contents

List of Figures

1 INTRODUCTION

1.1 Overview

In a financial services institution, IT risk management is driven by the need to adhere to industry and legislative regulation, hence data security is paramount. For this reason, financial institutions should stress test for potential vulnerabilities before migrating services to the public cloud.

The purpose of this research is to study one particular attack vector in cloud technology, the Virtual Private Network (VPN). The VPN is a gateway to an institution's private network. Malicious exploitation of this gateway could have potentially devastating effects on an institution's reputation and business. The penetration testing experiments and security analysis outlined in this paper demonstrate why a financial institution should favour a private cloud implementation over a public cloud implementation.

1.2 Thesis Statement

When migrating to the cloud, large financial institutions should create their own private cloud rather than adopting public cloud solutions due to vulnerabilities in VPN technology.

1.3 Scope

- **Examine the key enabling technologies** for public cloud and how public cloud may be used by a financial institution.
- **Investigate and compare the cloud services** on offer by a number of market-leading cloud vendors e.g. Amazon EC2, and perform a fit-for-purpose analysis of their services for use by a financial institution.
- **Research VPN technology** with emphasis on known vulnerabilities in IPsec implementations.
- **Implement a penetration test suite for cloud-based VPNs** in a virtual environment using freely available software.

- **Use state-of-the-art security stress testing tools** and techniques to demonstrate vulnerabilities in IPsec VPN solutions.
- **Analyse the results** of a number of penetration testing experiments and conclude whether the risks associated with VPN connectivity should deter a financial institution from migrating to the public cloud.

1.4 Significance

The author has worked for eight years in the financial services sector. During this time she has been employed by two global financial services institutions, both of which have yet to embrace cloud technology. Financial services institutions are traditionally quite conservative with respect to adopting state-of-the art technologies [39]. However, these companies are particularly reluctant to migrate their services to the cloud due to recent high-profile security breaches which have compromised sensitive customer data and disrupted services [36] [42] [72]. The purpose of this thesis is to prove that VPN technology, the de facto method of connecting to a company's network over public Internet, is a potential attack vector. The research experiments outlined in this paper demonstrate how vulnerabilities in cloud-based IPsec VPNs can be exploited, and highlight why a financial institution should adopt private instead of public cloud.

1.5 Research Methods

The following section briefly describes the research methods employed in researching material for this paper. Leedy & Ormrod make the point that research methodologies can evolve over time.

> *"The methodology in a qualitative study may continue to evolve over the course of the investigation."* [76]

With this in mind, the author has used a combination of Case Study and Action Research methodologies in her research of the topic, *'VPN Security Considerations for Financial Institutions Migrating to the Cloud'*.

1.5.1 Case Study Research

Case Study Research can be defined as follows:

> *"In a case study a particular individual, program, or event is studied in depth for a defined period of time."* [76]

Recall that the thesis scope includes the following tasks:

- Examine the key enabling technologies for public cloud and how public cloud may be used by a financial institution.
- Investigate the services on offer by a number of market-leading cloud vendors e.g. Amazon EC2, and perform a fit-for-purpose analysis of their services for use by a financial institution.
- Research VPN technology with emphasis on known vulnerabilities in IPsec implementations.
- Use state-of-the-art security stress testing tools and techniques to demonstrate vulnerabilities in IPsec VPN solutions.

The author has performed case studies of historical security breaches or service failures affecting third-party cloud vendors.

1.5.2 Action Research

Action research has been described as '*learning by doing'* [75]. This research methodology has driven the author's practical research of the thesis topic. Leedy & Ormrod explain that

> *"*Action Research f*ocuses on finding a solution to a local problem in a local setting."* [76]

The 'local problem' in this case is how to demonstrate why a financial institution should not adopt public cloud technologies due to vulnerabilities in VPN security.

Recall that the thesis scope includes the following tasks:

- Implement a penetration test suite for cloud-based VPNs in a virtual environment using freely available software.
- Use state-of-the-art security stress testing tools and techniques to demonstrate vulnerabilities in IPsec VPN solutions.
- Analyse the results of a number of penetration testing experiments and conclude whether the risks associated with VPN connectivity should deter a financial institution from migrating to the public cloud.

The information gathered in researching IPsec VPN technology is used to implement a virtual Site-to-Site VPN gateway. This virtual network topology is modelled on that of a popular public cloud service provider. Additionally, free security analysis tools have been researched in creating a penetration testing suite, which is used to expose vulnerabilities in the virtual VPN gateway.

1.6 Thesis Layout

The thesis begins with a review of existing scholarly writings related to cloud security, with emphasis on the distinction between the different cloud deployment models. In Chapter 2 the author defines cloud; describes the key enabling technologies of cloud; summarises the perceived benefits of adopting cloud; and introduces a number of cloud service providers. Also included in this chapter is a summary of Virtual Private Network (VPN) technology, on which the author has based her penetration testing experiments. Chapter 3 focuses on security tools that may be used to exploit vulnerabilities in VPN technology. The technical implementation of the penetration tests is outlined in Chapter 4. Finally, the author's concluding comments and ideas for future work are summarised in Chapter 5.

5 CONCLUSION

5.1 Concluding Comments

The purpose of this research was to demonstrate why a financial institution should create its own private cloud rather than adopting public cloud due to vulnerabilities in VPN technology.

This paper initially set out to investigate the key enabling technologies of cloud, along with a number of popular cloud service providers. The author focused on Amazon VPC as it incorporates the use of VPN technology, the de facto method of sending encrypted packets between two networks over the Internet. IPsec VPN technology was researched with emphasis on known vulnerabilities. The information gathered was then used to create a reusable suite of penetration testing tools using freely available software. For the penetration testing experiments, a simulated Site-to-Site VPN gateway network was created using GNS3. The simulated network topology was designed to mirror the Amazon VPC network topology so that the tests could be applied easily to this real production service in the future.

The experiments outlined in Chapter 4 demonstrate how IPsec VPN technology can be exploited such that connectivity to an organisation's internal network could be compromised. Certain types of VPN configurations, such as IKE in aggressive mode can expose pre-shared keys that could potentially be used to gain access to the data being shared between two IPsec endpoints. On a more practical level, the experiments detail the steps involved in setting up a penetration testing toolkit and a simulated network environment consisting entirely of free software. This research has also shown how simple it is to flood a router device with more traffic than it can handle affecting its ability to perform its job properly. The rate of successful pings to that network device decreased instantly once flood_router6 began flooding the network with router advertisements.

Section 4.5.1.6 describes how cloud service providers (CSPs) like Amazon have taken precautions to mitigate against distributed denial of services (DDoS) attacks. However, Amazon acknowledges that there may be vulnerabilities in the services and openly encourages customers to perform their own penetration testing and security analysis. The suggestion that customers should perform due diligence is testament to the fact that even Amazon cannot guarantee its cloud products to be completely safe 'out of the box'. Historical high-profile security breaches [36] [42] [72] highlight that no such guarantee could or should be made. Figure 3 illustrates how organisational control can vary according to cloud deployment model. This may be acceptable to certain types of companies. However, a financial institution that relies so heavily on reputation and security should consider all vulnerabilities before underwriting such risk. Moreover, it stands to reason that a financial institution can avoid the kind of operational risk introduced by extending its network to public cloud simply by not adopting public cloud.

Even if identifying vulnerabilities in VPN gateway were not enough to deter a financial institution from using public cloud, establishing a reusable suite of penetration testing tools would benefit the organisation in the long-term. This would help baseline VPN security capabilities and identify weaknesses. In addition, use of freely available and easy-to-use security tools, as documented in this paper, is also beneficial since it allows the testing to be performed by any IT professional; not just security experts. The accessibility of these tools serves to improve awareness of these vulnerabilities across the IT organisation.

It is important that financial institutions realise the very real risk of using cloud-based VPNs and take appropriate preventative measures. This research project has served to illustrate the ease at which freely available security tools can compromise IPsec VPN gateways. Choosing private cloud over public cloud removes the need for a VPN and this type of threat is eliminated.

REFERENCES

[1] Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing*. National Institute of Standards and Technology [online] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [last accessed 23 August 2013]

[2] IBM (2013). *NIST's Definition of Cloud Computing.* IBM Developer Works Technical Library [online] https://www.ibm.com/developerworks/mydeveloperworks/blogs/CloudComputing/entry/nist_s_definition_of_cloud_computing_what_is_cloud_computing?lang=en [last accessed 23 August 2013]

[3] Winkler V. (2011) *Securing the Cloud*. Syngress, an imprint of Elsevier, 255 Wyman Street, Waltham, MA. ISBN 978-1-597-49592-9.

[4] Krutz L. & Dean Vines R. (2010). *Cloud Security: a comprehensive guide to secure cloud computing.* Wiley Publishing Inc., Indianapolis IA. ISBN 978-0-470-58987-8.

[5] Jones, M.T (2008). *Cloud computing with Linux*. IBM Developer Works Technical Library [online] http://www.ibm.com/developerworks/linux/library/l-cloud-computing/index.html [last accessed 23 August 2013]

[6] Garfinkel, Simson (1999). Abelson, Hal. ed. *Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT*. MIT Press, Cambridge MA. ISBN 978-0-262-07196-3.

[7] Hurwitz, J. & Kaufman, M. (2011). *Private Cloud for Dummies, IBM Special Edition*. John Wiley & Sons Inc., Hoboken, NJ. ISBN 978-1-118-15263-8.

[8] Boampong, P. & Wahsheh, L. (2012). *Different Facets of Security in the Cloud*. Proceedings of the 15th Communications and Network Simulation Symposium. Society for Computer Simulation International. San Diego, CA. ISBN 978-1-61839-785-0.

[9] Jenson, M. et al (2009). *On Technical Security Issues in Cloud Computing.* 2009 IEEE International Conference on Cloud Computing. ISBN 978-0-7695-3840-2.

[10] Balduzzi, M. et al. (2012). *A Security Analysis of Amazon's Elastic Compute Cloud Service.* ACM New York, NY. ISBN 978-1-4503-0857.

[11] Amazon (n.d.). *Amazon Elastic Compute Cloud.* Amazon [online] http://aws.amazon.com/ec2/ [last accessed 23 August 2013]

[12] IBM, (n.d.). *What is Cloud?* IBM [online] http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html [last accessed 23 August 2013]

[13] IBM, (n.d.b.). *IBM SmartCloud.* IBM [online] http://www.ibm.com/cloud-computing/us/en/index.html [last accessed 23 August 2013]

[14] Maria Spinola (2009) *An Essential Guide to the Possibilities and Risks of Cloud Computing* [online] http://www.mariaspinola.com/whitepapers/An_Essential_Guide_to_Possibilities_and_Risks_of_Cloud_Computing-A_Pragmatic_Effective_and_Hype_Free_Approach_For_Strategic_Enterprise_Decision_Making.pdf [last accessed 23 August 2013]

[16] NIST (2002). *Federal Information Security Management Act of 2002*. NIST [online] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf [last accessed 23 August 2013]

[17] Boughn, J. (2009). *HIPAA Security Rule Conference* [online] http://csrc.nist.gov/news_events/HIPAA-May2009_workshop/presentations/1-051809-keynote.pdf [last accessed 23 August 2013]

[18] Yu, H. et al (2012). *Cloud Computing and Security Challenges*. ACM New York, NY. ISBN 978-1-4503-1203-5.

[19] VMware, (n.d.). *VMware vCloud Suite.* http://www.VMware.com/products/datacenter-virtualization/vcloud-suite/overview.html [last accessed 23 August 2013]

[20] Bacon, J. et al (2010). *Enforcing End-to-End Application Security in the Cloud (Big Ideas Paper).* ACM New York, NY. ISBN 978-3-642-16954-0.

[21] Amrhein, D., Quint, S. (2009). *Cloud Computing for the Enterprise Part 1 - Understanding cloud computing and related technologies* [online] http://www.ibm.com/developerworks/websphere/techjournal/0904_amrhein/0904_amrhein.html [last accessed 23 August 2013]

[22] IBM (2010). *IBM Survey: IT Professionals Predict Mobile and Cloud Technologies Will Dominate Enterprise Computing By 2015* [online] http://www-03.ibm.com/press/us/en/pressrelease/32674.wss [last accessed 23 August 2013]

[23] Turban E., Kyu J., King, D., McKay J., Marshall P. (2008). *Electronic Commerce 2008: A managerial perspective* (5th Ed.). Pearson Prentice Hall. Upper Saddle River, NJ. ISBN 978-0-132-24331-5.

[24] Goth, G (2007). *Virtualization - Old Technology offers huge potential* [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4134016 [last accessed 23 August 2013]

[25] Microsoft (n.d.). *Virtualization & Management* [online] http://www.microsoft.com/en-us/server-cloud/datacenter/virtualization.aspx [last accessed 23 August 2013]

[26] VMware, (n.d.b.). *Virtualization Overview* [online] http://www.VMware.com/virtualization/ [last accessed 23 August 2013]

[27] Gartner (2010). *Gartner Global IT Council for Cloud Services Outlines Rights and Responsibilities for Cloud Computing Services* [online] http://www.gartner.com/newsroom/id/1398913 [last accessed 23 August 2013]

[28] EU Directive 95/46/EC (1995). *The Data Protection Directive* [online] https://www.dataprotection.ie/viewdoc.asp?DocID=89 [last accessed 23 August 2013]

[29] Amazon (n.d.b.). *Amazon Global Infrastructure* [online] http://aws.amazon.com/about-aws/globalinfrastructure/#reglink-eu [last accessed 23 August 2013]

[30] Cloud Security Alliance (2011). *Security Guidance for Critical Areas of Focus in Cloud Computing v3.0* [online] https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf [last accessed 23 August 2013]

[31] IBM, (n.d.c.). IBM SmartCloud. *The cloud enterprises trust* [online] http://www.ibm.com/cloud-computing/ca/en/ [last accessed 23 August 2013]

[32] IBM, (n.d.d.). *Build your private cloud with IBM SmartCloud Foundation* [online] http://www.ibm.com/cloud-computing/ca/en/private-cloud.html [last accessed 23 August 2013]

[33] IBM (2012). *IBM SmartCloud Success Stories* [online] https://www-01.ibm.com/software/success/cssdb.nsf/solutionareaL2VW?OpenView&Count=30&RestrictToCategory=default_SmartCloudSolutions&cty=en_us [last accessed 23 August 2013]

[34] Amazon (n.d.c.). *Amazon Virtual Private Cloud* [online] http://aws.amazon.com/vpc/ [last accessed 23 August 2013]

[35] Amazon (n.d.d.). *Customer Success Powered by AWS Cloud* [online] http://aws.amazon.com/solutions/case-studies/ [last accessed 23 August 2013]

[36] Hutchinson, L (2012). ARS Technica. *Amazon Web Services outage once again shows the reality behind "the cloud"* [online] http://arstechnica.com/information-technology/2012/10/amazon-web-services-outage-once-again-shows-reality-behind-the-cloud/ [last accessed 23rd March 2013]

[37] VMware, (n.d.c.). *Who Are We* [online] http://www.vmware.com/company/ [last accessed 23 August 2013]

[38] VMware, (n.d.d.). *Another VMWare Cloud* [online] http://www.vmware.com/cloud-computing/another-vmware-cloud [last accessed 23 August 2013]

[39] Messmer, E. (2013). *Gartner: Long hard climb to high level of cloud computing security*, Network World [online] http://www.networkworld.com/news/2013/041013-gartner-cloud-security-268587.html?source=NWWNLE_nlt_daily_pm_2013-04-10&goback=.gde_3394596_member_231212944 [last accessed 23 August 2013]

[40] Nolle, T. (2009). SearchCloudComputing, *Network considerations in cloud computing* [online] http://searchcloudcomputing.techtarget.com/tip/Network-considerations-in-cloud-computing [last accessed 23 August 2013]

[41] Bütler, I. (n.d). Compass Security, *VPN Threat Analysis* [online] http://www.csnc.ch/misc/files/publications/VPNThreatAnalysis_CSNC.pdf [last accessed 23 August 2013]

[42] Jackson Higgins, K. (2011). *VPN An Oft-Forgotten Attack Vector* [online] http://www.darkreading.com/end-user/vpn-an-oft-forgotten-attack-vector/232300464 [last accessed 23 August 2013]

[43] Luminita, D.C.C. (2012). Academic World Education & Research Center*, Using penetration testing to discover VPN security vulnerabilities* [online] http://www.world-education-center.org/index.php/P-ITCS/article/viewArticle/685 [last accessed 4 August 2013]

[44] NIST (2001). *Advanced Encryption Standard (AES)* [online] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [last accessed 23 August 2013]

[45] NIST (1999). *Data Encryption Standard (DES)* [online] http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf [last accessed 23 August 2013]

[46] Enders, R. (2012). SearchCloudComputing, *How can incorrectly configuring VPN clients lead to a security breach?* [online] http://searchenterprisewan.techtarget.com/answer/How-can-incorrectly-configuring-VPN-clients-lead-to-a-security-breach [last accessed 23 August 2013]

[47] Parmenter, T. (2011). SearchCloudComputing, *VPN security breaches: How to avoid them* [online] http://searchenterprisewan.techtarget.com/news/2240104696/VPN-security-breaches-How-to-avoid-them [last accessed 23 August 2013]

[48] McClure, S. Scambray, J., Kurtz, G. (2012). *Hacking Exposed ™ 7: Network Security Secrets & Solutions* (7th Ed.). McGraw-Hill Osborne Media. ISBN 978-0-07-178028-5.

[49] Amazon (n.d.e.). *Amazon Virtual Private Cloud FAQs* [online] http://aws.amazon.com/vpc/faqs/ [last accessed 23 August 2013]

[50] NIST (2005). *Guide to IPsec VPNs* [online] http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf [last accessed 23 August 2013]

[51] Saraswathi, S. and Yogesh, P. (2012). *Mitigating Strategy to Shield the VPN Service From DoS Attack* [online] http://airccse.org/journal/ijcis/papers/2212ijcis05.pdf [last accessed 23 August 2013]

[52] Dunn, J. (2012). Tech World, *Attack on airport VPN bypassed multi-factor authentication, security firm reports* [online] http://news.techworld.com/security/3375826/attack-on-airport-vpn-bypassed-multi-factor-authentication-security-firm-reports/ [last accessed 23 August 2013]

[53] Thomas, A. (2012). Linux for You, *IPsec VPN Penetration Testing with Backtrack Tools* [online] http://www.linuxforu.com/2012/01/ipsec-vpn-penetration-testing-backtrack-tools/ [last accessed 23 August 2013]

[54] The Internet Engineering Task Force (1998). *Encapsulating Security Protocol* [online] http://www.ietf.org/rfc/rfc2406.txt [last accessed 23 August 2013]

[55] The Internet Engineering Task Force (1998). *Internet Key Exchange* [online] http://www.ietf.org/rfc/rfc2409.txt [last accessed 23 August 2013]

[56] Kali (n.d.). *Kali Linux* [online] http://www.kali.org/ [last accessed 23 August 2013]

[57] Rapid7 (n.d.). *Metasploit* [online] http://www.rapid7.com/products/metasploit/ [last accessed 23 August 2013]

[58] GNS3 (n.d.).*GNS3* [online] http://www.gns3.net/ [last accessed 23 August 2013]

[59] Wireshark (n.d.). *Wireshark* [online] http://www.wireshark.org/about.html [last accessed 23 August 2013]

[60] Nmap (n.d.). *Nmap* [online] http://nmap.org/ [last accessed 23 August 2013]

[61] Ike Scan (n.d.). *Ike Scan* [online] http://www.nta-monitor.com/tools-resources/security-tools/ike-scan [last accessed 23 August 2013]

[62] Ike Scan (n.d.b.). *Ike Scan User Guide* [online] http://www.nta-monitor.com/wiki/index.php/Ike-scan_User_Guide [last accessed 23 August 2013]

[63] Iron Geek (n.d.). *PSK-Crack* [online] http://www.irongeek.com/i.php?page=backtrack-3-man/psk-crack [last accessed 23 August 2013]

[64] Amazon (2010). *Extend Your IT Infrastructure with Amazon Virtual Private Cloud* [online] http://d36cz9buwru1tt.cloudfront.net/Extend_your_IT_infrastructure_with_Amazon_VPC.pdf [last accessed 23 August 2013]

[65] Amazon (n.d.f.). *What is Amazon VPC?* [online] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Introduction.html [last accessed 23 August 2013]

[66] Genc, M. (2011). *Murat Ahmet Genc's MyCSTubes.com Computer Science Tutorial Videos & Articles* [online] http://www.mycstubes.com/ [last accessed 23 August 2013]

[67] blindhog.net (2007). *Cisco – How To configure an IPSec VPN* [online] http://www.blindhog.net/cisco-how-to-configure-an-ipsec-vpn/ [last accessed 23 August 2013]

[68] ComputerNetworkingNotes.com (n.d.). *How to configure extended access list on router* [online] http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/extended-access-list.html [last accessed 23 August 2013]

[69] Cisco (n.d.). *Configuring IPSec and ISAKMP* [online] http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/ike.html [last accessed 23 August 2013]

[70] Kirsch, C. (2013). Rapid7 Community Forums. *Free Metasploit Penetration Testing Lab In The Cloud* [online] https://community.rapid7.com/community/metasploit/blog/2013/01/08/free-metasploit-penetration-testing-lab-in-the-cloud [last accessed 23 August 2013]

[71] Amazon (2013). *Amazon Web Services: Overview of Security Processes* [online] http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf [last accessed 23 August 2013]

[72] Schectman, J. (2012). Wall Street Journal, *Netflix Amazon Outage Shows 'Any Company Can Fail'* [online] http://blogs.wsj.com/cio/2012/12/27/netflix-amazon-outage-shows-any-company-can-fail/ [last accessed 23 August 2013]

[73] Mitchel, B. (n.d). About.com, *Internet Protocol Tutorial* [online] http://compnetworking.about.com/od/tcpiptutorials/a/ipaddrnotation.htm [last accessed 23 August 2013]

[74] Amazon (n.d.). *Penetration Testing* [online] https://aws.amazon.com/security/penetration-testing/ [last accessed 23 August 2013]

[75] Riley, T. & Moltzen, R. (2011). *Learning by Doing: Action Research to Evaluate Provisions for Gifted and Talented Students.* Education Resources Information Center [online] http://www.eric.ed.gov/PDFS/EJ935468.pdf [last accessed 23 August 2013]

[76] Leedy, P.D. & Ormrod, J.E. (2012). Practical Research: Planning and Design (10th Ed.). Pearson. Upper Saddle River, NJ. ISBN 978-0-132-69324-0.

[77] Mitchel, B. (n.d.b.). *What is a TCP/IP Routing Table?* [online] http://compnetworking.about.com/od/hardwarenetworkgear/f/routing_table.htm [last accessed 23 August 2013]

[78] Govshteyn M. (2010). Secure Cloud Review. *Cloud protection from DDoS attacks only slightly more effective than snake oil* [online] http://securecloudreview.com/2010/12/cloud-protection-from-ddos-attacks-only-slightly-more-effective-than-snake-oil/ [last accessed 23 August 2013]