To Cloud or Not to Cloud: A Study of Trade-offs between In-house and Outsourced Virtual Private Network

Fahad A. Arshad, Gaspar Modelo-Howard, Saurabh Bagchi
School of Electrical and Computer Engineering
Purdue University, West Lafayette, USA
{*faarshad, gmodeloh, sbagchi*}*@purdue.edu*

***Abstract*—The question of whether to migrate IT services to a cloud computing infrastructure arises before most IT decision makers today. To enable secure access to sensitive resources a virtual private network (VPN) is almost a required piece of technology. Setting up and managing a VPN server is a non-trivial task—there are a variety of modes in which VPN can be used (IPSec, SSL/TLS, PPTP), there are a variety of software-only and software-hardware solutions, and each comes with a rich set of configuration options. Therefore, it is a perplexing question to practitioners what option to choose, with an understanding of the performance and the security implications of each choice. In this paper, we consider the various factors that should go into such decision making and exemplify this by choosing among two competitive options for protecting access to IT resources of our NSF center which has a significant number of external (i.e., non-Purdue) users. The two options are an open-source software-only VPN (pfSense) and a commercial appliance, i.e., an integrated hardware-software solution. Further, the first is managed by us while the latter is outsourced to an entity that provides VPN services to multiple consumer organizations, and hence, referred by us as the cloud-based service. We follow up with conducting a post-deployment study of the VPN users which reveals that despite a two-fold reduction in throughput, the cloud-based service is considered satisfactory due to its non-intrusiveness with respect to other network activities and ease of configuration.**

***Keywords*-Virtual Private Network; Security; Configurability; Cloud Computing**

I. Introduction

With increasing complexity of software systems, administrators often find themselves outsourcing services to cloud infrastructures. The decision to outsource a given service typically depends on several factors, including the amount of configuration complexity, the hiring of extra personnel for management and the performance delivered to the users. If there is not enough performance difference between in-house and cloud-based service, the cloud option is preferred as it typically provides cost savings. These cost savings come at a risk of lower security, where the data is shipped to an external provider and thus requires the trustworthiness of the provider. Therefore, before outsourcing any service, a careful experimental study with respect to different dimensions should be conducted. We conduct such a study on Virtual Private Networks (VPNs) deployed as a service separately in an in-house setup and in a cloud-like environment. When critical services are migrated to the cloud, VPN is needed to protect an organization's critical resources when accessed remotely without the requirement of administering the service. In a SAAS-based (software as a service) cloud environment, we conduct a user-based post-deployment survey to understand the success of the deployed service. The VPN service is evaluated in light of the following research questions:

1) Which dimensions (performance, management effort, security) are considered critical when deploying a service to the cloud?
2) What are the important features exported by a service that are also desired by users (system administrators)?

The need for implementing a VPN service arises from a requirement of securing network hosts in any IT organization. To provide security with some minimum level of performance, it is a challenging task to setup a VPN service without any initial measurement-based experiments. This work provides a set of dimensions, i.e., performance, configuration and management to consider when deciding a VPN option. The work presents a study that evaluates two VPN options before a large-scale deployment is conducted. One, a cloud option where an external entity provides the VPN service and two, an in-house option where the service is implemented within the organization. For the cloud option, Cisco ASA 5520 appliance [1] is provided by the external provider while the in-house setup of VPN server is provided by pfSense 1.2.3 [2] running on a dedicated server-class hardware managed by us. The users of the VPN service are system administrators, developers and an IT manager who are part of an IT team called NEEScomm (Network for Earthquake Engineering Community and Communications). This team manages the production IT resources of a platform called NEEShub [3] that has been developed with the support of $120 million from the National Science Foundation (NSF) for providing simulation, experimental, and data facilities to earthquake engineers throughout the U.S.

A VPN solution can be selected from a range of options giving different levels of performance, security, configurability and post-deployment management of the infrastructure.

Table I
FEATURES BY VPN PROTOCOL TYPE

VPN Protocol	Client available in most OSes	Cryptographically secure	Firewall friendly
IPSec	No	Yes	No
SSL/TLS	No	Yes	Yes
PPTP	Yes	No	Mostly

An acceptable VPN performance [4], that provides a user the satisfaction to work productively when they connect to a remote VPN server is an essential requirement. To understand the limits of performance, an end-to-end measurement-based experimental study is conducted using a well-known network testing tool Iperf [5], for each of the VPN options. The results provide a decision criteria to eliminate options that are not feasible from the performance perspective.

Besides performance, security is another dimension to consider for a VPN solution. A solution can provide various security functions, for example, confidentiality, authentication and data-integrity. A combination of these functions implemented at different network layers are provided by standard VPN protocols such as Internet Protocol Security (IPSec), Secure Sockets Layer/Transport Layer Security (SSL/TLS) and Point-to-Point Tunneling Protocol (PPTP). Table I presents some of the features provided by typical VPN protocols.

Another dimension that is often overlooked in practical VPN infrastructures is VPN setup, the ease of configuring a VPN at both the server and the client. In addition to VPN setup, post-deployment management is also critical, e.g., how would the users of a VPN service be added and deleted and whether any migration of current user accounts is required. This is an important aspect as it involves the cost of employing an administrator for VPN management.

The remainder of the paper is organized as follows: Section II covers related work. Section III presents the general architecture for both in-house and cloud-based environments. Section IV covers the requirements of the VPN solution. Section V presents the detailed evaluation of each VPN solution. Section VI details on the post-deployment user-based survey. The conclusion is presented in Section VII.

II. RELATED WORK

Previous work has shown that complexity of VPN configurations, especially for IPSec protocol, is not trivial. To reduce configuration complexity exposed to the user, a configuration compiler Simple-VPN [6] automates VPN configurations based on the minimal configurations provided by the user. Instead of using a compiler, we outsource the management of configurations to an external VPN service provider which provides VPN as a shared service. To share a VPN service among several independent domains, a study [7] proposes a framework where multiple VPN domains can share a common policy with a provision of allowing for each domain to define its own configuration peculiarities. This is similar to the cloud scenario [8] where a given resource is shared.

The control functionalities [9] [10] that a cloud-based service provider allows to its consumers is a critical feature from the perspective of post-deployment reconfigurations. Ideally, a consumer would like to have as much control of its service as available in traditional in-house deployment, but that is not always the case. The main reason for this is due to the "one-size fits-all" nature of the cloud-based service, where there is not always a mechanism to provide differentiated configurations to each consumer for a shared service. In our scenario, the service provider does not export any control functionalities and any reconfigurations are done when a request is made by the service consumer.

VPN is commercially available both as an appliance [11] (hardware-cum-software) and as a software (CipherGraph [12] and Comsenso [13]). In this work, we experiment with the VPN service for both of these options.

III. VPN ARCHITECTURE

The network architecture for the in-house implementation of VPN service follows a typical client-server model (Figure 1), where a remote VPN client forms a connection by setting up a VPN tunnel to a VPN server through the public internet. On a successful VPN connection, the client becomes part of the organization's private network and can use network resources, such as, storage, printers, database, etc. For the in-house VPN set-up we deploy pfSense, an open-source distribution that provides commercial-level security and networking software. For cloud-based VPN, the external cloud-based service provider called HUBzero employs a Cisco-based appliance ASA-5520. The architecture of cloud-based implementation where the VPN service is shared among several VPN consumers is shown in Figure 2. Here the external service provider, an independent administrative domain, provides the VPN service as a shared service between four consumers; consumer A, consumer B, NEEShub Infrastructure and consumer C. Consumer C is HUBzero's internal users, while the rest of the consumers are external consumers (from HUBzero perspective).

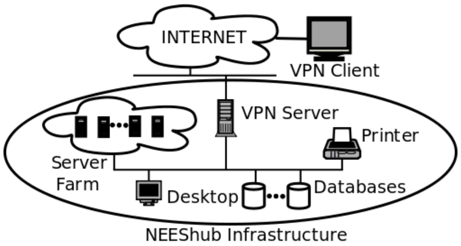

Figure 1. Network architecture for in-house implementation

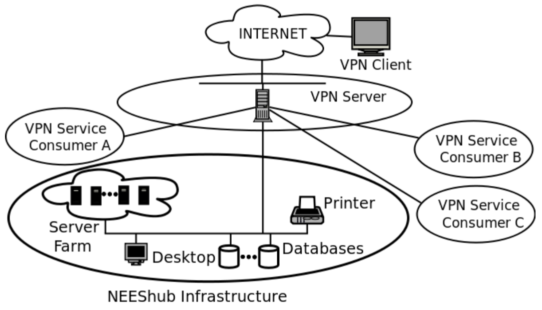

Figure 2. Network architecture for cloud-based implementation

IV. VPN Requirements

The requirements that were stated by the administrators at NEEScomm are listed as follows:

- The users of the VPN service should not experience poor connection speed while accessing their resources.
- The network resources should be secure and protected from the outside world.
- The VPN solution should implement simple management of VPN users. Adding and deleting VPN users to access internal resources should be easy to manage.
- At the client's end, the VPN service should be easily configurable (user-friendly).
- The VPN client software should be available for all major platforms, chiefly, Linux, Mac and Windows.

V. Analysis of VPN Solutions

The two alternatives considered at NEEScomm were Cisco ASA 5520 [1] appliance and pfSense 1.2.3 [2]. Cisco's solution comprises of hardware-cum-software solution with its configuration coordinated by HUBzero [14]. Configuring pfSense, an open source VPN solution, does not require any dependency on HUBzero, though it involves the extra labor to configure a VPN server on off-the-shelf hardware.

A. VPN Performance Experiments

An end-to-end measurement experiment, where a client sets up a VPN tunnel to the VPN gateway and communicates to an end-host on the private network is conducted. The metrics for network performance comparison are network throughput and jitter (statistical variance of packet inter-arrival time). The results are shown in Table II. These metrics are measured using iperf [5]. Iperf is used in TCP mode to test data throughput and in UDP mode to test network jitter.

For each experiment, the memory usage and CPU consumption are measured at both client and server hosts. All the experiments are conducted across the three protocols offered by pfSense (IPSec, SSL/TLS and PPTP) and the one protocol (IPSec) implemented in Cisco's product. All the results are averaged across 5 runs, each running for 300 seconds. For statistical significance, 95% confidence intervals are presented for all measurements.

Table II
Network Throughput, Client and Server Memory and CPU Measurements

Solution	Protocol	Network Throughput (Mbits/sec)	Client Memory (kB)	Server Memory (kB)	Client CPU (%)	Server CPU (%)
pfSense	IPSec	143.2±1.4	1241.6±1.8	1252.8±0.1	19.2±4.9	2.1±0.1
	SSL/TLS	169±7.4	1035.1±1.4	1251.2±0.3	1.1±0.5	3.9±0.3
	PPTP	61.7±3.7	1240.8±28.4	1248.8±0.4	0.4±0.3	3.3±0.4
Cisco	IPSec	73.3±2.1	1283.2±39.1	1308.0±4.3	5.1±3.2	8.9±4.3

B. Results

1) Network Throughput: The solution based on pfSense achieves a significantly better (2x) end-to-end throughput for at-least two protocols, IPSec (143 Mbps) and SSL/TLS (169 Mbps) (Table II), while Cisco's solution which implements only IPSec, achieves 73 Mbps. Further, when comparing across protocols, SSL/TLS, due to its use of UDP (default mode) for transport layer, performs the best (169 Mbps). All iperf clients have similar memory consumption, except for SSL/TLS, which has lower memory consumption due to TCP (iperf flow control) over UDP (SSL/TLS) tunnel. Here TCP over UDP means that after VPN tunnel which uses UDP as transport layer protocol in SSL/TLS has been setup, iperf-client then sets-up a TCP connection with iperf-server. TCP over UDP throttles the rate of packets and therefore, the client resource consumption is less. The iperf-server memory is similar for all pfSense versions since the iperf server's main job is to only sink the received packets. The CPU usage trend is different on the iperf-server side as the decryption of IPSec traffic is done at the VPN gateway as opposed to the end host (iperf-server) and therefore does not show up in these results.

2) Jitter: The network jitter and packet loss results are shown in Table III. The maximum jitter (0.35ms) experienced with Cisco-5520 is within 0.5ms, a typical service level agreement (SLA) value [15] for backbone ISPs. pfSense (IPSec) experiences significantly high (19%) packet loss. A reason for this high packet loss is the absence of flow control (UDP mode), where an iperf-client sends data at a high rate (seen by 63% iperf-client CPU usage), but the iperf-server or the VPN gateway is unable to handle all incoming packets. A similarly high packet loss (55.5%) is seen for SSL/TLS. The low packet loss values along with acceptable jitter for Cisco-5520 are a positive, but that is at the cost of a lower throughput.

C. VPN Client Configurability

The ease of configuring a VPN client to operate with a given VPN protocol (IPSec, PPTP, SSL/TLS) and a vendor (Cisco, pfSense) on a particular operating system (Windows, Mac, Linux) is evaluated in this section. A summary of VPN

Table III
NETWORK JITTER, PACKET LOSS, CLIENT AND SERVER MEMORY AND CPU MEASUREMENTS

Solution	Protocol	Network Jitter (msec)	Packet Loss (%)	Client Memory (kB)	Server Memory (kB)	Client CPU (%)	Server CPU (%)
pfSense	IPSec	0.131±0.075	19±1.1	1301.5±2.0	1207.6±532.0	63.4±5.0	1.0±0.5
	SSL/TLS	0.027±0.005	55.5±0.4	1085.8±425.8	911.3±647.5	5.2±5.0	1.1±0.4
	PPTP	0.032±0.0	0.0±0.0	1301.5±2.2	1506.8±35.2	32.3±6.4	2.3±0.3
Cisco	IPSec	0.352±0.096	0.001±0.0007	1341.5±2.11	1242.7±4.4	6.4±0.5	6.3±1.1

Table IV
CLIENT CONFIGURABILITY BY OS TYPE FOR CISCO ASA 5520

VPN Client	OS type	OS version	Complexity of Configuration
Cisco VPN client (5.0.07.0440)	Windows	Windows 7, Windows Server 2008	LOW
Cisco VPN client (4.9.01.0100)	Mac	Mac OS X (10.6.8)	LOW
vpnc client (0.5.1)	Linux	Debian 5.0, Ubuntu 10.04	MEDIUM

Table V
CLIENT CONFIGURABILITY BY OS TYPE FOR PFSENSE 1.2.3

Protocol	VPN Client	OS type	OS version	Complexity of Configuration
IPSec	Shrew Soft client	Windows	Windows 7	MEDIUM
	Shrew Soft client	Linux	Ubuntu 10.04, Debian 5.0	MEDIUM
PPTP	In-built	Windows	Windows 7, Windows Server 2008, Windows XP	LOW
	pptp-linux	Linux	Debian 5.0	MEDIUM
	pptp-linux	Mac	Mac OS X (10.6.8)	LOW
SSL/TLS	openvpn	Windows	Windows 7, Windows server 2008	HIGH
	openvpn	Linux	Debian 5.0, Ubuntu 10.04	HIGH

clients tested by the operating system type for both solutions is given in Table IV and Table V. The complexity of the configuration column is a qualitative measure, i.e., “LOW” represents a simple GUI based configuration where the user enters minimal configurations. “MEDIUM” represents the client is either command-line based or requires several tabs to be configured in the GUI. “HIGH” represents a requirement of several command-line or file-based configurations and transfer of files between client and server. The general configuration of Cisco’s VPN client is straightforward as opposed to pfSense (Table V).

D. VPN User Management

To authenticate a user at NEEShub, an LDAP (Lightweight Directory Access Protocol) server is currently employed. To integrate VPN access to current infrastructure, a VPN user is required to authenticate against the LDAP server. Cisco’s solution supports the LDAP integration, while pfSense provides no native support for authenticating users against an LDAP server. In pfSense, PPTP and IPSec maintain an in-built database for user management, and therefore a username is required to be added for each new user. SSL/TLS requires even more configuration steps, where keys/certificates are generated using a script at the server for each new user. These keys/certificates need to be securely transferred to the client in order for it to authenticate against the SSL/TLS server. A summarized comparison of the studied dimensions for the two solutions is presented in Table VII.

VI. POST-DEPLOYMENT STUDY

The cloud-based option provides a reasonable throughput (at-least 73 Mbps) with low management costs and therefore it was chosen as the final VPN service to be used in production. With the VPN service in use for nine months (Oct 2011-Jun 2012), we conducted a survey among the users of the VPN service to answer three questions:

- What is the quality of the service delivered by NEEScomm VPN?
- Whether the VPN service affects other services running on the user’s local machine?
- Are there any improvements or new features that can help improve the productivity of users?

A. Threats to Validity

All survey based studies are valid under certain assumptions. In this survey, we assume that the users are technologically savvy and hence the responses are accurate. We make this assumption as a majority (75%) of the users are NEEScomm IT employees working in roles that include system administrators, developers and IT managers. Further, the number of participants, 12/28 (43%) might be viewed as a low percentage. Given the scale of the organization (greater than 10 employees), we argue that the response rate is enough to bring out useful insights.

B. User Environment Statistics

Among the 12 respondents, the majority (42%) were Microsoft Windows and Mac (42%) users followed by Linux (17%)(Table VI). It was observed that 92% of users have a home internet connection that supports up-to a maximum of 20 Mbps. This observation implies that a given user would experience the same throughput with both VPN options (Cisco or pfSense), as both options provide a throughput of greater than 20 Mbps (Section V-B).

C. What is the quality of service delivered by NEEScomm VPN?

To answer this question, we asked NEEScomm VPN users to respond to the following two statements on a Likert-scale [16] (Strongly Disagree=1 to Strongly Agree=5).

1) *Every time, I connect to NEEScomm VPN, the connection is successful without any connection problem.*
2) *When using NEEScomm VPN, most of the time my connection drops and I have to RECONNECT again and again.*

Table VI
USERS' SYSTEM CONFIGURATION AND VPN USAGE

Operating System	Windows 5 (42%)	Mac 5 (42%)	Linux 2 (17%)	–	–
Type of User	System admin, Developer, Manager 9 (75%)	Regular user 3 (25%)	–	–	–
Internet Connection Speed	<= 500kbps DSL or Cable 2 (17%)	<= 1Mbps DSL/Cable 3 (25%)	<= 10Mbps 3 (25%)	<= 20Mbps 3 (25%)	<= 100Mbps 1 (8%)
Times a user connects to VPN	once every 3 to 6 months 2 (17%)	once every 1 to 3 months 3 (25%)	2 to 3 times per month 1 (8%)	once every week 1 (8%)	2 to 6 times per week 5 (42%)
Time spent per VPN session	less than 5 minutes 3 (25%)	less than 30 minutes 1 (8%)	more than 30 minutes 8 (67%)	–	–

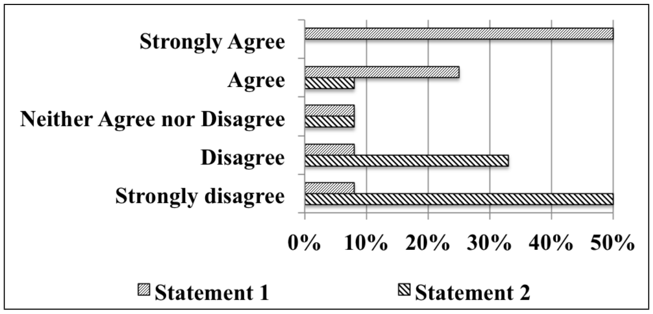

Figure 3. NEEScomm VPN Quality as Perceived by Users

The responses to the above two statements (Figure 3) measure the NEEScomm VPN quality from the user's perspective. The responses to the first statement has a mean Likert-score of 4.0 (std. dev. = 1.35), thus validating that the VPN connection set-up phase is successful without retries. The responses to the second statement measure the post-connection experience where a mean Likert-score of 1.75 (std. dev. = 0.97) implies that users find their VPN connections to be relatively stable.

D. Whether the VPN service affects other services running on the user's local machine?

To answer this question, we asked NEEScomm VPN users to respond to the following three statements.

3) *After connecting to NEEScomm VPN, my machine often gets SLOW and UNRESPONSIVE.*
4) *My experience of using local applications (MS Office, games, etc.) on my home machine is significantly POOR while I am connected to NEEScomm VPN.*
5) *After connecting to NEEScomm VPN, my web browsing and network-related application experience is SIGNIFICANTLY AFFECTED.*

The responses (Figure 4) to statement no. 3 above had a mean Likert-score of 1.83 (std. dev. = 0.94) (lower is better) implying that users agreed that their local machine was not slow or unresponsive when connected to NEEScomm VPN. Also, users agreed that their local applications were not significantly affected (mean Likert-score=1.83) by NEEScomm VPN with even a lesser standard deviation of 0.72 compared to the previous statement. Further, the statement no. 5, that measured whether any network related applications were possibly affected from connecting to NEEScomm VPN had a mean score of 2.0 (lower is better) (std. dev. = 0.95) validating that NEEScomm VPN did not significantly affect the local host.

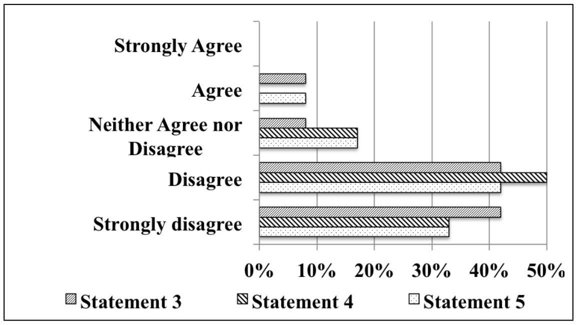

Figure 4. Local Host Degradation by NEEScomm VPN as Perceived by Users

E. Are there any improvements or new features that can help improve the productivity of users?

To answer this question, we asked users of NEEScomm VPN the question: *Which NEEScomm VPN properties would they consider essential for their job*. The answers (multiple choices allowed) depicted in Figure 5 show the essential requirement of user-friendly VPN client-installation by 83% of the users, who responded to this question. Further 75% of users wanted a higher VPN throughput. Another related question (multiple choices allowed) in the survey was: *Which additional VPN features would you wish for?* 88% of users wanted a support for a client for Apple iOS (iPhone, iPad) while 25% wanted a client for Android OS. Additionally 63% wanted seamless roaming (when connecting through mobile networks).

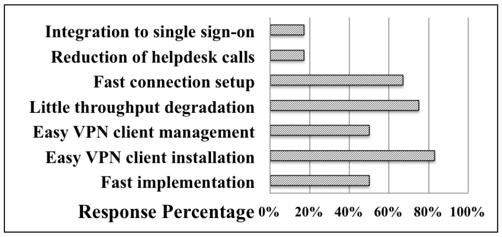

Figure 5. Features that can increase user productivity

Table VII
COMPARISON OF CISCO ASA 5520 AND PFSENSE 1.2.3

	Cisco ASA 5520	pfSense 1.2.3	pfSense 1.2.3
Protocol	IPSec	IPSec	SSL/TLS
Performance	73 Mbps	143 Mbps	169 Mbps
Client configurability	Windows, Mac OS X, Linux	Windows, Linux	Windows, Linux
External Authentication	Supports LDAP	No support for LDAP	No support for LDAP
VPN user Management	LOW	HIGH	HIGH
VPN setup and configuration	LOW	MEDIUM	HIGH

The above answers lead us to see two important trends that administrators are beginning to adopt. First, they are shifting towards accessing their work resources from their portable handheld devices. Second, they prefer client software that requires lesser and preferably automatic configuration management.

VII. CONCLUSION

This work has evaluated VPN performance, user management and client configurability for the solutions offered by Cisco ASA 5520 and pfSense 1.2.3 in cloud-based and in-house environments respectively. In-house pfSense solution outperforms cloud-based Cisco solution with respect to performance. The experiments in this work have shown that cloud-based Cisco's solution can still give a throughput around 73 Mbps, which is sufficient for connecting from the home internet (greater than 50 Mbps raw bandwidth for home internet connection is rare as shown by a 2010 survey [17]).

Besides performance, the cloud-based Cisco appliance has easier client configurability and compatibility for all (Windows, Mac, Linux) operating systems with a minimal amount of configuration needed, whereas the in-house pfSense VPN server has non-trivial client-side configurability for Mac OS X. Further, Cisco's solution integrates support for LDAP authentication, which is already used at NEEShub for its services.

A post-deployment survey revealed the success of outsourced NEEScomm VPN service verifying that users of the service are able to connect to the VPN service without any significant problems. Also users do not experience any significant slowdown to their local machines when connected to the service.

ACKNOWLEDGMENTS

We would like to acknowledge the contributions of some other members of our NEEScomm IT team - Brian Rohler and Dawn Weisman for help with the NEES IT infrastructure, and of HUBzero team members - Craig Van Tassle and Pascal Meunier - for deployment of VPN on the Cisco appliance.

REFERENCES

[1] "Cisco ASA 5520 appliance." [Online]. Available: http://www.cisco.com/en/US/products/ps6120/index.html

[2] "pfSense." [Online]. Available: http://www.pfsense.org/

[3] "Network for Earthquake Engineering Simulation NEEShub." [Online]. Available: http://www.nees.org/

[4] S. Narayan, K. Brooking, and S. de Vere, "Network performance analysis of vpn protocols: An empirical comparison on different operating systems," in *Proceedings of the 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 01*, ser. NSWCTC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 645–648.

[5] "Iperf, a tool for network testing." [Online]. Available: http://iperf.sourceforge.net/

[6] S. Srivatsan, M. Johnson, and S. M. Bellovin, "Simple-VPN: Simple IPsec configuration," Department of Computer Science, Columbia University, Tech. Rep. CUCS-020-10, July 2010. [Online]. Available: https://mice.cs.columbia.edu/getTechreport.php?techreportID=1433

[7] S. Ioannidis, S. Bellovin, J. Ioannidis, A. Keromytis, and J. Smith, "Design and implementation of virtual private services," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on*, june 2003, pp. 269 – 274.

[8] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[9] H. C. Lim, S. Babu, J. S. Chase, and S. S. Parekh, "Automated control in cloud computing: challenges and opportunities," in *Proceedings of the 1st workshop on Automated control for datacenters and clouds*, ser. ACDC '09. New York, NY, USA: ACM, 2009, pp. 13–18.

[10] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 85–90.

[11] "Barracuda SSL VPN." [Online]. Available: https://www.barracudanetworks.com/ns/products/sslvpn_overview.php

[12] "Secure Cloud VPN (SaaS)." [Online]. Available: http://www.ciphergraph.com/

[13] "Secure Remote Access." [Online]. Available: http://www.comsenso.com/secure-remote-access/

[14] "HUBzero." [Online]. Available: http://hubzero.org/

[15] "Jitter-SLA." [Online]. Available: http://www.voip-info.org/wiki/view/QoS

[16] R. Likert, "A technique for the measurement of attitudes." *Archives of psychology*, 1932.

[17] "2010 Report on Internet Speeds in All 50 States." [Online]. Available: http://www.speedmatters.org/2010report?nocdn=1