Analysis of Different Features and the Application of Cisco's SecureX Architecture in Secure Environment

Ammar Yassir & Smitha Nayak,

Department of Computing, Muscat College, Sultanate of Oman

ABSTRACT—Security incidents are rising at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center operators, network administrators and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today.

In this study, we try to explore the concept of "Future of Network Security" in a holistic context. The main focus of the research is on "Network Security" and its relation with cloud computing. The research also analyzes many aspects of network security and tries to gauge its effect on "Cisco, SecureX and Security architecture. Finally, the research describes various factors which are responsible for "Network Security" and tries to describe the overall effect of network security on Cisco, SecureX and Security architecture.

Keywords: Security, Network Security, cloud computing, SecureX, Security architecture.

I. INTRODUCTION

Network security has become more important to personal computer users, organizations and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. Network security is a complicated subject, historically only tackled by well-trained and experienced experts.

In an increasingly mobile, borderless world, this construct is becoming significantly less relevant. To address new network and security dynamics, new security architectures need to be much more sophisticated. We need a sophisticated policy language that can be expressed in terms of who, what, where, when, and how. Security needs to be separated from the physical infrastructure underneath it. And it needs to be highly distributed so it can be deployed globally and can be available wherever and whenever the borderless enterprise touches the public Internet.

Cisco has developed a bold new architecture to meet the needs of borderless networks, allowing organizations large and small to collaborate easily and their new workforce to roam freely, with confidence (Midkiff, 2008).

This architecture allows for more effective, higher-level policy creation and enforcement. Since it uses a broad array of parameters for policy, it allows for much more effective security and enables situational awareness. Instead of a great many complex firewall rules, security policy can now be based on context, such as "the VP of sales can access the global sales forecast, but if she is seeking access through a Smartphone in China using a strange protocol, and meanwhile she already authenticated herself through the main campus in California two hours ago, this connection is invalid" (Spainhower et al, 2008).

Problem Statement:

This sort of intelligent policy enforcement uses next-generation scanning elements that are meshed into the new Cisco SecureX Architecture.

The Cisco SecureX Architecture is a context-aware, network-centric approach to security that enables: Greater alignment of security policies with business needs integrated global intelligence, Simplified security delivery & Consistent security enforcement throughout the organization.

The result is automated security enforcement from the end point to the cloud that is seamless to the end user and more efficient for the IT organization. Within this new architecture the next-generation end point is able to automatically find the nearest scanning element somewhere in the virtual security fabric and to make a seamless connection. Systems security is an important issue that has received considerable attention as a result of the increasing number of attacks on information systems. Despite the importance of this issue, very little empirical research is available for promoting understanding on the hacking behaviour and the effectiveness of deterrence measures in discouraging hacking. The behavior of a hacker halfway around the world is noted that information is shared and traffic from the hacker's servers is blocked because your network now knows that it comes from someone that it cannot trust. Policy is centrally managed but intelligence is gathered globally, with highly distributed enforcement (Garcia-Luna-Aceves, 2005).

Purpose:

The purpose of the proposed research will be to analyze the future aspects of network security.

The main focus of the research is on "Network Security" and its relation with cloud computing. The research also analyses many aspects of network security and tries to gauge its effect on "Cisco, SecureX and Security architecture.

Manuscript received September 5, 2012
Manuscript revised September 20, 2012

II. AIMS AND OBJECTIVES

• Exploring the concept of "Future of Network Security" in a holistic context.
• Understanding "Network Security" and illustrating its relation with cloud computing.
• Explaining many aspects of network security and identifying its effect on "Cisco, SecureX and Security architecture.
• Analyzing various factors which are responsible for "Network Security".

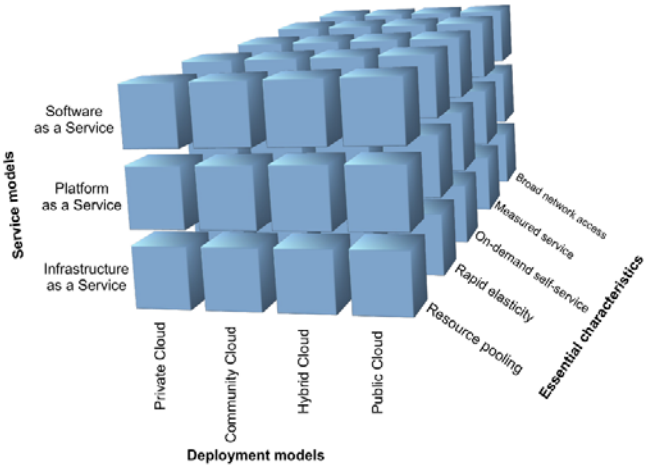
III. SIGNIFICANCE

Computers do not use the chain to negotiate together. They do not lead the discussion, as people - they exchange small packets of data. These packets can contain a variety of data: e-mail messages, compressed graphic images, video and audio, telephone conversations on the Web.
In order to facilitate the transfer computers divide large files into packets. (Think for yourself that the letter of 10 pages was sent to 10 different parts of the envelopes. Recipient opens the message and restores all the original form of writing. With all of this packages should arrive in sequence, the order of the respective pages and come to one destination and the same way) (Spainhower et al, 2008).
These packets are sent through a network of routes. There are different protocols - Ethernet, TCP and the rest - but the basic principles of their operation are similar. Router forwards packets to the specified addresses in them. They may not know the exact location of the recipient but they have some idea of which direction to send the packet. This is somewhat recalls the postal system.
The postman comes to your house confiscate all outgoing mail and delivers it to your local post office. There might not know where the house on 173 Pitter-patter Lane Fingerbon, Idaho, in which resides Mr. X but has information that an envelope together with the rest of the correspondence should be lowered in car which travels to the airport. Employees also address the airport are not aware of where he lives Mr. X but know that they need to send a letter by plane to Chicago.
In the Chicago airport post office know that they have to pass a letter to a flight to Boise. In the town of Boise post office know that the letter be delivered to the train that goes to Fingerbon. And finally, post Fingerbona have accurate information, the address where indicated and the postman delivered the letter (Milanovic et al, 2004).

IV. LITERATURE REVIEW

Most of the security solutions being deployed were developed at time when the enterprise network was relatively static. Users would come in to work and sit at a desk to use a PC that rarely moved because it was connected by a wire to a port in the wall.
The PC had a controlled set of software—the "corporate image"—that included security scanning and configuration. This corporate endpoint was one of the primary places that security was enforced.
Today, that endpoint has burst into thousands of pieces. The rapid pace of innovation in endpoint technology has created wave after wave of consumer devices that are flooding in to the enterprise whether we like it or not. New users sometimes known as "millenials" are demanding the right to use devices of their choice and to blend their personal and professional lives on endpoints that are often as much an accessory as a work tool.
According to recent surveys two-thirds of these new additions to the workforce, when forced to choose, will select a lower-paying job that provides flexibility for how and where they do their job and what devices they can use.
At Cisco, our internal IT team saw this trend and implemented an "any device" policy that allows users the choice of mobile phone, desktops or laptops and even choice of operating system. After two years of "any device" we have found not only end-user satisfaction has increased but also that the cost to serve our end user population has been dramatically reduced. This combination of lower cost and greater end-user satisfaction has helped drive widespread interest in an "any device" policy across the industry (Malekzadeh et al, 2005). Furthermore, as businesses enter into increasingly complex relationships with contractors, partners, suppliers and customers, the clear line between employees and "not employees" has also dissolved. At many companies, the number of partners, contractors and non-traditional employees that need to access corporate assets often exceeds the number of employees that need access. These trends have led most IT strategists to realize that we can longer depend on a controlled configuration at the endpoint.
Web was designed as an equal network: anyone can "move" on him by the usual connection with another PC.
The system signal outside the band must be managed centrally, as the phone system. Will be available endpoints and domestic routes, and they will be different. This system has nothing to do with the current Web (Wang, 2005).
Cloud computing is utility computing or grid computing, or software-as-service or managed service. Roughly, it describes highly scalable computing resources provided as an external service via the internet on a pay-as-you-go basis.
Economically, the main appeal of cloud computing is that customers only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location via the internet. There's no need to worry about how things are being maintained behind the scenes – you simply purchase the IT service you require as you would any other utility. Because of this, cloud computing has also been called utility computing, or 'IT on demand'

I really like the new Cloud Computing definition from the US's National Institute of Standards and Technology (NIST) for the most part. They define three service models, five essential characteristics, and four deployment models. I have represented their model on a cube, as below:



Only NIST's "Hybrid Cloud" encapsulates the full vision of what I believe Cloud Computing is about (interoperability etc). Therefore I would change the NIST deployment models as follows:

- **Private Compute Utility:** An infrastructure physically dedicated to one organization.
- **Private Community Cloud:** An infrastructure spanning multiple administrative domains that is physically dedicated to a specific community with shared concerns.
- **Public Cloud:** An infrastructure spanning multiple administrative domains that is made available to the general public / businesses, without physical partitioning of resource allocations. (There is arguably only one public Cloud – hence the phrase "host it in The Cloud".)
- **Hybrid Cloud:** A combination of public and private compute utilities in order to allow "cloud bursting" for some requirements, or to allow a private compute utility owner to sell their spare capacity into The Cloud.

The emergence of cloud computing provides many opportunities for academia, the information technology (IT) industry and the global economy as an information technology revolution. Compared to other distributed computing paradigms such as Grid computing and High Performance Computing (HPC), cloud computing provides broader inter-operability over the world-wide web networks. As IT industry leaders such as Google, IBM and Amazon are striving to promote this innovative computing paradigm, it is reasonable to expect that cloud computing will bring profound changes to every aspect of the IT industry and to various sectors of the economy. But the opposite is not true. Of all these concepts, more familiar to the user takes one or several principles, but with their own dynamics there is to know understanding. In addition to being influenced by these technologies as well as trends toward virtualization, automation, massively parallel processing and service orientation, cloud computing is emerging as a result of expectations created by Web 2.0 among users (Yan, 2010). Recently, Steve Mills, senior vice president and chief executive of the software unit of IBM, Network World noted the role of the new model for the excitement with which people are receiving capabilities and Web 2.0 mashup.

The idea that an application does not exist in a particular place, but can be composed of multiple pieces from multiple sites is owed to the Web 2.0 (Lehal, 2011).

The vision of online access to its computer applications being substituted for the local access is now becoming a reality for all categories of users. In recent years, there has been a gradual shift towards the use of Rich Internet Application (RIA) at the expense of traditional applications to install on their PC. This technological evolution, called Software as a Service (SaaS) is only one facet of a much larger reality, the Cloud computing (Carthy & Kechadi, 2011).

V. RESEARCH METHODOLOGY

This section mainly focuses on designing a comprehensive methodology in resemblance of proposed research study. Though, research is undertaken to get findings about a topic by taking into consideration some facts, experiences, concepts, hypotheses, principles and laws. A well designed research defines the problem clearly, takes on proper technique, discourses objective evidence, argues logically and provides valuable inferences which provides the researcher with practical insight of complete study.

The case study technique is very much popular among the methods used in designing the qualitative study. According to Yin (2004), the case study refers to "an empirical inquiry that investigates a contemporary phenomenon within its real life-context." Therefore, case study uses all possible sources to investigate organisations, individuals, groups, or events (Yin, 2009) but in systematic manner. In this context the methods which are usually in case study are interviews documentary analysis and taking field notes (Adleman, Jenkins & Kennis, 1976).

V.1 DATA COLLECTION TECHNIQUES

In fact, without the contribution of secondary research no research can be conducted as literature review is the most important part of research that is added to the every form of research which is totally based on already conducted researches.This shows the actual importance of secondary

research. Similarly, in this research, literature was reviewed in the second chapter. However, the research may also be conducted completely depended on secondary research but in the proposed research secondary research only contributed to the section of literature review.

Qualitative research will be used for proposed study. Qualitative research is more subjective as compared to quantitative research and uses very different methods of collecting information which could be both primary and secondary. As already mentioned, this study will choose the secondary method.

The theme of this type of research will be investigative along with open-ended. This type of research is often less expensive than outlines and is extremely effective by acquiring information. It is often the method of choice in the examples where quantitative measurement is not required.

The criteria of selection for the literature will be relevance to the research topic and the year of publication. Both public and private libraries as well as online libraries will be visited to access the data.

There were different resources used in terms of collecting secondary data. In this regard, the required data was gathered from books, peer-reviewed articles and magazines. Moreover, online databases including IEEE, Science Direct, Inter science Wiley, JSTOR, SSRN, SAGE Online Google Books and other printed books etc. were accessed for the sake of more reliable data.

V.2 Scope & Limitations

References the scope of this proposed research will be based on the reflection of the application and different features associated to Cisco's SecureX architecture. SecureX offers something for everyone ... such as a simpler, yet richer, management model for SecOps, deeper levels of security for users within and outside the corporate network, centralized policy creation that extends beyond the corporate firewall, and increased protections for users as they utilize mobile endpoints to access corporate and cloud-based applications. IT business leaders should be pleased with better protections and compliance tools, especially as their vulnerabilities increase with mobile endpoints seeking network access growing.

The main limitation to the study was the case study that will be designed under qualitative mood which always contains the issue of generalizability as many of the scholar have said that qualitative study cannot be generalize directly, though, the different aspects gained during the process of research can be generalized separately to the other components of external world. But the results or conclusions of research study cannot be generalized as done in quantitative form of research. Another limitation to the study is the time constraint as limited number of public and private libraries are visited.

V.3 Procedure

Though, case study is not a standard package of methodology, usually used in most of the researches. However, it also involves some advantage and disadvantages, too, as found in other methods of research design. Regarding the nature of data, only scholarly work was accumulated which could be quoted easily.

V.4 Assumptions

Though, the study was designed on primary research, it involves secondary research, too as practised in every kind of research. In fact without the contribution of secondary research no research can be conducted as literature review is the most important part of research that is added to the every form of research which is totally based on already conducted researches. This shows the actual importance of secondary research. However, the research may also be conducted completely depended on secondary research but in the proposed research secondary research only contributed to the section of literature review.

VI. Preliminary Results & Discussion

The results suggest that the Cisco SecureX Architecture is smart. It knows what application is being used or what specific site is being accessed. It is also expected that the Cisco SecureX Architecture knows where in the world a user is tapping into the network, what time of day it is, how the secure network is being accessed (iPod, smartphone, desktop PC or any other device) whether or not that device has been compromised and what role that user plays in the organization.

The Cisco SecureX Architecture protects the evolving network with security and policy that spans from the mobile user to the virtualized data center and the cloud. Policies are enhanced in real time as the network shares dynamic intelligence on both the local and global level.

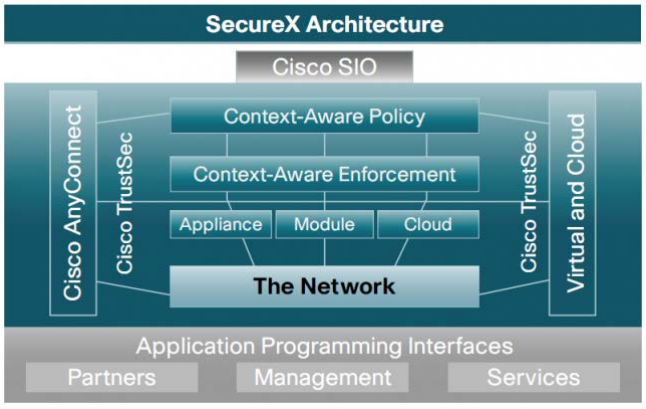


Figure 1. Secure Architecture

Additionally it may be expected from the results that the vision of online access to its computer applications being substituted for the local access is now becoming a reality for all categories of users. In recent years there has been a gradual shift towards the use of Rich Internet Application (RIA) at the expense of traditional applications to install on their PC. This technological evolution called Software as a Service (SaaS) is only one facet of a much larger reality, the Cloud computing (Carthy & Kechadi, 2011).

Today's ultra-modern generation has successfully embraced the "Software as a Service (SaaS)" for custom rich internet application development. SaaS Application Development is an on-demand information technology trend, which has become a huge player in the industry. This is the next generation of software implementation models enable "on-demand software" to work as a service that can be managed by a vendor individually.

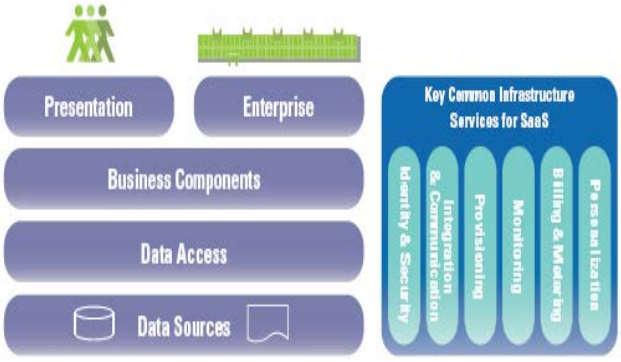


Figure 2: SaaS Architecture

Figure 2 shows a conceptual diagram of this more comprehensive architecture. Moreover, the deployment of SaaS and Cloud Computing technologies plays a major role in minimizing hefty expenditure on dedicated hardware and software.

Long-Range Consequences:

To address the new dynamics of networking and security, new security structures have to be much more sophisticated. We need a policy language that can be expressed in terms of who, what, where, when and how.

Security should be separate from the physical infrastructure that exists beneath it. And it must be so arranged that easily can be implemented globally and may be available where and when the company without borders touches the public internet.

The Cisco SecureX security framework allows you to establish and enforce security policies across the entire distributed network not just at a single point in the data stream. By leveraging using global and local security intelligence for dynamic, real-time threat protection, Cisco SecureX responds to the evolving security needs of today's borderless network environments. More specifically, Cisco SecureX:

- Establishes and enforces context-aware policy across your entire distributed network
- Creates a converged security strategy across your wired, wireless, and VPN networks
- Gives you the ability to create policies that correlate directly with IT enforcement needs and business rules

SecureX Cisco has developed a bold new architecture to meet the needs of borderless networks, enabling organizations large and small companies to collaborate easily and his new work force to move freely with confidence. This architecture allows security policies to a level higher than consider a wide range of parameters in your application. Provides a more effective security-sensitive context of the situation in which there is access to the network.

VII. CONCLUSION

The Cisco SecureX Architecture is a next-generation security framework that brings together flexible solutions, products, and services to address and enforce consistent business policy throughout the distributed network The Cisco SecureX

Architecture blends global threat intelligence and contextual awareness to address unique security challenges, such as the increase in highly mobile users, the wide variety of network-enabled mobile devices, or the move to cloud based infrastructures and services by protecting information, applications, devices and users. The Cisco SecureX Architecture protects today's borderless networks by providing effective security for any user, using any device, from any location, and at any time. This new security architecture uses a higher-level policy language that understands the full context of a situation, the who, what, where, when and how. With highly distributed security policy enforcement, security is pushed closer to where the end user is working, anywhere on the planet.

The work place is changing, which has required all of us to change the way we think about security. Cisco SecureX simplifies policy language and does for security what content delivery networks did for webpages. It brings scanning and protection to wherever the users are. By reimagining security, we can transform it from being a gatekeeper to being an enabler that allows companies to adopt and benefit from new technologies. Security becomes

a competitive weapon, not for what it keeps out, but for what it lets in—the great advances of the future.

SecureX is not just about extending security to mobile devices but to capturing contextual information in the use of policy creation. Contextual information includes user and device identity plus location, login time of day, plus which specific applications users attempt to access too, and this information is not only collected upon login but during their entire network connected session. Context aware policy allows IT leaders to use this information in the creation of policy with the end result of either allowing or denying access to IT resources, independent upon endpoint device and method of which access is attempted.

and while SecureX is security, in reality, it's bigger than just security, because security is a necessary integrated attribute to enable mobility, video, voice and web collaboration, etc. To create a secure IT environment, IT services need to interact with security services with minimum to no user intervention that steals productivity. In short, SecureX seeks to make Cisco security and network devices work better together through context aware policy so access and deny decisions are improved and are built upon so that anomalistic behavior remediation is automated post access through traffic monitoring.

References

[1] Armbrust, M, Fox, A, Griffith, R, Joseph, A, Katz, R, Konwinski, A, Lee, G, Patterson, D, Rabkin, A, Stoica, I, & Zaharia, M 2010, 'A View of Cloud Computing', Communications of the ACM, 53, 4, pp. 50-58.

[2] Bisong, A, & Rahman, S 2011, 'An Overview of the Security Concerns in Enterprise Cloud Computing', International Journal of Network Security & Its Applications, 3, 1, pp. 30-45.

[3] Dlodlo, N 2011, 'Legal, Privacy, Security, Access and Regulatory Issues in Cloud Computing', Proceedings of the European Conference on Information Management & Evaluation, pp. 161-168.

[4] Durkee, D 2010, 'Why Cloud Computing Will Never Be Free', Communications of the ACM, 53, 5, pp. 62-69.

[5] Etro, F 2011, 'The Economics of Cloud Computing', IUP Journal of Managerial Economics, 9, 2, pp. 7-22.

[6] Liang and Wang, (2005), W. Liang and W. Wang, On performance analysis of challenge/response based authentication in networks, The International Journal of Computer and Telecommunications Networking 48 (2) pp. 267–288.

[7] Madruga and J.J. Garcia-Luna-Aceves 2005, " Scalable Multicasting: The Core Assisted Mesh Protocol “, accepted for publication in ACM/Baltzer Mobile Networks and Applications Journal.

[8] Malekzadeh et al., 2005 M. Malekzadeh, A.A.A. Ghani, Z.A. Zulkarnain and Z. Muda, Security improvement for management frames in IEEE 802.11 networks, International Journal of Computer Science and Network Security 7 (6) pp. 276–284.

[9] Naraghi-Pour and Desai, 2008 M. Naraghi-Pour and V. Desai, Loop-free traffic engineering with path protection in MPLS VPNs, Computer Networks 22 (12) (2008), pp. 2360–2372.

[10] Palmieri, 2003 Palmieri F. VPN scalability over high performance backbones evaluating MPLS VPN against traditional approaches. In: Proceedings of the eighth IEEE international symposium on computers and communications (ISCC), vol. 2, June–July 2003. p. 975–81.

[11] Ruan, K, Baggili, I, Carthy, J, & Kechadi, T 2011, 'Survey On Cloud Forensics And Critical Criteria For Cloud Forensic Capability: A Preliminary Analysis', Proceedings of the Conference on Digital Forensics, Security & Law, pp. 55-69

[12] Salem and Hubaux, 2006 N.B. Salem and J.-P. Hubaux, Securing wireless mesh networks, IEEE Wireless Communication 13 (2), pp. 50–55.

[13] Sen, 2009 J. Sen, A survey on network security, International Journal of Communication Networks and Information Security (IJCNIS) 1 (2), pp. 59–82.

[14] Singh, G, Sharma, A, & Lehal, M 2011, 'Security Apprehensions In Different Regions Of Cloud Captious Grounds', International Journal of Network Security & Its Applications, 3, 4, pp. 48-57

[15] Spainhower et al., 2008 M. Spainhower, J. Butts, D. Guernsey and S. Shenoi, Security analysis of RSVP-TE signaling in MPLS networks, International Journal of Critical Infrastructure Protection 1, pp. 68–74.

[16] Yan, H 2010, 'On the Clouds: A New Way of Computing', Information Technology & Libraries, 29, 2, pp. 87-92.

Ammar Yassir received the B.Sc. degree with Honors in Computer Science in the year 2002 from Future University, Sudan and Master in Business Administration and Information Technology degree from Sikkim Manipal University, India in 2006 and currently a Ph.D. candidate in Information Technology, CMJ University, Shillong, India. He is now lecturer at Muscat College, Sultanate of Oman. He has published international papers in IJCSNS.

Smitha Nayak received the B.Sc. degree in Physics in 1998 from Mumbai University, India and Master of Computer Application degree from Visweshwaraiya technological University, India in 2001 and currently a Ph.D. candidate in Information Technology, CMJ University, Shillong, India. She is now lecturer at Muscat College, Sultanate of Oman. She has published international papers in IJCSNS.