On Implementing Real-time Detection Techniques in Future Network Access Control (NAC)

Adnan Ashraf[1]
adnanlooking@ieee.org

Manzoor Hashmani[2]
mhashmani@yahoo.com

B.S. Chowdhry[2]
bsc_itman@yahoo.com

Abstract— **Designing network security perimeters to nullify security threats is the objective of 'security gurus' involved in the development of security applications and devices. An organization, not uncompromising on security, dedicates a hefty budget proportion for deploying security plans and updates. Fighting and chasing the modern attackers 24x7 has enforced thoughts of redesigning security framework. Existing perimeter is layered of border routers, firewalls, IDS, IPS, VPN devices, software architecture over DMZs and subnets, beside server and host filters and antivirus applications. These are not fully customizable against adversaries in providing strong security framework. The current deployment nature of security perimeter where these layered components are prone to various egress and ingress nasty activities raises some serious questions. The traditional perimeters do not provide sufficient security to overcome these limitations in order to provide uncompromised security nodes [3][11][12]. To address security needs efficiently, at critical knots within a network, we introduce a security framework. The proposed framework focuses three key areas related to defense-in-depth; (1) maximizing synchronization among layered security services (2) modularizing various services for better endpoint security (3) reducing traffic while providing secure mechanism for encrypted updates in traditional networks. We show through analysis and emulation that our proposed framework meets the unique security needs of network infrastructure in a better way.**

Keywords-Network switch security; Security framework; Network security perimeter; Network access control; Antivirus retention

I. INTRODUCTION

Advancements in interception, intrusion, modification and fabrication posed potential threats to security perimeter of the time. Inescapable battle has been set and various mature hijacking and sniffing systems have been developed. This is why a large portion of corporate budget sinks in buying competitive security solutions. These solutions projects lists of precautions indicating the way a network should be accessed. Instead of molding the solution for the network, the network is asked to change the priorities. In fact, the level of security of these solutions is not scaled accurately for responsiveness, efficiency and reliability by vendors themselves.

The project was accomplished in the Mehran University of Engineering and Technology, Pakistan (MUET). The author[1] is a PhD candidate and co-authors[2] are members of the research faculty IICT, MUET.

The history proves that the users, administrators and hackers scale the security solutions through the nuisance or ease of working. In fact, the seller buys the solution and not the security. At the end of the day, the blame of failure is deposited to 'not updating timely.'

Today, a corporate network consists of security devices, applications, firewalls, sensors, fingerprint agents, filters, intrusion detection, and prevention systems to participate in security perimeter design [6][9][14]. Our research is based on the analysis of providing an enhanced and synchronized version of security perimeter. The solutions must be designed to respond the security needs of a network and not the vice-versa.

Another critical situation arises when internal network is turned internally for attacks. During HELLO, the catalyst considers the node(s) as privileged and enters its MAC in CAM table without knowing destination address [16][17]. It creates traffic by forwarding the frame for authentication on all ports except the one, it came from. Authentication is responded and MAC of the server is entered with destination entry to establish an authentic link for further communication. In traditional network, usually, this is the time for seeking updates of various profiles including antivirus. What, if a malicious endpoint corrupts or attacks its switched-neighbors before the antivirus updates this client. Now, whatever the solution exists, it shall be the reactive. Searching for some proactive measures shall take you buying another tool without scaled security but doubtful promises. The only thing growing as quickly as the number of security threats to the network is the number of tools one has to deploy to guard against them. How many security tools do we have in our existing network today? More to the point, how much time does a security administrator spend managing these tools - installing upgrades, downloading new signature files, and so on? It's overwhelming [18]. Therefore, we make following contributions in this paper:

Our purpose is to achieve maximum synchronization of security framework components in existing network security. This is to improve the performance of the network core layer concerning the speed, traffic load and transparent control of security perimeter.

-- We present a more secure network security framework and tested in real environment during peak traffic hours. It addresses potential threats in node and helps defining modularity among security components effectively. It also works with existing blocks of the traditional networks.

-- We identify critical challenges, the components facing in the internal-network and emulated the proposed framework in components at access layer. This speeds-up and liberates the core layer from unwanted traffic to confirm its efficiency.

-- We present the design of framework and then a mechanism to implement it. The proposed framework helps to reduce the amount of traffic on the core layer of the network.

Section 2 provides summary of related work in security perimeter building blocks. Section 3 presents our security framework while discussing the synchronization of policy based services, antivirus applications, role of catalyst, handshaking of routing components with communication nodes down the network, mechanism and arrival of updates before the authentication process of an endpoint occurs. Section 4 gives analysis of our proposed security framework, evaluation and comparison of results. Section 5 portrays the future roadmap, whereas sections 6 and 7 have been summarized for conclusion and recommendations for an integrated framework in modern designs of hardware.

II. RELATED WORK

We deal the security issues with an equal perspective of both, the hackers and the anti-hackers. The current security scenario indicates that hackers are one step ahead of implanted security solutions [14][15]. They like to hack the image or identity of any point from client or server and beyond. Generally those attacks perceive the faults in systems that the security builders, often do not know while launching solutions.

Researchers have addressed many areas of the network security perimeter. Majority of the research has focused on strengthening the individual perception of components like firewall, activity filter, antivirus sensitivity, secure routing, secure key distribution and securing server or node privacy. Whereas, work in bits is found on the components synchronization and interdependencies while providing logical separation among all components to provide defense-in-depth. The security solution is required to be quantified aa a strong and integrated fence. Developing platform independent prevention and detection tools [1][4][8], enforcement and approaching new security policies [2][4][6][7], and strengthening antivirus applications [10][13][15] have been a few kinds of work in this direction. Introducing endpoint security with network access control (NAC) has challenged the security consultants to revise the corporate security needs and number of tools employed for the desired security [3][12].

Learning that 'it is vain to do with more what can be done with fewer' - William of Ockham - a few gateways are free to install as a replacement of personal hodge-podge of security solution. These claim to be a single, integrated, enterprise-grade tool that provides a firewall, VPN, bandwidth management, virus scanning, anti-spam, anti-phishing and more [5][11].

III. THE PROPOSED SECURITY FRAMEWORK

A. *Maximizing synchronization*

Success rests in the fact that the policy-based services or firewall, secure routing schemes, authentication mechanisms, antivirus, applications and hardware must be, theoretically, one entity [10]. It is achieved by distributing services carefully and capitalizing the synchronization among these services. Figure 1 next, shows a theoretical defense-in-depth single window solution.

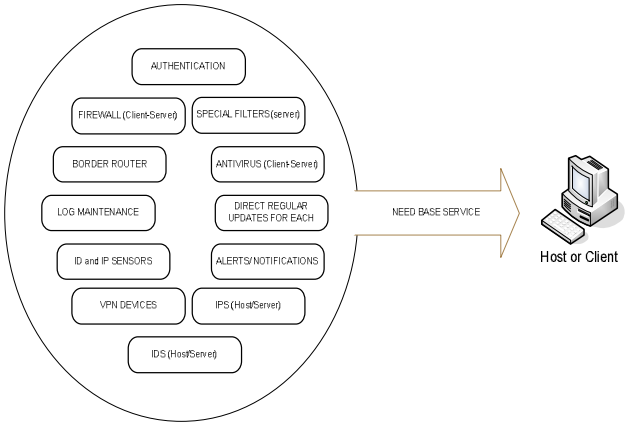

Figure 1. Ideal security perimeter: A model

B. *Modularizing the solution for potential threats*

In order to take real-time advantages from the system in existing infrastructure the existing perimeter was appended to analyze the performance and tolerance to the network. Today the existing designs of network security perimeter present the layers-of-devices but functionally overlapping of results of these devices cause failure of the perimeter fence [4][6]. Figure 2 next is a logically view of separated services to achieve the above fundamental objectives from the security perimeter.

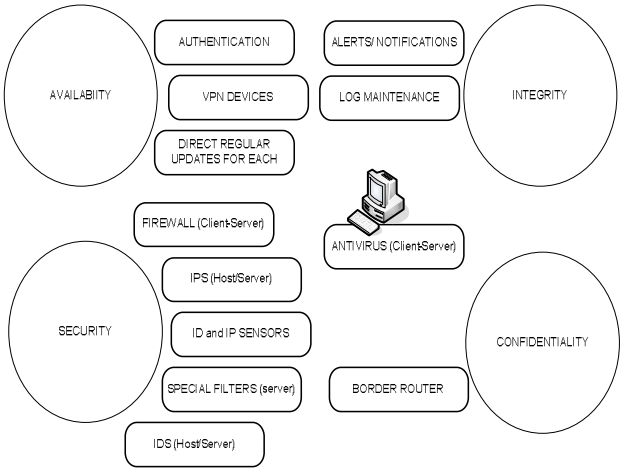

Figure 2. Optimal requirements from a traditional network

C. *Minimizing the unnecessary traffic load and avoiding threats at core layer*

The main issue at the backbone or core layer is that any failure (even in terms of delay) will likely be felt everyone within the inter-network. The Speed plays a vital role at core layer. Due to sheer volume of traffic that will be entering the backbone, few activities that consume routing or switching resources should be applied in this layer. In other words, routing, ACL-access lists, ACE-access entries compression encryption, and other resource consuming activities should be done before the packet arrives at the core [8][14][16][17], as shown in Figure 3 next.

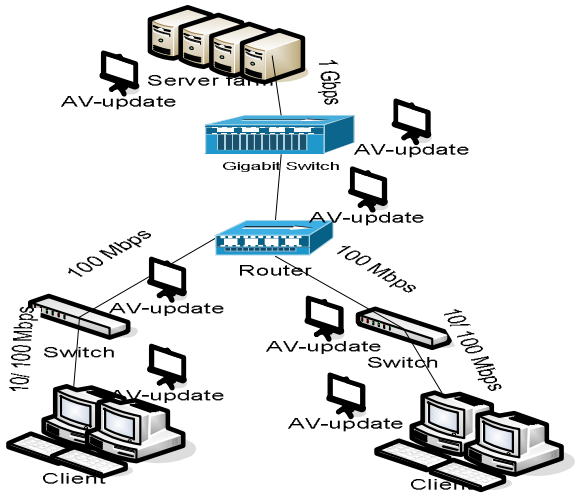

Figure 3. Updates in the traditional security framework

Similarly, the traffic during antivirus updates must be shed and can be either placed at configurable switches of distribution layer (provided that hardware vendor reserve space) or access layer. This clearly sheds the load on core layer as well as, maintains the integrity within these switches. Firewall rules are distributed passively in the same way and exploit the features of these switches unlike hackers that do in the opposite directions. This also prevents from the malicious opportunists to write virus code and flooding in form of hello to neighbors in a group.

D. *Secure framework*

Acclimatizing a traditional network with core, distribution and access layer devices and each service is running from the farm-of-servers obliging the results from each other at a single log. The single logger can be a powerful analyzing tool or administrator. We were accustomed with Snort® in our scenario. The antivirus server performs the following functions.

Antivirus server shall PUSH encrypted updates once on each destination (catalyst) as soon as, routers flood framed <HELLO> for authentication. This contains updates in encrypted format and are, usually, in kilobytes.

Every time a membership changes on joining or disjoining group, the server serves the query if any update is received from the builder of the antivirus.

The switch with encrypted virus updates is responsible for following tasks.

-- If this is a distribution layer switch then, it shall PUSH updates to access layer's configurable switch.

-- Once these updates reached the destination LAN switch, <AV-HELLO> may be forwarded only to those hosts interested in <HELLO> or flooded to all hosts by a non multicast-enable layer 2 switch. In any of the above case, each <HELLO> must be followed by <AV-HELLO> packet.

--It must receive ACK for each <HELLO>. Otherwise check for retransmission of <HELLO>. Storage of these bytes require more pace at switches.

--It shall behave similarly to any alert or notification as, if <HELLO> acknowledge is not received, i.e. MAC should be removed from the CAM table and report is generated for servers at core-layer.

--Upon successful echo replies for both, the frame is forwarded known communication link furnishing destination port in the CAM table of switch.

--The updating part of proposed framework, in the model given in figure 3, is performed by 'routing and information server'. It played the role of flash-memory updater in switches. Consequently, we propagate memory resident encrypted security updates among the hosts linked to our special PC-router at access layer.

Applications at antivirus server signs a contract with available access layer catalyst through the device API. It overrides encrypted security updates in the flash memory of the manageable catalyst.

IV. ASSESSMENT OF PROPOSED FRAMEWORK

This section consists of two parts. The first part gives an analysis of the presented proposal through arguments, and second part analyzes the results of the evaluation which support the arguments presented in the first part.

A. *Analysis of the proposed framework*

This section presents an analysis of the features of the proposed framework [refer section 3]. Those features make the framework feasible to implement in existing network infrastructures.

Unlike other security perimeters, the switches in the proposed framework do not generate or direct the redundant traffic at every nook and cranny of the core layer. This traffic reduction is due to the nearby accessibility of regularly deemed updates, alerts, notifications, acknowledgements and log reports maintenance by endpoint security applications.

As, the execution of compatible updates is only at client side therefore, neither complexity nor memory upgrade is required in the switches of the access layer. This makes the updating process. For these reasons, the constraint of hardcode

has negligible effect on the results. Whereas, the proposed flow of the update mechanism in figure 4 provides stronger resilience towards various internal attacks and malicious code, e.g. sinkhole, continuous ping, hello flood.

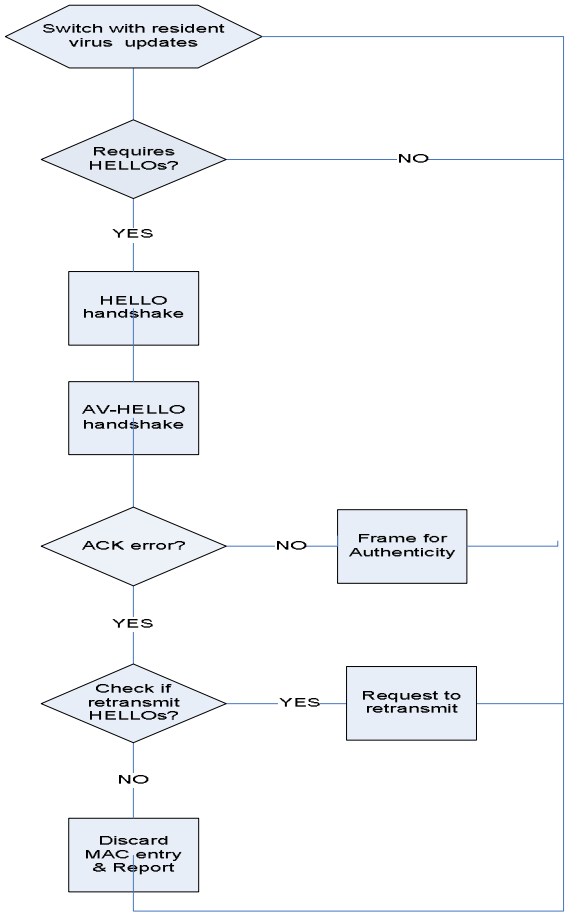

Figure 4. Switch communicating updates

The flow of security information and the update is proposed in such a way that, only privileged applications at server, can resend or rewrite the entries. The encrypted security updates at client require temporarily acquired permission from the client operating system. This quantifies the ownership of updating <AV-HELLO>.

Distinctiveness of the framework is its ability to give maximum protection at first step, from trojans, logic bombs, virus, trapdoors, backdoors and information leaks.

B. Emulation and scalability of the proposed framework

The technique presented in this framework takes both the configurable and non-configurable switches into account. The emulation of the proposed security framework is set over a campus network of 540 nodes, domain controller, DHCP server, corporate firewall server, proxy server and an exchange server. An empirical state of the proposed model is given in figure 5.

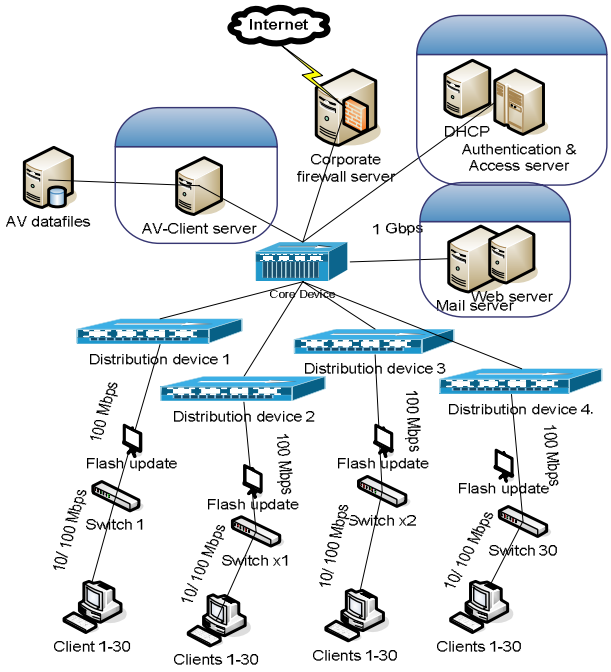

Figure 5. Proposed framework-based campus-wide security perimeter

It contains one core, four distribution and 30 access layer switches in its perimeter.

C. Discussion of results

The results of the proposed fence and traditionally deployed fence were compared and reported in figure 6 (x-axis→ threats, y-axis: # of threats)

Also, a higher number of attacks are detected by applications running for antivirus and firewall servers.

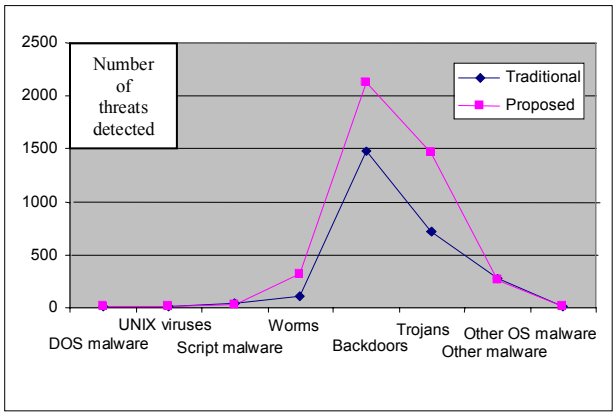

Figure 6. Network perimeter defense-in-depth analysis (proposed secure framework versus traditional secure framework)

The statistics of the whole activity is given in Table 1.

TABLE I. TABLE1. STATISTICS OF ATTACKS AND DEFENSE

Name of attacker	Attacks	Statistic of attacks (blocked)	
		T.N.P.M	***P.N.P.M***
DOS malware	50	8	16
UNIX viruses	44	8	8
Script malware	232	35	24
Worms	517	111	324
Backdoors	3851	1477	2130
Trojans	3653	725	1461
Other malware	371	279	269
Other OS malware	137	19	8
Total	**8855**	**30.1%**	**47.9%**

→ T.N.P: Traditional network perimeter model

→ P.N.P Proposed network perimeter model

The technique presented in this framework takes non-configurable switches into consideration that do not participate in storing and sending <AV-HELLO> related elements. These switches can not use IGMP to find out the multicast hosts. Now router can direct these switches about multicast group membership using CGMP. This allows multicast-enabled switches to forward multicasts only to hosts that are new and participating in the group. This shall save further need of processing cost in switches to accommodate this framework.

The switches deployed can be further reprogrammed to remove MAC of corrupt node for the strict security in the network by employing some rules. Assuming the ongoing developments in network infrastructure, catalyst processing and storage, adaptive networks, it can be proclaimed that the framework may be deployed in even larger networks. The customizable nature of the framework makes it viable for small and medium size organizations.

V. METHODS FOR FUTURE INTEGRATION

Currently we are staging to project efforts in two directions. One direction is to develop a vendor-specific powerful API that can perform AV-updates in configurable catalysts down the network. This development shall help adaptive rules to veto or pass the communication through the endpoint [1][9][18]. The second is the hardware architecture for such devices. A wide role of industry professionals is expected.

A. The software

An open standard APIs development that shall help loosing monopolized control of companies in security products. On the other hand, it shall help customizing the varying demands of security perimeter in organizations.

B. The Hardware

The cooperation of catalyst vendors can be sought to design a service-oriented hardware that inherits the potential to implement this framework. Only a powerful module (a catalyst in our case) can perform great for security perimeter. In general, a dedicated hardware helps to implement a strong security policy.

C. Device update

The verification of encrypted updates can be sought by "knowledge consistency checker" at distribution or access layer device. We are successful to analyze characteristics of the proposed perimeter in following three perspectives for future working. I) Mannerism of the system: Decreased complexity of the perimeter, improved integration of services (passive and active components), reduced overall cost of deployment, reduced dependency from hard coded (proprietary) solutions for high system stability and budget-friendly. II) The cost of computation: Our proposal helps in faster logging of alerts or notifications, short-time service updates for endpoint protection, fewer bottlenecks, less waiting, and simple group policy, and III) Improved results: The proposed framework ensures reduced error probability, ease in archiving the automatic reports and automatic workflows.

Analyzing the bottlenecks of network security devices and tools for delivering the proper support, we suggest few enhancements in solutions at corporate level.

D. Device memory reservation

A reserved space may be endorsed into catalyst. It shall serve the purpose of a base station in antivirus client-server architecture for sending encrypted updates to each host in the network.

E. Merger of powerful applications

The security giants should come forward from areas of firewall, routing and antivirus for joint ventures of integrating such modularity in related network hardware.

F. Roadmap requirements

Industries that are engaged in application development or device manufacturing for setting up advanced security solutions must initialize competitions and research challenges to effectively simulate likely frameworks.

VI. CONCLUSION

In this paper we have presented a network security perimeter for a true defense-in-depth approach which is designed from a healthy synchronization approach embedded at first place of the network. We have presented a hierarchical model with true logical separations among different services. Some services were pre-deployed as the security was a priority. Now emulating this we have quantified the framework for providing better security on the basis of results obtained. We plan to recommend this framework having confidence as first step towards merger of antivirus services with other network resident services.

ACKNOWLEDGMENTS

Our special gratitude goes to our network engineers (Engr. Raheel, Engr. Ali, Engr. Yousuf, are a few names) at Internet

Control Computer Center, Mehran UET for the real-time simulation of the framework in campus network. Our special thanks to IT-specialist Miss: Marvi Mussadiq.

REFERENCES

[1] Hae-Jin Jeong; Il-Seop Song; et-al; "A Multi-dimension Rule Update in a TCAM-based High-Performance Network Security System"Advanced Information Networking and Applications, 2006. AINA 2006, 20th International Conference on Volume 2, 18-20 April 2006 Page(s):62 – 66

[2] Al-Shaer, E; "Network Security Policies: Verification, Optimization and Testing"
Network Operations and Management Symposium, 2006. NOMS 2006, 10th IEEE/IFIP, 2006 Page(s):584 – 584

[3] Magic quadrant, "Symantec network access control; the key to endpoint security" advertising section report 2006, www.symantec.com/endpoint

[4] Hamed, H.; Al-Shaer, E; "Taxonomy of conflicts in network security policies"
Communications Magazine, IEEE, Volume 44, Issue 3, March 2006 Page(s):134-141

[5] Salim, R.; Rao, G.S.V.R.K;" Design and Development of Network Intrusion Detection System Detection Scheme on Network Processing Unit" Advanced Communication Technology, 2006. ICACT 2006, the 8th International Conference, Volume 2, 20-22 Feb. 2006 Page(s):1023 – 1025

[6] Adnan A. Arain, Marvie, Manzoor Hashmani, "An analytical revelation for a safer network security perimeter", 2006 proceedings of Intentional Conference on Information and Networks-ICOIN2006 Sendai, Japan, 14-17 January 2006

[7] Schaelicke, L.; Freeland, J.C.; "Characterizing sources and remedies for packet loss in network intrusion detection systems" Workload Characterization Symposium, 2005. Proceedings of the IEEE International 6-8 Oct. 2005 Page(s):188 – 196

[8] Jiang-Neng Yi; Wei-Dong Meng; Wei-Min Ma; Jin-Jun Du; "Assess model of network security based on analytic network process" Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on Volume 1, 18-21 Aug. 2005 Page(s):27-32 Vol. 1

[9] Harrison, J.V.; "Enhancing network security by preventing user-initiated malware execution" Information Technology: Coding and Computing, 2005. ITCC 2005, International Conference on Volume 2, 4-6 April 2005 Page(s):597 - 602 Vol. 2

[10] Yanhui Guo; Cong Wang; "Autonomous decentralized network security system" Networking, Sensing and Control, 2005. Proceedings, 2005 IEEE, 19-22 March 2005 Page(s):279-282

[11] Stephen Northcutt, Lenzy, et-al, "Inside network perimeter security: The definitive guide to firewalls, virtual private networks (VPNs), routers, and intrusion detection systems", ISBN 0672327376, SAMS; 2nd Edition, March 4, 2005

[12] Brian Monroe, Security Engineer-STILLSECURE, "Demystifying network access control", white paper 2005, www.stillsecure.com

[13] Djordjevic, I.; Phillips, C.; Dimitrakos, T; "An architecture for dynamic security perimeters of virtual collaborative networks" Network Operations and Management Symposium, 2004. NOMS 2004, IEEE/IFIP, Volume 1, 19-23 April 2004 Page(s):249 - 262 Vol.1

[14] Sean Convery, "Network security architectures", ISBN: 158705115X, Cisco Press; 2nd Edition Edition, April 19, 2004

[15] Stephen Northcutt, Judy Novak, "Network intrusion detection", ISBN 0735712654, SAMS; 3rd Edition, August 27, 2002

[16] Todd Lammle, Sean Odom, Kevin, "CCNP- Routing (study guide)"; SYBEX press Exam 640-503Fdsf

[17] Wendell Odom, "CCNA Intro (self study guide)", CISCO press; Exam 640-821

[18] Glen Kunene, "Perimeter security ain't what it used to be, experts Say" Senior Editor, DevX, www.devx.com/security/ Article/20472