International Journal of Security and Its Applications
Vol. 1, No. 1, July, 2007

An Efficient and Intelligent Intrusion Detection and Response System using Virtual Private Networks, Firewalls and Packet Filters

Emmanuel Hooper
Information Security Group University of London Royal Holloway, Egham, Surrey, TW20 OEX, UK. EHSC, Camarillo, California, USA.
ehooper@aya.yale.edu, E.Hooper@rhul.ac.uk

Abstract

There major challenges for current Intrusion Detection Systems (IDS) which attempt to identify suspicious network traffic. Due to the high percentage of alerts generated by such systems, the level of false positives is among the significant problems. We present intelligent strategies for reduction of false positives and infrastructure protection using a novel approach using adaptive responses from firewall packet filters in what we call, network quarantine channels (NQC). This involves using an efficient and intelligent intrusion detection and response system using Virtual Private Networks, firewalls and packet filters. The firewall packet filters provide effective intelligent responses by to granting access to the normal packets and denying malicious traffic access to the network, after the identity of the connections are verified through the statistical analysis in the NQC. These effective strategies reduce false positives and increases detection capability of the IDS

1. Introduction

The strategic detection and response strategies consist of packet firewall packet filtering policies in the NQCs. Intrusion Detection System (IDS) lack effective collaborative responses [1, 5, 16, 15] to real attacks and large volumes of normal traffic in various infrastructures [5, 16, 18]. Furthermore, the increasing packet rates and attacks fast network environments reduce the performance of IDSs [4, 14, 16, 17, 20]. In this paper, we describe how the effective strategies including firewall packet filtering policies and their response to attack packets. After the NQC has determined the status of the packet using interactive responses of simulated scripts, actual final responses to the hosts determine whether they are permitted final access to the destination hosts. Normally, IDSs respond directly to the hosts which generate alerts with considerable false positives. We propose multiple strategies including firewall packet filters and policies to permit access normal users and deny access to astute hackers.

2. Network quarantine channels and Firewall Packet Filter

The strategic response approach involves the use of firewalls and packet filters in responses from hosts in various network subnets of the network quarantine channels (NQCs) described in [10]. The scripts in the hosts in the NQC simulate initial responses to packets from source hosts and obtain additional packets from the hosts. Subsequently, they are analysed in the attack patterns database using statistical analysis including Bayes classification, discriminant analysis and hierarchical clustering

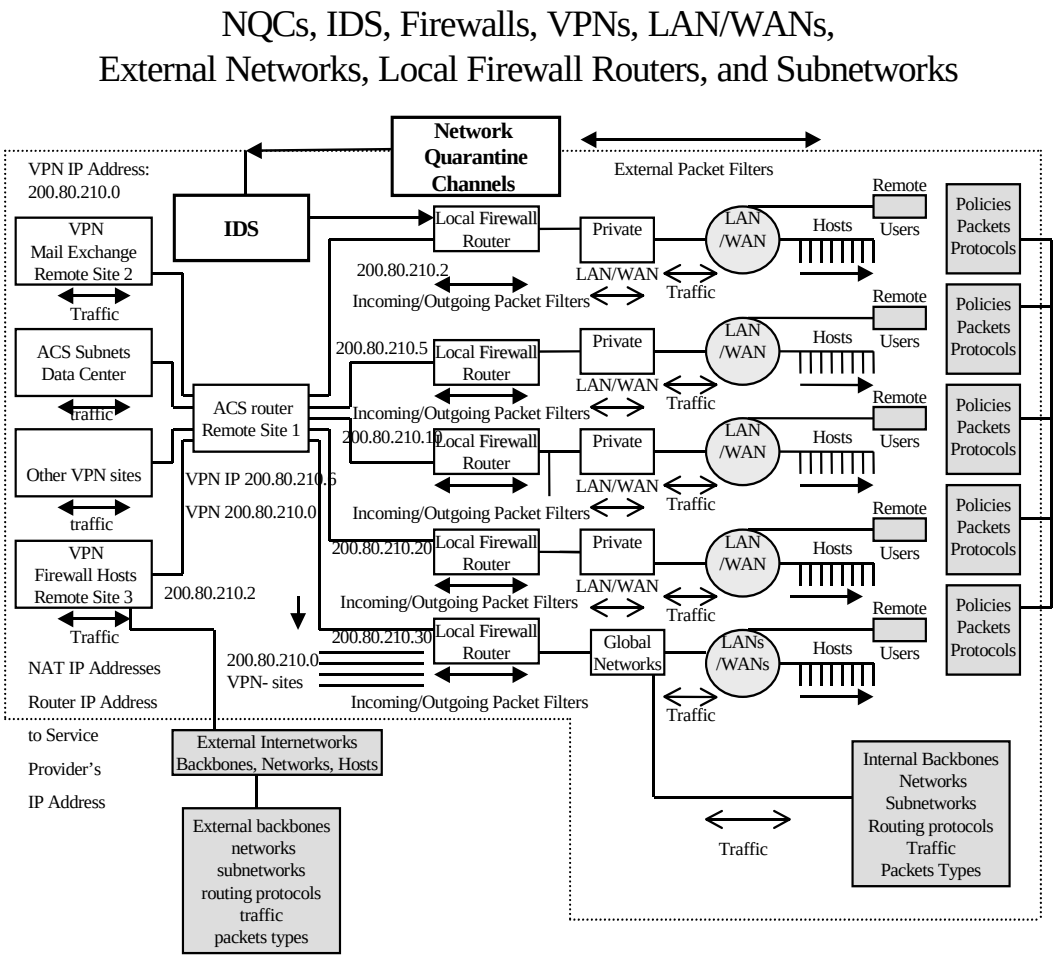

Figure 1. Multiple VPNs and firewall architecture for attack and false positives in NQC zones

techniques. The final status of the alerts determined from the statistical analysis is fed back to the IDS alert monitor using various feedback techniques. This includes adaptive rules in the IDS Alert filter and Alert Policies. This is described in detail in [10]. The additional remote traffic is controlled, segregated and filtered using Cisco Secure Access Control Servers (ACS) [3] routers to prevent access to sensitive segments of the internal VPNs. The additional traffic from the segregated sites, including packets from the VPN mail exchange servers, ACS subnet data centre and other VPN firewall host sites are diverted to the NQCs for analysis. See Figure 1. The external and internal backbones are further isolated in various zones using gateway packet filtering, multiple protocols, packet filtering and policies. Furthermore, Network Address Translation (NAT) hides internal addresses from external hosts, reducing the risks of unauthorised access to internal hosts using internal IP addresses. The NQCs examine and respond to the remote and external traffic and send feedback to the IDS on their final statuses. The firewalls in each zone are then instructed to deny or permit final access to the respective destinations based on whether they are benign or malicious packets.

The strategies for the final responses to the connecting hosts once the status of the packet has been established by the NQC involves the following process:

1. NQC sends the final status of the packet to the IDS alert monitor.

2. The NQC constructs Final Reply Rulesets in IDS to respond to the source host.

3. The NQC uses Reply Rulesets in IDS to respond to the source host.

4. The Firewall constructs Packet Filtering Rules based on the rules from NQC-based IDS Reply Ruleset.

5. The Firewall Permits access to normal hosts and denies access to astute hacking hosts.

6. The NQC-based Firewall and IDS log the sessions on IP addresses of connected or denied hosts for subsequent analysis.

The packet filters are applied to various categories of alerts, such as exploits and reconnaissance categories. Examples of policies pertaining to firewall packet filters for exploits and reconnaissance attack categories are shown in Tables 1 and 2. Table 3 shows a packet filter policy for SMTP W32 Mimail worm. Table 4 shows packet filter policy for alerts using SMTP using protocol. The attacks of "high" severity have more priority than those of "Medium" severity. The "policy target" indicates the targets of the suspicious source hosts.

Table 1. Firewall Policies and packet filter for exploits category

Policy	**Policy Target**	**Alert Firewall Policy**	**Policy Sever-ity**
Enable	Exploits	Server port	High
Enable	Exploits	Buffer Memory Exhausted	High
Enable	Exploits	Internal hosts	High

Table 2. Firewall Policies and packet filter for reconnaissance category

Policy	Policy Target	Alert Firewall Policy	Policy Severity
Enable	Reconnaissance	DMZ hosts	High
Enable	Reconnaissance	Perimeter routers	High
Enable	Reconnaissance	External firewall interfaces	High

Table 3. Firewall Packet Filter Name – SMTP W32 Mimail.c Worm

Firewall IP Action	Source IP Start	Source IP End	Destination IP Start	Destination IP End
Deny	198.52.95.19	198.52.95.19	150.20.10.5	150.20.10.5

Table 4. Firewall Policies for alert categories using protocol – SMTP

Policy No.	**Policy Target**	**Alert-Enabled Policy**	**Policy Severity**
Enable	SMTP	W32 Mimail.c Worm	High
Enable	SMTP	Heap Overflow in Windows Script	High
Enable	SMTP	Long SEND Parameters Buffer Overflow	High
Enable	SMTP	Microsoft Outlook Field Buffer Overflow	High
Enable	SMTP	Shellcode Found in SMTP Command	High
Enable	SMTP	MaZ Worm Email	High
Enable	SMTP	Message Header Overly Long	Medium

Table 5. Firewall Policies for alert categories using protocol – Netbios

Policy No.	**Policy Target**	**Alert-Enabled Policy**	**Policy Severity**
Enable	MSSQL	Xp sqlinventory Buffer Overflow	High
Enable	NETBIOS	XP Shell Buffer Overflow	High
Enable	MSSQL	Xp Registry Access	High
Enable	NETBIOS-SS	Windows 2000 Null Password	High
Enable	MSSQL	OpenRowSet Possible Buffer Overflow	High
Enable	NETBIOS-SS	Copy Executable File Attempt	Medium

Table 6. Firewall Policy and Packet Filter – Buffer Memory Exhausted

Firewall IP Action	**Source IP Start**	**Source IP End**	**Destination IP Start**	**Destination IP End**
Deny	190.20.25.12	190.20.25.12	150.10.20.2	150.10.20.2

Table 7. Firewall Alert Filter Name – User login failed

Firewall IP Action	**Source IP Start**	**Source IP End**	**Destination IP Start**	**Destination IP End**	**Destination Port End**
Permit	50.20.10.0	50.20.10.0	50.20.10.0	50.20.10.0	1029

Table 8. Firewall Packet Filter Name – NETBIOS-SS Windows 2000 Null Password

Firewall IP Action	**Source IP Start**	**Source IP End**	**Destination IP Start**	**Destination IP End**
Permit	50.20.106.4	50.20.106.4	50.20.106.32	50.20.106.32

Table 9. Firewall Packet filter policies for Outside Firewall

		Description of Policy Rule Set: Include all except for the RECONNAISSANCE category; Exclude noisy signatures					
Include	**Categories**	**Protocols**	**Operating**	**Applications**	**Max. Attack**	**Max. Benign**	**Trigger**
/Exclude			**System**		**Severity**	**Trigger**	
Include	All	All	All	All	High	Low	All
Exclude	Reconnaissance	All	All	All	High	Low	All

Table 10. Firewall Packet filter policies for Inside Firewall

		Description of Policy Rule Set: Include alerts for protocols ? TFTP, TELNET, RIP; Exclude noisy signatures					
Include	**Categories**	**Protocols**	**Operating**	**Applications**	**Max. Attack**	**Max. Benign**	**Trigger**
/Exclude			**System**		**Severity**	**Trigger**	
Include	All	All	All	All	High	Low	All

Table 11. Firewall Packet filter policies for False Positives

		Description of Policy Rule Set: Policy that turns off signatures for ignoring traffic generating false positives					
Include	**Categories**	**Protocols**	**Operating**	**Applications**	**Max. Attack**	**Max. Benign**	**Trigger**
/Exclude			**System**		**Severity**	**Trigger**	
Include	All	False Positives	All	All	High	Low	All

3. Responses using Packet Filter Rule, NQC and IDS

The NQCs send messages with the firewall and packet filter rules, that state which the source IP address and destination, port and packet type should be filtered from the IDS alert monitor to reduce false positives. An example of a firewall packet filter for memory buffer exhaustion is illustrated as follows. See Table 6. This prevents memory exhaustion by alerting the IDS through the NQC system. The host with IP address, 190.20.25.12 and using buffer memory exploits is denied access to the internal network. Table 8 shows an example for permitting an SQL normal packet access to its intended destination. Table 7 shows an example for permitting a normal netbios packet access to its intended destination. The Firewall Packet Filters policies were designed and applied in the NQC for responding to various categories of attacks and normal packets using multiple protocols. The example below illustrate the policies designed for the firewall rule set for All-Inclusive and Audit. Examples of firewall packet filters policies are shown in Tables 9 to 11 as follows:

1. **Firewall Packet filter policies for Outside Firewall:**
   Firewall Packet Filters for ingress/egress packets approaching/ leaving the outside Firewall. See Table 9.

2. **Firewall Packet filter policies for Inside Firewall:**
   Firewall Packet Filters for ingress/egress packets approaching/ leaving the inside Firewall. See Table 10.
3. **Firewall Packet filter policies for Outside Firewall:**
   Firewall packet filters for ingress/egress packets, resulting in false positives, approaching/leaving network. See Table 11.

4. Experimental Details

In this section we describe the experimental environment. The objective of the experiment is to use the intelligent packet filters the intelligent response strategies to reduce false positives and increase the detection capability of the IDS. The adaptive firewall packet filters were applied to the IDS in a network environment comprising the NQCs, isolated by subnets and PIX Firewalls [2] from the internal private network. Each subnet of the NQCs has different IP addresses than those of the internal network. In addition, Network Address Translation (NAT) is used to conceal the internal IP addresses from the suspect host and the firewalls prevent access to the NQCs. The datasets consist of alerts from suspicious network traffic from suspect hosts, generated by the IDS detection mechanism and logged in the IDS Database. These were diverted for analysis in the NQC before they arrived at the IDS monitor.

4.1. Method

The experiments involving the adaptive firewall packet filters in responses from the NQCs were conducted as follows. The method involves the diversion of suspected network attacks to the quarantined channel zones. This is followed by sending responses to the suspicious packets, which appear as valid return packets to the potential attacker. This results in further packets from the attacker, which if they persist, are directed to subsequent zones for additional responses.

5. Results

This section describes the results of the effective use of firewall packet filters in the intelligent response strategies using the NQC. This results in effective in the final responses to normal hosts seeking to establish connections in the internal network and malicious intentions and hosts. The packet filters improved the response capability of the IDS after accurate detection of the final status of the packets. See Table 12:

6. Discussion

The results of the experiments are significant since they provide effective responses, reduce false positives and improve the detection and response capability of the IDS. The test accuracies are significant as they indicate high detection accuracy and reduction in false positives. Refer to Table 12. The total test accuracy for 7,730 Remote to Local (R2L) connections is 100.0%. These accuracies demonstrate the significance of the strategies in using adaptive policies and alert filters in the NQC in reducing false positives and distinguishing between benign connections and actual attacks in real-time.

Table 12. Results: Adaptive Firewall Packet Filters using NQC-IDS test dataset - Remote to Local (R2L) Confusion Matrix Accuracy Summary

Class target	**Positives**	**Negatives**	**Testing Accuracy**
FTP Bounce Attack	450	0	100.00%
HTTP Read Password	390	0	100.00%
REXEC Login	210	0	100.00%
MS Registry Remote Write	850	0	100.00%
IM ICQ Transfer	515	0	100.00%
RSH Null login	280	0	100.00%
DCERPC Invalid UID	650	0	100.00%
HTTP IIS cmd.exe	750		100.00%
Totals:	**Actual Positives**	**Actual Positives**	**Accuracy**
	4095	**0**	**100.00%**

7. Related work

These strategies in this research using NQC-based collaborative firewalls and IDS packet filters improve on related work. These strategies are not employed in honeypots [6, 11, 12, 19]. Honeypots only capture suspicious connections and tend to attract hackers. Furthermore, weaknesses in their design can expose the internal network to more attacks [21, 8, 7, 9]. The firewall packet filters respond to suspicious hosts using the NQCs designed with separate subnets, routers and firewalls to segregate traffic from the internal network. Furthermore, audit data analysis do not use firewall packet filters, NQCs or collaborative IDS and firewall responses of respond adaptively to source hosts. The analysis involves evaluation of traffic from infrastructures without adaptive interactive responses [14, 13, 22, 23].

8. Conclusion

The Firewall permits access to normal (benign) hosts and denies access to malicious traffic and complex attacks from astute hackers. Finally, the NQC-based Firewall and IDS logs of the sessions on both the source and destination IP addresses of connected or denied hosts provide additional monitoring capability and subsequent analysis in real-time as well as off-line analysis. These intelligent final response strategies are effective in the reduction of false positives and improvement in the response capability of the IDS to both normal and astute malicious traffic in current complex infrastructures. These intelligent strategies involve secure communication, traffic management, packet classification, content inspection and filtering, using adaptive packet filters, intelligent co-processors, and intelligent detection and response in network infrastructures.

9. References

[1] T. Bowen, D. Chee, and M. Segal. “Building survivable systems: An integrated approach based on intrusion detection and damage containment.” In IEEE Proceedings of the DARPA Information Survivability Conference and Exposition, volume II of II, IEEE Computer Society Press, 2000, pages 84–999.

[2] Cisco Systems Inc. Cisco PIX firewall 525 and Software, version 6.0, San Jose, CA, USA, 2005.

[3] Cisco Systems Inc. Cisco Secure ACS for Windows, version 4.0, San Jose, CA, USA, 2005.

[4] H. Debar and A. Wespi. “Aggregation and correlation of intrusion-detection alerts.” In Recent Advances in Intrusion Detection (RAID2001), volume 2212 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2001, pages 85–103.

[5] G. Helmer, J. Wong, V. Honavar, and L. Miller. “Intelligent agents for intrusion detection.” In Proceedings of the 2003 IEEE Information Technology Conference, IEEE Computer Society Press. Syracuse, NY, USA, September 1998, pages 121–124.

[6] T. Holz and F. Raynal. “Detecting honeypots and other suspicious environments.” In Proceedings of the Sixth IEEE Workshop on Information Assurance and Security, IEEE Computer Society Press, United States Military Academy, West Point, NY, USA, June 15–17 2005.

[7] Honeypot Project. “Know your enemy:genii honeynets. 2005,

http://www.honeynet.org/papers/gen2/index.html.

[8] Honeypot Project. “Know Your Enemy. Addison-Wesley Press, New York, NY, USA, 2nd edition, 2004.

[9] Honeypot Project. “Know your enemy:genii.” Honeynets, 2005.

http://www.honeynet.org/papers/gen2/index.html.

[10] E. Hooper. “An intelligent detection and response strategy to false positives and network attacks.” In Proceedings of the Fourth IEEE International Workshop on Information Assurance (IWIA 2006), IEEE Computer Society Press, University of London, Royal Holloway, United Kingdom, April 13–14 2006, pages 12–31.

[11 T. R. Jackson, J. G. Levine, J. B. Grizzard, and O. H. L. “An investigation of a compromised host on a honeynet being used to increase the security of a large enterprise network.” In Proceedings of the 5th Annual Information Assurance Workshop, IEEE Computer Society Press, West Point, NY, USA, 2004, pages 9–15.

[12] J. Levine, R. La Bella, H. Owen, D. Contis, and B. Culver. “The use of honeypots to detect exploited systems across large enterprise networks.” In Proceedings of the 2003 IEEE Workshop on Information Assurance. IEEE Computer Society Press, 2003.

[13] R. P. Lippmann, S. E. Webster, and D. Stetson. “The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection.” Computer Networks: The International Journal of Computer and Telecommunications Networking, 3949 of Lecture Notes in Computer Science: 307–326, 2002.

[14] M. V. Mahoney and P. K. Chan. “An analysis of the 1999 DARPA Lincoln Laboratory evaluation data for network anomaly detection.” In Recent Advances in Intrusion Detection (RAID2003), volume 2820 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 2003, pages 220–237.

[15] B. Morin, L. Me’, H. Debar, and M. Ducasse. “M2D2: A formal data model for IDS alert correlation.” In Recent Advances in Intrusion Detection (RAID2002), volume 2515 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, Zurich, Switzerland, 16–18, October 2002, pages 115–137.

[16] Network Associates. NAI Intruvert IDS: 1200, 2600 and 4000 Series, Santa Clara, CA, USA, 2004.

[17] V. Paxson. “Bro: A system for detecting network intruders in real-time.” Computer Networks, 1999, 31(23–24):2435–2463.

[18] L. Portnoy, E. Eskin, and S. Solfo. “Intrusion detection with unlabelled data using clustering. In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001), 2001, pages 76–105.

[19] N. Provos. “A virtual Honeypot framework. CITI Technical Report 03-1, Center for Information Technology

[20] T. H. Ptacek and T. N. Newsham. “Insertion, evasion and denial of service: Eluding network intrusion detection.” Technical Report, Secure Networks (McAfee) Inc., Santa Clara, CA, USA, January 1998. http://citeseer.ist.psu.edu/ptacek98insertion.html.

[21] J. S. Robin and C. E. Irvine. “Analysis of the Intel pentium’s ability to support a secure virtual machine monitor. ” In Proceedings of 9th USENIX Security Symposium, Denver, Colorado, USA, USENIX Press, August 14–17 2000.

[22] W. Wang and T. E. Daniels. “Building evidence graphs for network forensics analysis.” In 21st Annual Computer Security Applications Conference (ACSAC’05), Tucson, AZ, USA, IEEE Computer Society Press, December 2005, pages 254–266.

[23] W. R.Weiss and A. Baur. “Analysis of audit and protocol data using methods from artificial intelligence. In Proceedings of the 13th National Computer Security Conference, Washington, D.C., USA, October 1990, pages 109–114.

Authors

Emmanuel Hooper

Dr. Emmanuel Hooper earned a record of 3 PhDs within 5 years. He earned a PhD at the University of London, Royal Holloway, Information Security Group, UK, 2007; a PhD in Computing Sciences from the University of East Anglia, UK, 2006; and PhD in Historical Statistical research from the University of Birmingham, UK, 2005. He holds a BSEE from Portsmouth University, UK, multiple MA degrees from various universities including Yale University, USA, He has 27 years experience in infrastructure security and is an adjunct faculty member at the University of California, Riverside, USA. He is a member of various organizations including IEEE, a researcher and consultant in security for various major US and UK companies and President of EHSC/CISO in Camarillo, California, USA.