Fuzzy Logic Aided Intelligent Threat Detection in Cisco Adaptive Security Appliance 5500 Series Firewalls

Nitin Naik[1], Paul Jenkins[1], Brian Kerby[1], Joseph Sloane[1] and Longzhi Yang[2]

[1]Defence School of Communications and Information Systems, Ministry of Defence, United Kingdom
[2]Department of Computer and Information Sciences, Northumbria University, United Kingdom
Email: {nitin.naik100, paul.jenkins683, brian.kerby645, joe.sloane486}@mod.gov.uk,
longzhi.yang@northumbria.ac.uk

***Abstract*—Cisco Adaptive Security Appliance (ASA) 5500 Series Firewall is amongst the most popular and technically advanced for securing organisational networks and systems. One of its most valuable features is its threat detection function which is available on every version of the firewall running a software version of 8.0(2) or higher. Threat detection operates at layers 3 and 4 to determine a baseline for network traffic, analysing packet drop statistics and generating threat reports based on traffic patterns. Despite producing a large volume of statistical information relating to several security events, further effort is required to mine and visually report more significant information and conclude the security status of the network. There are several commercial off-the-shelf tools available to undertake this task, however, they are expensive and may require a cloud subscription. Furthermore, if the information transmitted over the network is sensitive or requires confidentiality, the involvement of a third party or a third-party tool may place organisational security at risk. Therefore, this paper presents a fuzzy logic aided intelligent threat detection solution, which is a cost-free, intuitive and comprehensible solution, enhancing and simplifying the threat detection process for all. In particular, it employs a fuzzy reasoning system based on the threat detection statistics, and presents results/threats through a developed dashboard user interface, for ease of understanding for administrators and users. The paper further demonstrates the successful utilisation of a fuzzy reasoning system for selected and prioritised security events in basic threat detection, although it can be extended to encompass more complex situations, such as complete basic threat detection, advanced threat detection, scanning threat detection, and customised feature based threat detection.**

I. Introduction

The global security threat landscape is changing on a daily basis and more than million threats are emerging every day, as reported by Internet security teams at Symantec and Verizon [1]. The security of network infrastructure has become the main priority for any organisation. Amongst the multi-layer security solutions available for network infrastructure, a firewall layer is one of the oldest and primary defences for any network. A firewall monitors network traffic and allows or denies particular traffic based on its set of rules. Cisco Adaptive Security Appliance (ASA) 5500 Series Firewalls are one of the most popular and technically advanced firewalls for securing organisational networks and systems. It includes some of the features of antivirus, Intrusion Prevention System (IPS) and Virtual Private Network (VPN) [2], [3].

One of the most valuable feature of the Cisco ASA Firewall is threat detection that is available on any Cisco ASA Firewall that runs a software version of 8.0(2) or subsequent version. Threat detection operates at layers 3 and 4 to determine a baseline for network traffic, analysing packet drop statistics and generating threat reports based on traffic patterns. Despite producing a large volume of statistical information relating to several security events, the threat detection feature requires additional effort for mining and visual reporting of more significant information to determine the security status of the network. There are several commercial off-the-shelf tools available to mine the firewall log and enhance the threat detection process of the Cisco ASA Firewall. However, they are expensive and may require an additional cloud subscription. Additionally, if the information is sensitive, requiring confidentiality, involving a third party or third-party tool may place organisational security at risk. Therefore, to provide an enhanced threat detection facility requires an effective yet simple reasoning and analysis solution.

The nature of the collected data in security logs may limit the use of some AI techniques for mining and reasoning purposes [4]. Fuzzy logic and reasoning offers an effective and simple rule-based solution for these types of security applications and it is already employed in Windows fuzzy firewall [5], [6], [7], [8] and fuzzy intrusion detection system based on Snort [9], [10], [11], [12]. The success of these fuzzy reasoning systems for security applications provides sufficient empirical evidence for the development of a fuzzy logic aided intelligent threat detection system, for larger organisations, presented in this paper. This fuzzy logic aided intelligent threat detection system is a cost-free and intuitive solution to enhance and simplify the threat detection process. It employs a fuzzy reasoning system which is based on the threat detection statistics and presents results/threats through the developed UI for ease of understanding for firewall administrators/users. The paper demonstrates the successful use of a fuzzy reasoning system for selected and prioritised security events in basic threat detection: Denial by Access Control List (DACL), SYN Attack Detected (SAD) and DoS attack detected (DAD). However, it can be extended to cover complete basic threat detection, advanced threat detection, scanning threat detection and more complex and customised feature based threat detection.

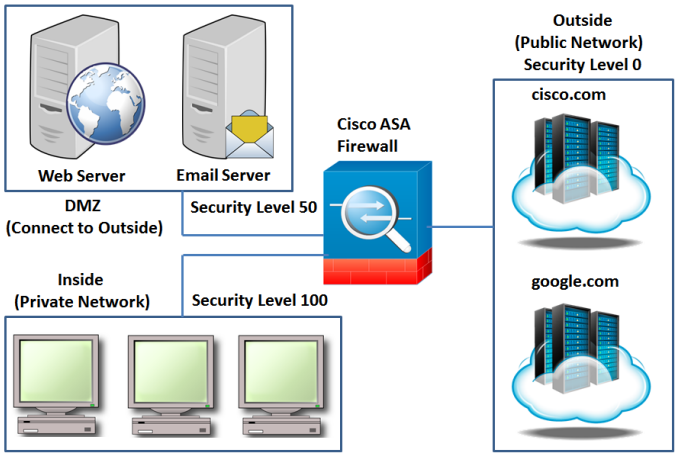

Fig. 1. Structural diagram of the Cisco ASA Firewall illustrating the connectivity of inside, outside and DMZ networks

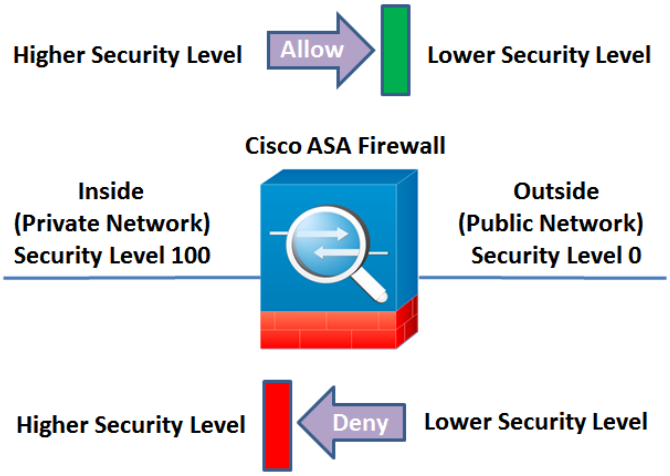

Fig. 2. Cisco ASA security levels and default policies for allowing and denying network traffic

The remaining paper is organised as follows. Section II explains the technical background of Cisco Adaptive Security Appliance - 5500 Series Firewalls, its security levels, threat detection and basic threat detection statistics. Section III describes the complete development process of a fuzzy logic aided intelligent threat detection system which is called FR-CiscoFirewall. Sections IV presents the experimental results of the simulated attacks. Section V reveals some of main limitations of the threat detection process of the Cisco ASA Firewall. Finally, Section VI presents the conclusion and specifies about the future extension of the proposed fuzzy logic aided intelligent threat detection system.

II. Technical Background

A. Cisco Adaptive Security Appliance (ASA) - Cisco ASA 5500 Series Firewalls

A firewall is a security tool that monitors inbound and outbound network traffic and decides whether to allow or deny any particular traffic depending on a defined set of security rules [13]. Cisco ASA 5500 Series Firewall is an advancement over the previous model Cisco PIX 500 Series Firewall, as it includes some of the features of antivirus, Intrusion Prevention Systems (IPS) and Virtual Private Networks (VPN) [2], [3]. Additional security functionality can be added to the Cisco ASA Firewall by employing add-on modules which offer a variety of security features. A typical structural diagram of the Cisco ASA Firewall is shown in Fig. 1, illustrating the connectivity and traffic flow among three different networks namely, Inside, Outside and De-Militarized Zone (DMZ), representing three different security levels. The DMZ or perimeter network, is a purpose-built local network for improving security by isolating Inside (private) and Outside (untrusted) networks and avoiding their direct connectivity. The Cisco ASA Firewall is a cost-effective and flexible security solution for both small and large networks. It has the largest share in the hardware firewall appliance market, compared to other firewall products such as SonicWall, Checkpoint, Juniper Netscreen, WatchGuard [14].

B. Cisco ASA Firewall Security Levels

The Cisco ASA Firewall contains some intrinsic security policies that are based on *Security Levels* (or relative trust). The security levels are assigned to network interfaces and they range from 0 (the least amount of trust) to 100 (the greatest amount of trust) [3]. Consequently, interfaces with higher security levels are considered to be more trusted than interfaces with lower security levels. Usually, the *Inside* interface is assigned the highest security level 100 as it is a private network consisting of all the trusted users. Similarly, the *Outside* interface is assigned with the lowest security level 0, as it is a public network consisting of all untrusted parties. The remaining ASA Firewall interfaces can be assigned any intermediate security level between 1 and 99 depending on the level of their trust/security. The entire network traffic in the Cisco ASA Firewall is subjected to the four default security policy rules unless otherwise modified by the Access Control List (ACL) [15].

1) Traffic flowing from a higher-level security interface to a lower-level security interface is permitted by default (see Fig. 2).
2) Traffic flowing from a lower-level security interface to a higher-level security interface is denied by default (see Fig. 2).
3) Traffic flowing from any interface to any other interface with the same security level is denied by default.
4) Traffic flowing into an interface and then out of the same interface is denied by default.

Therefore, the default rule is that the Cisco ASA Firewall allows packets from a higher (trusted) security interface to a lower (untrusted) security interface without the need for an ACL explicitly allowing the packets.

C. Threat Detection in the Cisco ASA Firewall

The threat detection feature is one of the highlighted features of the Cisco ASA Firewall, utilising the collection of different levels of statistics related to various security threats. Threat Detection feature is available on any Cisco ASA firewall that runs a software version of 8.0(2) or subsequent version. Threat detection statistics can aid a firewall administrator or user to monitor, identify, understand, and stop attacks against the internal network infrastructure. The effective use

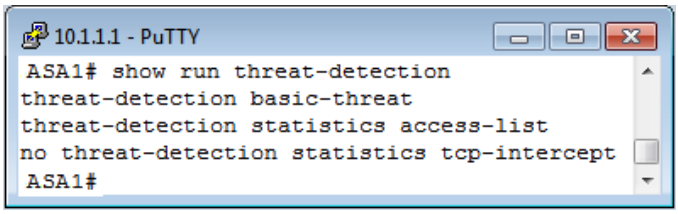

Fig. 3. Default Threat Detection Settings in the Cisco ASA Firewall

of this threat detection feature relies on a number of different triggers and statistics, which may require configuration to mine information intelligently. Threat detection in the Cisco ASA Firewall can be classified into three types: basic threat detection, advanced threat detection and scanning threat detection.

1) Basic Threat Detection: Basic Threat Detection monitors dropped packet rates for various security events and provides information about attack activity for the system as a whole. It measures the drop-rate of each event in a configurable time period in seconds. The process simply logs the traffic and statistics without shunning or blocking it, looking for the signature-based threats which are mostly static in nature. Basic threat detection statistics are enabled by default (see Fig. 3), without affecting the system performance and have no major impact on the performance [16].

2) Advanced Threat Detection: Advanced Threat Detection monitors threat statistics at a granular object level, reporting activities for individual networks, hosts (IPs), ports, protocols, or access control lists. Furthermore, it measures the drop-rate of each event related to a particular object in a configurable time period in seconds. However, similarly to basic threat detection, it only logs the traffic and statistics but does not shun or block it. Advanced threat detection statistics are resource intensive because they retain the track of various statistics in memory [17]. Thus, they are not enabled by default since they can affect the system performance adversely [16]. The exception is the access control list (ACL) statistics, which are enabled by default (see Fig. 3).

3) Scanning Threat Detection: Scanning Threat Detection monitors and maintains the track of suspected attackers who create connections to many hosts in a subnet, or many ports on a host/subnet [17]. Conceptually, it is based on basic threat detection, and therefore, it measures the drop-rate of each event related to a particular attacker in configurable time period in seconds. This type of threat detection can optionally react to an attack by shunning the attacker's IP, therefore, this is the only type of threat detection that can actively affect connections through the Cisco ASA Firewall.

Scanning threat detection statistics are extremely resource intensive because they maintain a database of attackers and target IP addresses that can assist further analysis of the hosts involved in the scan, and therefore, it is disabled by default (see Fig. 3).

D. Basic Threat Detection Statistics in the Cisco ASA Firewall

Basic threat detection statistics are enabled by default in which the rate of dropped packets are monitored due to the following security events [16], [17]:

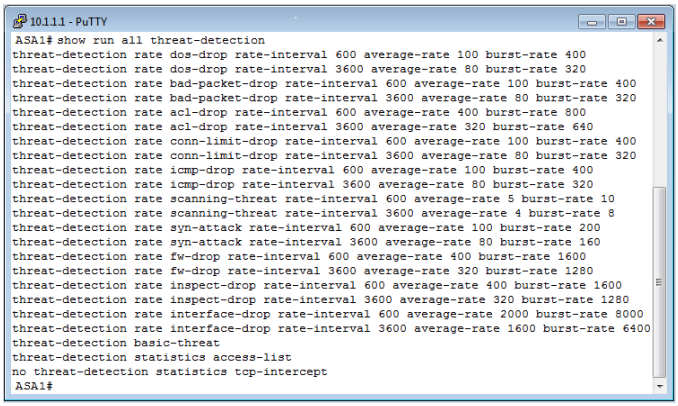

Fig. 4. Default Basic Threat Detection Statistics for 10 minutes (600 seconds) and 60 minutes (3600 seconds)

- Denial by Access Control List (ACL)
- Bad Packet Format
- Exceeded Connection Limits
- Denial of Service (DoS) Attack Detection
- Basic Firewall Check Failure
- Suspicious ICMP Packets Exceeded
- Application Inspection Packet Failure
- Interface Overload
- Scanning Attack Detection
- SYN Attack (Incomplete Session) Detection

When any of these threats are detected by the Cisco ASA Firewall, a syslog message will be generated on the device (and the external *syslog* server, if configured). For each security event, basic threat detection measures the drop-rate of that event in a configurable time period in seconds, which is called the average rate interval (ARI) and can be in the range from 600 seconds to 30 days (see Fig. 4). If the total number of security events occurred within the ARI exceeds the configured rate thresholds, then the Cisco ASA Firewall considers these events a threat [17].

There are two configurable thresholds for basic threat detection when it considers security events to be a threat: the *average rate* and the *burst rate* (see Fig. 4). The *average rate* is the average number of drops/second within the configured ARI. The *burst rate* is normally 1/30th of the *average rate* or 10 seconds, whichever is higher. Each time these limits are exceeded and a basic threat is detected, the ASA Firewall generates a *syslog* message *%ASA-4-733100* to alert the administrator/user that a potential threat has been identified [17]. The two separate *syslog* messages will be generated in case of both the *average rate* and the *burst rate* being exceeded, with a maximum of one message for each rate type per burst period. Normally, basic threat detection does not affect the performance, except only when there are significant drops or potential threats.

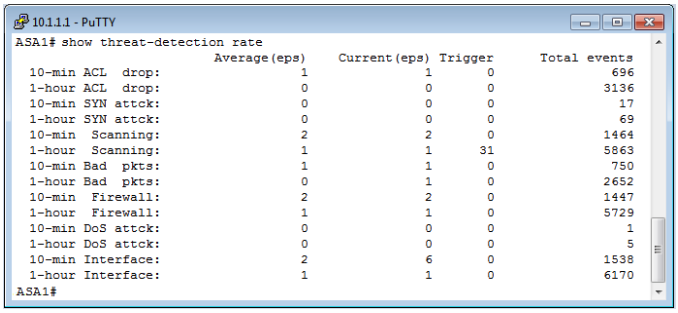

Fig. 5. Collected Basic Threat Detection Statistics for 10 minutes (600 seconds) and 60 minutes (3600 seconds)

III. Development of Fuzzy Logic Aided Intelligent Threat Detection

A. Requirements for Fuzzy Logic Aided Intelligent Threat Detection

Basic threat detection statistics provides significant and timely information about several security events (see Fig. 5). These can aid administrators/users to protect their ASA Firewall and networks from various security threats. However, it generates merely the raw data which requires mining to gain insight of security status of the network. The mining necessitates a good understanding of the detailed information, relative analysis of various security events and intelligently linking and presenting them for the system as a whole. To achieve the full understanding of the threat, all these activities require further processing or sophisticated tools to accomplish this task. There are several commercial off-the-shelf (COTS) tools available to accomplish the above tasks by mining the firewall log and enhance the Cisco ASA Firewall threat detection process and its analysis for securing the network. These tools are expensive and may require an additional cloud subscription. Furthermore, if the information is sensitive then involving a third party or a third-party tool may place organisational security at risk. Therefore, this paper has identified several requirements for designing this fuzzy logic aided intelligent threat detection system:

- Requires a mechanism to analyse the recorded logs in the basic threat detection process
- Requires relative analysis of various security events for the system as a whole
- Requires the prioritization of security events according to the organisational requirements
- Requires an automatic and real-time update of network traffic for timely actions
- Requires visual presentation of results/threats for easy understanding for everyone
- Requires the same performance level with additional and intelligent features in threat detection
- Requires a cost-free solution without involving third party tool to avoid any security risks
- Requires a simple reasoning solution for all the above requirements such as fuzzy reasoning which allows for a closer imitation of human reasoning [18]

B. Data Analysis and Fuzzy Variables

In this design, only three threat detection statistics are considered and prioritised for the development of a fuzzy logic aided intelligent threat detection system: Denial by Access Control List (DACL), SYN Attack Detected (SAD) and DoS Attack Detected (DAD). The further analysis and determination of fuzzy variables are based on these three selected parameters and their default settings of the *average rate* and *burst rate*, which are given in Table I. To obtain normalised and symmetrical values of the *average rate* and *burst rate* for the same time period (here 20 seconds), the *average rate* for these parameters is computed for the period of 20 seconds. In addition, the fuzzy logic aided intelligent threat detection system can monitor and analyse both average rate and burst rate after every 20 seconds continuously. Furthermore, the total number of threat detection statistics and their values can be customised depending on the requirements of an organisation or even an individual network.

TABLE I. Default Settings of Basic Threat Detection Statistics in Cisco ASA Firewalls [16]

Types of Attack	**Threat Detection Trigger Settings**	
Packet Drop Reasons	**Average Rate**	**Burst Rate**
Denial by Access Control List (ACL)	400 drops/second over the last 600 seconds.	800 drops/second over the last 20 second period.
SYN Attack Detected (TCP SYN incomplete sessions)	100 drops/second over the last 600 seconds.	200 drops/second over the last 20 second period.
Denial of Service (DoS) Attack Detected	100 drops/second over the last 600 seconds.	400 drops/second over the last 20 second period.

1) Denial by Access Control List (DACL): As previously mentioned in Table I, the default average rate for denial by access control list is 400 drops/second over the last 600 seconds, and the burst rate for denial by access control list is 800 drops/second over the last 20 second period. For further analysis and design purposes, it is necessary to normalise both values over the period of 20 seconds, therefore, the average rate computed for 20 seconds is around 14 drops/second. These two values (average rate = 14 drops/second and burst rate = 800 drops/second) over the period of 20 seconds, provide the range (14-800 drops/second) for the first fuzzy input variable DACL. Based on the detailed analysis and experiments, the fuzzy input variable - DACL is divided into three fuzzy sets: Low, Medium and High, attack categories with their corresponding ranges 14-335 drops/second, 250-570 drops/second and 480-800 drops/second respectively. Above 800 drops/second (the burst rate), a firewall administrator can decide the appropriate actions to take in advance to stop the attack. The Matlab design of this fuzzy input variable DACL is shown in Fig. 6, where fuzzy sets are chosen as a triangular membership function for this fuzzy input variable.

2) SYN Attack Detected (SAD): Similarly, the statistics of SYN attack detected are given in Table I, where, the default average rate for SYN attack detected is 100 drops/second over the last 600 seconds, and the burst rate for SYN attack detected is 200 drops/second over the last 20 second period. Again, for further analysis and design purposes, it is necessary

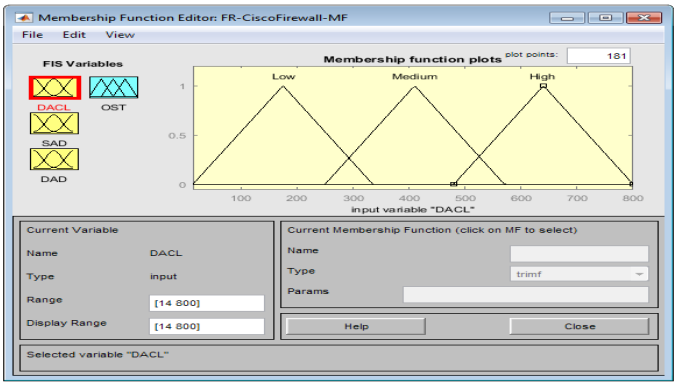

Fig. 6. Fuzzy input variable DACL and its fuzzy sets

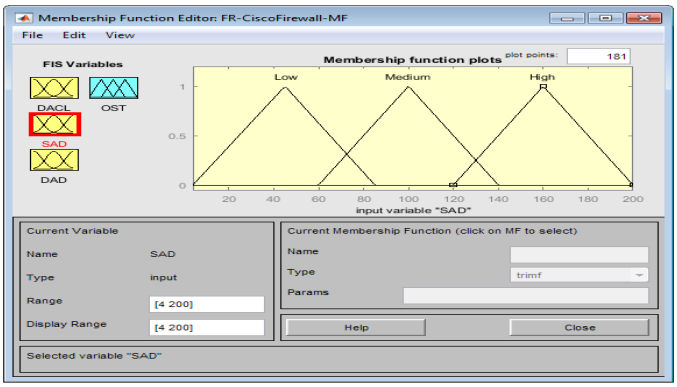

Fig. 7. Fuzzy input variable SAD and its fuzzy sets

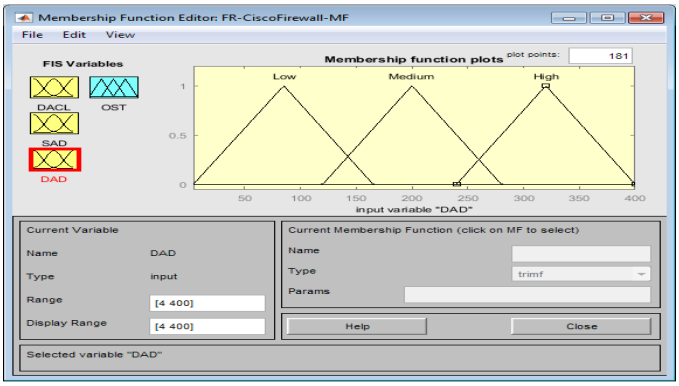

Fig. 8. Fuzzy input variable DAD and its fuzzy sets

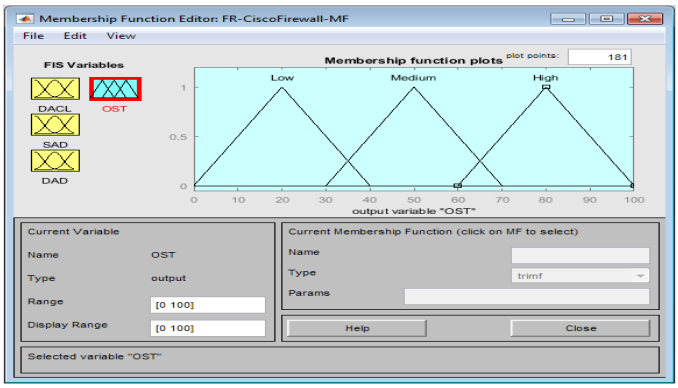

Fig. 9. Fuzzy output variable OST and its fuzzy sets

to normalise both values over the period of 20 seconds, therefore, the average rate computed for 20 seconds is around 4 drops/second. Now these two values (average rate = 4 drops/second and burst rate = 200 drops/second) over the period of 20 seconds, provide the range (4-200 drops/second) for the second fuzzy input variable SAD. Based on the detailed analysis and experiments, this fuzzy input variable - SAD is divided into three fuzzy sets: Low, Medium and High attack categories with their corresponding ranges 4-85 drops/second, 60-140 drops/second and 120-200 drops/second respectively. Above 200 drops/second (the burst rate), a firewall administrator can decide the appropriate action to take in advance, to stop the attack. The Matlab design of this second fuzzy input variable SAD is shown in Fig. 7, where fuzzy sets are chosen as a triangular membership function for this fuzzy input variable.

3) DoS Attack Detected (DAD): Finally, the statistics of DoS attack detected are given in Table I, where, the default average rate for DoS attack detected is 100 drops/second over the last 600 seconds, and the burst rate for DoS attack detected is 400 drops/second over the last 20 second period. Again, for further analysis and design purposes, normalising both values over the period of 20 seconds, the average rate computed for 20 seconds is approximately 4 drops/second. These two values (average rate = 4 drops/second and burst rate = 400 drops/second) over the period of 20 seconds, provide the range (4-400 drops/second) for the third fuzzy input variable DAD. Based on the detailed analysis and experiments, this fuzzy input variable - DAD is divided into three fuzzy sets: Low, Medium and High attack categories with their corresponding ranges 4-165 drops/second, 120-280 drops/second and 240-400 drops/second respectively. Above 400 drops/second (the burst rate), a firewall administrator can decide the appropriate actions in advance to stop the attack. The Matlab design of this third fuzzy input variable DAD is shown in Fig. 8, where fuzzy sets are chosen as a triangular membership function for this fuzzy input variable.

4) Overall Security Threat (OST): Based on the above three fuzzy input variables DACL, SAD and DAD, the overall security threat (OST) to the ASA Firewall and network is determined for the fuzzy logic aided intelligent threat detection system. The OST is represented as a percentage and its entire range (1-100%) is also divided into three fuzzy sets: Low, Medium and High attack categories with their corresponding ranges 1-40%, 30-70% and 60-100% respectively. The Matlab design of this fuzzy output variable OST is shown in Fig. 9, where fuzzy sets are also chosen as a triangular membership function for this fuzzy output variable.

C. Fuzzy Rule Base and Fuzzy Reasoning System

The three input and output variables described in the previous subsection and their corresponding value ranges are utilised in the development of a fuzzy reasoning system (based on Mamdani's inference [19]) as shown in Fig. 10. The total 27 fuzzy rules are educed based on the three chosen fuzzy input variables, which is shown in Fig. 11. Finally, the fully developed fuzzy rule base is obtained for reasoning purposes,

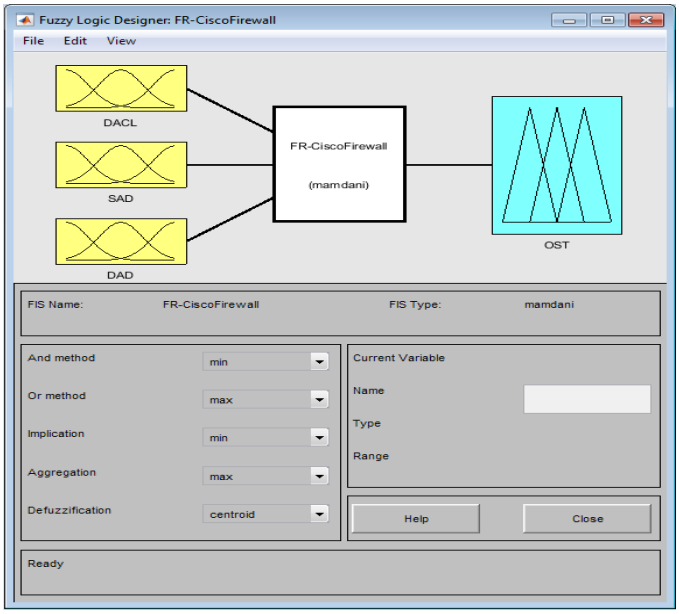

Fig. 10. Fuzzy reasoning system consisting of input and output variables for the fuzzy logic aided intelligent threat detection system - FR-CiscoFirewall

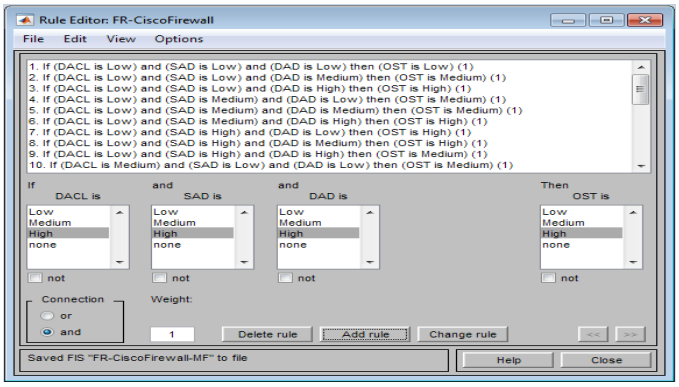

Fig. 11. Fuzzy rules for the fuzzy logic aided intelligent threat detection system - FR-CiscoFirewall

which is shown in Fig. 12. The development of this fuzzy rule base and fuzzy reasoning system provides additional intelligence to the threat detection process of the Cisco ASA Firewall and thus, creates an intelligent threat detection system as shown in Fig. 13.

IV. Experimental Results

This section illustrates the experimental results for a fuzzy logic aided intelligent threat detection system, FR-CiscoFirewall based on a number of simulated threat conditions and compares them with the outputs of a standard Cisco ASA Firewall. Firstly, Table II shows the threat detection outputs for simulated threat conditions by the standard Cisco ASA Firewall, where it only generates the standard *syslog* message- *%ASA-4-733100* for every individual threat because all drop rates are above the *average rate* for the corresponding security events DACL, SAD and DAD. This is the default configuration for the Cisco ASA Firewall's threat detection engine, however, reading numerous *syslog* messages- *%ASA-4-733100* in the very large *syslog* file is a tedious task and

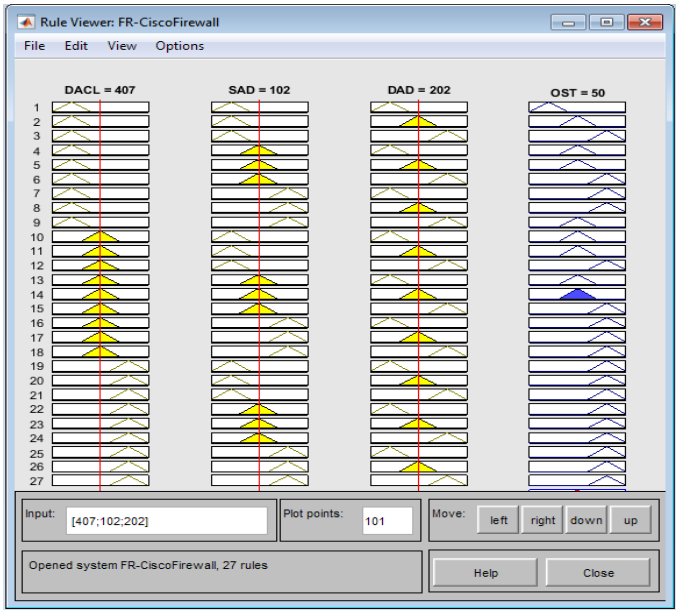

Fig. 12. Fuzzy rule base forthe fuzzy logic aided intelligent threat detection system - FR-CiscoFirewall

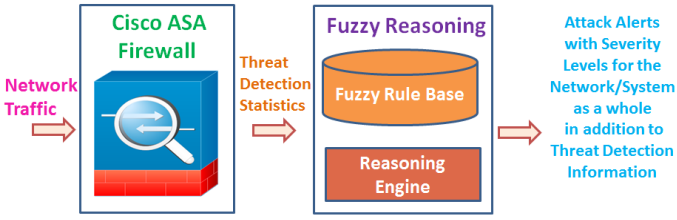

Fig. 13. Block diagram of the fuzzy logic aided intelligent threat detection system - FR-CiscoFirewall

requires networking expertise for the analysis. Despite this, it does not provide the relative analysis of various security events and cannot conclude or inform the overall threat for the system as a whole.

Table III shows the threat detection outputs for the similar simulated threat conditions by the developed fuzzy logic aided intelligent threat detection system - FR-CiscoFirewall, where it generates additional threat alerts with their severity based on the fuzzy reasoning system, alongside that of the standard *syslog* message- *%ASA-4-733100*. The results of FR-CiscoFirewall indicates that it generates simplified results of the threat analysis related to the individual security event and for the complete network, whereas this is not possible in the standard Cisco ASA Firewall. Furthermore, all the threat alerts are reported visually on the host through the FR-CiscoFirewall dashboard user interface as shown in Figs. 14 to 17. Evidently, visually reported results are processed quicker and are easily understandable to any firewall administrator/user. Based on the severity of the threat alert, a network administrator or user can apply the pre-decided strategy or decide the next course of action to protect the network from further attacks such as shun the attacker or immediately shut down the host/network until the investigation is carried out.

This experimental simulation using the fuzzy reasoning system demonstrates the effective working of the fuzzy logic

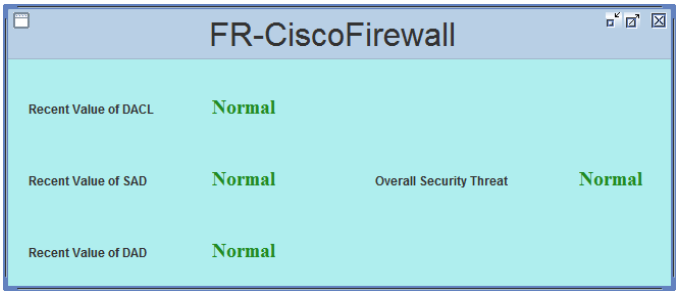

Fig. 14. FR-CiscoFirewall dashboard reporting overall security threat is Normal

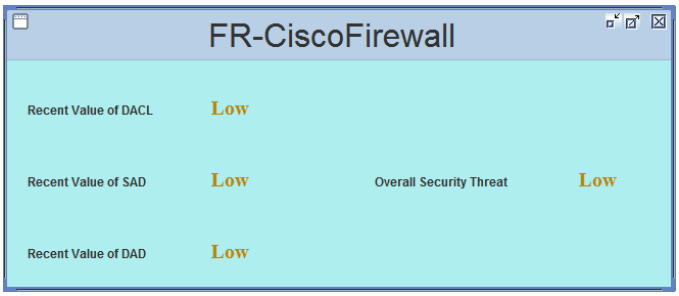

Fig. 15. FR-CiscoFirewall dashboard reporting overall security threat is Low

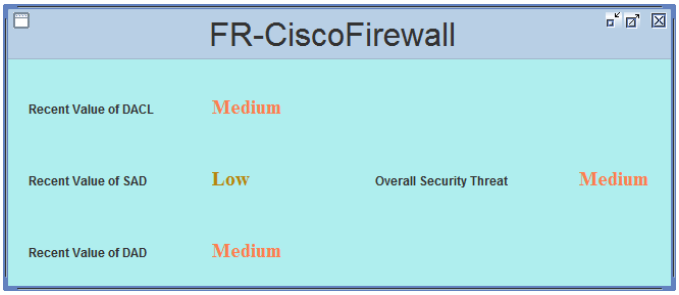

Fig. 16. FR-CiscoFirewall dashboard reporting overall security threat is Medium

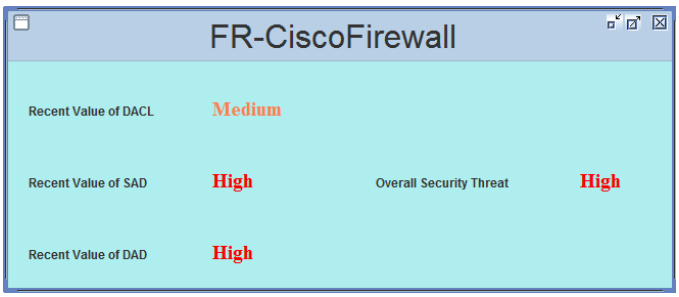

Fig. 17. FR-CiscoFirewall dashboard reporting overall security threat is High

aided intelligent threat detection system, FR-CiscoFirewall based on the three selected and prioritised attack categories Denial by Access Control List (DACL), SYN Attack Detected (SAD) and DoS Attack Detected (DAD). This approach can readily be customised for other types of security events in basic threat detection, such as scanning attack detection, exceeded connection limits, basic firewall check failure, application inspection packet failure and suspicious ICMP packets exceeded; depending on the priority of events for a particular organisation. Additionally, an organisation is able to further refine this system based upon their specific security events and performance efficiencies, thus providing the organisation with the optimum defence.

TABLE II. CISCO ASA FIREWALL THREAT DETECTION OUTPUTS FOR THE OVERALL SECURITY THREAT IN THE NETWORK

Obs. No.	Cisco ASA Firewall			
	Input Parameters			Output Parameter
	DACL Rate	SAD Rate	DAD Rate	Syslog Message
1	85	43	105	*%ASA-4-733100*
2	257	77	193	*%ASA-4-733100*
3	463	169	336	*%ASA-4-733100*
4	627	153	209	*%ASA-4-733100*
5	212	59	119	*%ASA-4-733100*
6	241	117	108	*%ASA-4-733100*

V. LIMITATIONS OF CISCO ASA FIREWALL THREAT DETECTION

Threat detection is an additional and powerful feature of the Cisco ASA Firewall and it offers some of the features of an IPS. This makes the Cisco ASA Firewall a unique and superior security tool in comparison to other commercial firewalls of the same capacity. However, before using the threat detection features, it is important to note that it has a few limitations:

- Threat Detection can only be used on any Cisco ASA Firewall that runs a software version of 8.0(2) or subsequent version.
- While threat detection is not a replacement for an exclusive IPS, it can still be employed in networks, where an IPS is unaffordable, to deliver an additional layer of defence [17].
- Threat detection is not supported on the Cisco ASA 1000V Cloud Firewall.
- Threat Detection is only supported in single context mode but not in a multiple context mode.
- Threat detection monitors only ”through-the-box” but not ”to-the-box” traffic.
- All the TCP connection attempts which are reset by the targeted server is not counted as a SYN attack or Scanning threat [17].

VI. CONCLUSION

This paper presented the fuzzy logic aided intelligent threat detection system to enhance and simplify the threat detection process of Cisco Adaptive Security Appliance (ASA) 5500 Series Firewalls for everyone. The proposed system employed a fuzzy reasoning system which was based on the threat detection statistics and the presented results/threats, through to the developed dashboard user interface for ease of understanding for administrators/users. The paper has demonstrated the successful use of a fuzzy reasoning system for selected and prioritised security events in basic threat detection: Denial by Access Control List (DACL), SYN Attack Detected (SAD)

TABLE III. FUZZY LOGIC AIDED INTELLIGENT THREAT DETECTION OUTPUTS FOR THE OVERALL SECURITY THREAT IN THE NETWORK

Obs. No.	FR-CiscoFirewall			
	Input Parameters			Output Parameter
	DACL Rate	SAD Rate	DAD Rate	OST Rate
1	85	43	105	Security Threat is LOW
2	257	77	193	Security Threat is MEDIUM
3	463	169	336	Security Threat is HIGH
4	627	153	209	Security Threat is HIGH
5	212	59	119	Security Threat is LOW
6	241	117	108	Security Threat is MEDIUM

and DoS Attack Detected (DAD). However, depending on the requirements of an organisation or even an individual network, the proposed fuzzy logic aided intelligent threat detection system can be extended to cover complete basic threat detection, advanced threat detection, scanning threat detection. Furthermore, a more complex and customised threat detection system can be designed depending upon an organisation's requirements. In the future, it is essential to implement the aforementioned threat detection categories for testing the wider acceptability of the proposed approach with the Cisco ASA Firewall. Additionally, based on the Dynamic Fuzzy Rule Interpolation (D-FRI) framework [20], [21], [22], [23], [24] and adaptive FRI [25], [26], [27], [28], this proposed system can be made adaptive system in the future.

REFERENCES

[1] V. Harrison and J. Pagliery. (2015) Nearly 1 million new malware threats released every day. [Online]. Available: http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html

[2] J. Frahim, O. Santos, and A. Ossipov, *Cisco ASA: all-in-one firewall, IPS, and VPN adaptive security appliance*. Pearson Education, 2014.

[3] Cisco.com. (2010) Cisco ASA 5500 Series Configuration Guide using the CLI. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config.pdf

[4] N. Naik, P. Jenkins, N. Savage, and V. Katos, "Big data security analysis approach using computational intelligence techniques in R for desktop users," in *IEEE Symposium Series on Computational Intelligence (SSCI)*, 2016.

[5] N. Naik and P. Jenkins, "Fuzzy reasoning based windows firewall for preventing denial of service attack," in *IEEE International Conference on Fuzzy Systems*, 2016, pp. 759–766.

[6] ——, "Enhancing windows firewall security using fuzzy reasoning," in *IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2016, pp. 263–269.

[7] N. Naik, P. Jenkins, R. Cooke, D. Ball, A. Foster, and Y. Jin, "Augmented windows fuzzy firewall for preventing denial of service attack," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE, 2017, pp. 1–6.

[8] N. Naik, R. Diao, C. Shang, Q. Shen, and P. Jenkins, "D-FRI-WinFirewall: Dynamic fuzzy rule interpolation for windows firewall," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*. IEEE, 2017, pp. 1–6.

[9] N. Naik, "Fuzzy inference based intrusion detection system: FI-Snort," in *IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2015, pp. 2062–2067.

[10] N. Naik, R. Diao, and Q. Shen, "Application of dynamic fuzzy rule interpolation for intrusion detection: D-FRI-Snort," in *IEEE International Conference on Fuzzy Systems*, 2016, pp. 78–85.

[11] ——, "Dynamic fuzzy rule interpolation and its application to intrusion detection," *IEEE Transactions on Fuzzy Systems*, 2017.

[12] L. Yang, J. Li, G. Fehringer, P. Barraclough, G. Sexton, and Y. Cao, "Intrusion detection system by fuzzy interpolation," in *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2017, pp. 1–6.

[13] Cisco.com. (2018) What is a Firewal ? [Online]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[14] Cxtec.com. (2018) What is the Cisco ASA? [Online]. Available: https://www.cxtec.com/resources/blog/what-is-cisco-asa-security-appliance/

[15] Cisco.com. (2017) Chapter 1 : Configuring Service Policy Rules on Firewall Devices. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-2/user/guide/CSMUserGuide_wrapper/pxservrules.pdf

[16] ——. (2010) Chapter 50 : Configuring Threat Detection. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/conns_threat.pdf

[17] ——. (2015) ASA Threat Detection Functionality and Configuration. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html

[18] L. A. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[19] E. H. Mamdani and S. Assilina, "An experiment in linguistic synthesis with a fuzzy logic controller," *International Journal of Man-Machine Studies*, vol. 7, no. 1, pp. 1–13, 1975.

[20] N. Naik, P. Su, and Q. Shen, "Integration of interpolation and inference," in *UK Workshop on Computational Intelligence*, 2012, pp. 1–7.

[21] N. Naik, "Dynamic Fuzzy Rule Interpolation," Ph.D. dissertation, Department of Computer Science, Institute of Mathematics, Physics and Computer Science, Aberystwyth University, UK, 2015.

[22] N. Naik, R. Diao, C. Quek, and Q. Shen, "Towards dynamic fuzzy rule interpolation," in *IEEE International Conference on Fuzzy Systems*, 2013, pp. 1–7.

[23] N. Naik, R. Diao, and Q. Shen, "Genetic algorithm-aided dynamic fuzzy rule interpolation," in *IEEE International Conference on Fuzzy Systems*, 2014, pp. 2198–2205.

[24] ——, "Choice of effective fitness functions for genetic algorithm-aided dynamic fuzzy rule interpolation," in *IEEE International Conference on Fuzzy Systems*, 2015, pp. 1–8.

[25] L. Yang and Q. Shen, "Adaptive fuzzy interpolation," *IEEE Transactions on Fuzzy Systems*, vol. 19, no. 6, pp. 1107–1126, 2011.

[26] ——, "Closed form fuzzy interpolation," *Fuzzy Sets and Systems*, vol. 225, pp. 1–22, 2013.

[27] L. Yang, F. Chao, and Q. Shen, "Generalized adaptive fuzzy rule interpolation," *IEEE Transactions on Fuzzy Systems*, vol. 25, no. 4, pp. 839–853, 2017.

[28] J. Li, L. Yang, X. Fu, F. Chao, and Y. Qu, "Dynamic QoS solution for enterprise networks using tsk fuzzy interpolation," in *Fuzzy Systems (FUZZ-IEEE), 2017 IEEE International Conference on*. IEEE, 2017, pp. 1–6.