D-FRI-CiscoFirewall

Naik, Nitin Kumar; Shang, Changjing; Shen, Qiang; Jenkins, Paul

Published in:
2019 IEEE International Conference on Fuzzy Systems

DOI:
10.1109/FUZZ-IEEE.2019.8858999

Publication date:
2019

Citation for published version (APA):
Naik, N. K., Shang, C., Shen, Q., & Jenkins, P. (2019). D-FRI-CiscoFirewall: Dynamic Fuzzy Rule Interpolation for Cisco ASA Firewall. In *2019 IEEE International Conference on Fuzzy Systems: FUZZ-IEEE* Article 8858999 (IEEE International Conference on Fuzzy Systems; Vol. 2019). IEEE Press. https://doi.org/10.1109/FUZZ-IEEE.2019.8858999

D-FRI-CiscoFirewall: Dynamic Fuzzy Rule Interpolation for Cisco ASA Firewall

Nitin Naik[1], Changjing Shang[2], Qiang Shen[2] and Paul Jenkins[1]

[1]Defence School of Communications and Information Systems, Ministry of Defence, UK
[2]Dept. of Computer Science, Faculty of Business and Physical Sciences, Aberystwyth University, UK
Email: nitin.naik100@mod.gov.uk, cns@aber.ac.uk, qqs@aber.ac.uk, paul.jenkins683@mod.gov.uk

***Abstract*—Dynamic fuzzy rule interpolation (D-FRI) enhances the accuracy of sparse rule-based fuzzy reasoning via efficiently exploiting fuzzy rule interpolation to produce dynamic rules. Owing to its adaptive nature in delivering a dynamic rule base, it is particularly useful for those systems which experience frequent changes. Network security is one such area where frequent changes are quite likely due to changing network conditions and traffic. Thus, D-FRI has the potential to offer an optimised and adaptive approach for improving network security. The popular Cisco Adaptive Security Appliance (ASA) Firewall is capable of monitoring and alerting a range of common threats, by baselining the traffic of a network and analysing the statistics of dropped packets. An ASA process yields a large volume of statistical information relating to certain security events. Yet, threat detection is a rudimentary function since additional intelligence is required to automate the extraction of meaningful information for alerting the users. This could be achieved using expensive automated tools offered by a third party, but doing so may unnecessarily expose an organisation to other security threats. This paper takes a different approach, presenting a D-FRI-CiscoFirewall in support of automated threat detection for Cisco ASA Firewall. Through utilising threat detection statistics, the approach can customise the detection process according to organisational requirements. It performs the relative analysis of prioritised security events and is able to predict comprehensive security situations while no matching rules are available. In particular, the approach supports the creation of a dynamic rule base, derived from changing network conditions and traffic density. Its efficacy is demonstrated by experimental evaluations.**

I. Introduction

The success of fuzzy inference to a large extent relies on the rule base and its coverage of the problem domain. Accurate inference results can be obtained using fuzzy inference if the rule base contains a significant number of rules to cover the entire problem domain. Fuzzy rule interpolation (FRI) based reasoning offers an effective approach to perform inferences when no rules can be found that match a certain given observation. However, it generally incurs more computational overheads. The chances of running fuzzy inference directly, by firing any existing rules, or performing interpolation to derive reasoned results depend on the pertinent rule base. Most fuzzy rule bases have no mechanism to update their rules and their static nature makes them unproductive over time. Dynamic Fuzzy Rule Interpolation (D-FRI) has been developed to successfully address this problem, by providing a dynamic rule base in an attempt to produce more accurate reasoning results [1].

Today, cyber infrastructure is considered to be the greatest asset for many organisations and therefore, its defence is the main focus. To this end, organisations employ defence mechanisms, including firewalls forming the primary requirement for every network and every system. The Cisco Adaptive Security Appliance (ASA) Firewall is popularly used as a network firewall by enterprises; it offers advanced functionality for threat detection and alerts on a number of common threats [2]. Threat detection is achieved by baselining the traffic of a given network and successively analysing the statistics of dropped packets [3]. This feature is an added advantage for the Cisco ASA Firewall users because it yields a large volume of statistical information regarding security events that can be used for further analysis [4]. However, threat detection is a rudimentary function requiring additional intelligence to automate the extraction of meaningful information for the users. Whilst this could be achieved using expensive and automated tools offered by a third party, it may unnecessarily expose an organisation to other security threats.

This problem can be resolved by developing a small add-on for the Cisco ASA Firewall to extract useful information and present it in a user-friendly way. Following the idea that was exploited to strengthen the capability of the Windows Firewall, as per the work on D-FRI-WinFirewall [5], in conjunction with the initial investigation of [6], this paper proposes a further application of D-FRI for the Cisco ASA Firewall, developing a D-FRI-CiscoFirewall for automated threat detection. The proposed approach utilises the statistics gained over the process of threat detection and can be customised with respect to organisational requirements. It performs the relative analysis of prioritised security events and predicts comprehensive security conditions even when no matching rules are found. It produces a dynamic rule base according to the changing network conditions and traffic in an effort to perform more accurate detection. This is demonstrated by the use of comparative experimental results. It is also shown that the D-FRI-CiscoFirewall can be readily modified to cover certain severe threats specific to a given organisation.

This paper consists of the following sections: Section II explains the D-FRI approach, the Cisco ASA Firewall, its default security policy, threat detection and basic threat detection statistics. Section III describes the design and implementation of the D-FRI-CiscoFirewall. Sections IV presents comparative experimental results of the D-FRI-CiscoFirewall, based on simulated attacks. Finally, Section V concludes the work and discusses future extensions of the proposed D-FRI-CiscoFirewall.

II. Background

A. Dynamic Fuzzy Rule Interpolation (D-FRI)

Fuzzy rule firing-based inference is powerful with a dense rule base while fuzzy rule interpolation is effective with a sparse rule base. They can be combined to achieve improved reasoning by working together while dealing with a sparse rule base. Such a combined system is particularly beneficial for applications where it is difficult to design and maintain a dense rule base such as network security [5]. Despite its potential effectiveness, the problem of a static rule base remains, which forms a challenge in its application in continuous adaptation scenarios. D-FRI offers an effective solution for this problem by entailing a concurrent rule base according to the current requirements of the application area [1].

The integration of fuzzy rule-firing, fuzzy rule interpolation and dynamism leads to the development of a dynamic and intelligent approach for fuzzy reasoning that works for sparse rule bases. This is well-suited for network security applications where the perpetual changes in the network conditions and traffic are unavoidable. In the implementation presented herein, Mamdani's fuzzy inference [7] and transformation-based rule interpolation (T-FRI) [8] are employed. The working procedure of D-FRI is outlined in Fig. 1 and its elaboration can be found in [1].

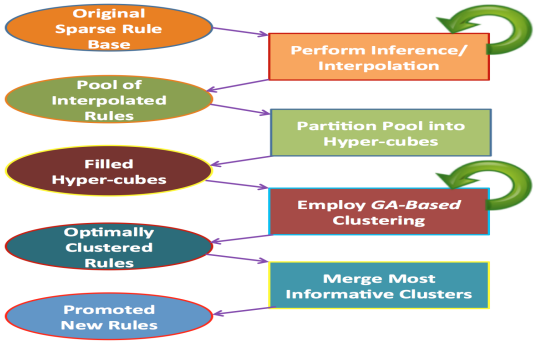

Fig. 1. Dynamic Fuzzy Rule Interpolation (D-FRI) [1]

B. Cisco ASA Firewall and Default Security Policy

The Cisco ASA Firewall is a security device used to monitor network traffic in order to allow or deny network access based on given security rules [3]. Add-on modules may be included to provide additional security functionalities. A flow diagram for the Cisco ASA Firewall is shown in Fig. 2, displaying the connectivity and flow of traffic among three separate networks, namely Inside, Outside and De-Militarized Zone (DMZ). DMZ is a consciously designed local network to improve the security by separating the Inside (private) and Outside (untrusted) networks and obviating any direct connectivity between them.

The basic security policy of the Cisco ASA Firewall depends on the relative trust known as *Security Levels*. These security levels are numbered from 0 to 100, where level 0 is used for the least trusted network and level 100 for the highest trusted [9]. The default settings on the Cisco ASA Firewall is level 0 for the public network and level 100 for the private network. Any other network can be assigned a level number depending on its trust level. The complete traffic flow in the

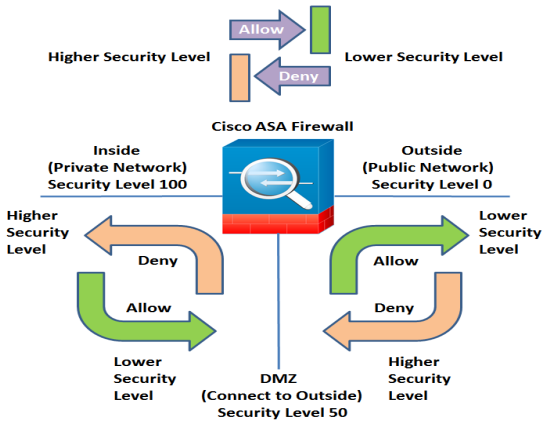

Fig. 2. Traffic flow in Cisco ASA Firewall and default security policies

Cisco ASA Firewall is controlled by the following four default rules of security policy [9]:

- Traffic flow is permitted from a higher-level security interface to a lower-level security interface.
- Traffic flow is denied from a lower-level security interface to a higher-level security interface.
- Traffic flow is denied from any interface to any other interface with the same security level.
- Traffic flowing into an interface and then out of the same interface is denied by default.

These default policy rules can be modified by the use of an Access Control List (ACL) [9]. Based on such default rules, traffic flow is automatically allowed from a higher level to a lower level without changing any settings or writing rules.

C. Threat Detection with Cisco ASA Firewall

The Cisco ASA Firewall threat detection function is available on firewall software version of 8.0(2) or later [2]. Threat detection statistics helps a firewall user to monitor, detect, understand, and prevent attacks against a certain network. It can be divided into following three categories:

1) Basic Threat Detection: It observes dropped packet rates for different security events and presents information about possible threat activities over the entirety of a given network/system. It calculates the drop-rate of every security event for a defined time period. Such a detection process records the traffic and statistics for finding static and signature-based threats, but does not block or prevent the system from them. This feature is enabled by default (see Fig. 3), and does not affect the overall system performance significantly [2].

2) Advanced Threat Detection: It observes threat activities and statistics for a particular object such as one of the access control lists, protocols, ports, hosts (IPs), and specific networks. It also calculates the drop-rate of every security event related to a particular object for a defined time period. Such a detection process records the traffic and statistics, but does not block or prevent the system from them. It is a resource intensive process due to the need to maintain the track of different statistics in memory [4]. Therefore, this feature is not enabled by default, as it may affect the system performance adversely [2], except that the access control list (ACL) statistics is enabled by default (see Fig. 3).

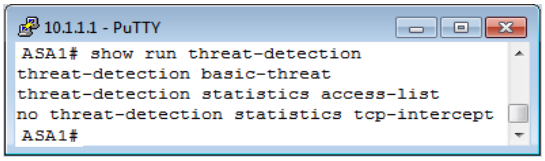

Fig. 3. Default settings of threat detection in Cisco ASA Firewall

3) Scanning Threat Detection: It observes and maintains only the track of suspicious attackers who may establish connections to several hosts in a subnet, or several ports on a host machine [4]. It may be seen as a specific basic threat detection process for a target attacker and thus, it calculates the drop-rate of every security event related to a particular attacker for a defined time period. Scanning threat detection is the only process which not only records the traffic and statistics but also blocks or prevents the system from them. It is also a resource intensive process due to the maintenance of a database of attackers and target IP addresses [4]. Therefore, this feature is not enabled by default (see Fig. 3), as it may also affect the system performance adversely [2].

D. Basic Threat Detection Statistics in Cisco ASA Firewall

In the Cisco ASA Firewall, basic threat detection statistics is enabled automatically, where the rate of dropped packets is monitored regarding the following security events [2], [4]:

1) Drop due to ACL
2) Drop due to Bad Packet Format
3) Drop due to Exceeded Connection Limits
4) Drop due to Denial of Service (DOS)
5) Drop due to Basic Firewall Check Failure
6) Drop due to Suspicious ICMP Packets Exceeded
7) Drop due to Application Inspection Packet Failure
8) Drop due to Interface Overload
9) Drop due to Scanning Attack
10) Drop due to SYN Attack (Incomplete Session)

The Cisco ASA Firewall generates a *syslog* message when it detects any basic threat given in the above list. It calculates and records the drop-rate of each security event for a defined time period. Such a period is known as the Average Rate Interval (ARI), taking values from the range of 600 seconds to 30 days (see Fig. 4). The Cisco ASA Firewall reflects any event as a threat when it exceeds the configured threshold rate in ARI [4]. The configurable thresholds are of two types: *average rate* and *burst rate* (again, see Fig. 4). The former is the average number of dropped packets per second in the configured ARI, and the latter is usually 1/30th of the *average rate* or 10 seconds, whichever is greater. A basic threat is detected whenever any threshold limit is surpassed, and as a result, the ASA Firewall alerts the administrator by generating a *syslog* message *%ASA-4-733100* [4].

III. Design and Implementation

The D-FRI-CiscoFirewall is designed as shown in Fig. 5, which contains three components: the Cisco ASA Firewall, a fuzzy inference system and a D-FRI system. This design is dependent on basic threat detection statistics, as explained in the preceding section. As an initial work, only three security events are herein considered and prioritised: drop due to

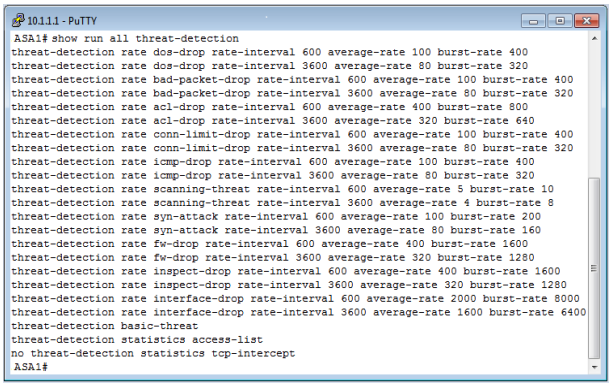

Fig. 4. Default settings of basic threat detection statistics for 10 minutes (600 seconds) and 60 minutes (3600 seconds)

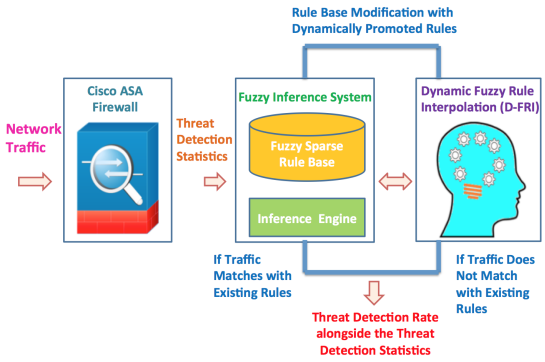

Fig. 5. Block diagram of D-FRI-CiscoFirewall

Access Control List (ACLD), drop due to SYN attack (SYND) and drop due to Denial of Service attack (DOSD).

A. Baseline Analysis of Threat Detection Statistics

Basic threat detection statistics is helpful to extract significant and timely security information regarding a number of possible security events (see Fig. 6). As indicated above, such an analysis is herein focused on three threat detection statistics: ACLD, SYND and DOSD. The *average rate* and *burst rate* of ACLD, SYND and DOSD are shown in Table I. These are normalised over the same time period, which is set to 20 seconds in the present case. As such, it is much faster than the default setting of 600 seconds for threat detection (see Fig. 4). In other words, D-FRI-CiscoFirewall can regularly monitor and analyse both average rate and burst rate in the interval of 20 seconds. However, all these basic security events and their corresponding values may change with regard to the requirement and priority of a given organisation in any practical application of this work.

1) ACL Dropped (ACLD) Packets: Table I indicates that the default average rate for the drop due to the Access Control List (ACL) is 400 dropped packets/second over the last 600 seconds, and that the burst rate is 800 dropped packets/second over the last 20 second period. Therefore, the average rate calculated for 20 seconds is approximately 14 dropped packets/second. This determines the range of ACLD that is 14-800 dropped packets/second over the period of 20 seconds.

2) SYN Dropped (SYND) Packets: Table I indicates that the default average rate for drop due to the SYN attack is 100 dropped packets/second over the last 600 seconds, and

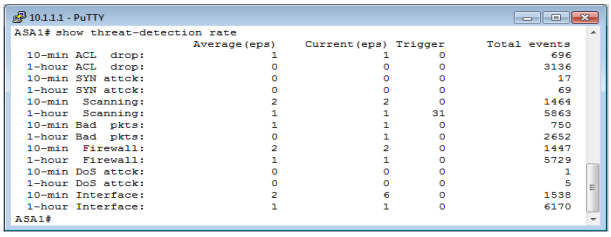

Fig. 6. Gathered basic threat detection statistics for 10 minutes (600 seconds) and 60 minutes (3600 seconds)

TABLE I. BASIC THREAT DETECTION STATISTICS AND DEFAULT SETTINGS OF SELECTED SECURITY EVENTS [2]

Typical Threat	**Default Threat Detection Settings**	
Security Event	**Average Rate**	**Burst Rate**
Drop due to Access Control List (ACL)	400 dropped packets/second over the last 600 seconds.	800 dropped packets/second over the last 20 second period.
Drop due to SYN Attack (TCP SYN incomplete sessions)	100 dropped packets/second over the last 600 seconds.	200 dropped packets/second over the last 20 second period.
Drop due to Denial of Service (DOS) Attack	100 dropped packets/second over the last 600 seconds.	400 dropped packets/second over the last 20 second period.

that the burst rate is 200 dropped packets/second over the last 20 second period. Therefore, the average rate calculated for 20 seconds is approximately 4 dropped packets/second. This determines the range of SYND that is 4-200 dropped packets/second over the period of 20 seconds.

3) DOS Dropped (DOSD) Packets: Table I indicates that the default average rate for drop due to the Denial of Service (DOS) attack is 100 dropped packets/second over the last 600 seconds, and that the burst rate is 400 dropped packets/second over the last 20 second period. Therefore, the average rate calculated for 20 seconds is approximately 4 dropped packets/second. This determines the range of DOSD that is 4-400 dropped packets/second over the period of 20 seconds.

B. Fuzzy Rule Firing-based System

Based on the baseline analysis of the *average rate* and *burst rate* for three selected security events ACLD, SYND and DOSD, three fuzzy input variables are devised.

1) ACL Dropped (ACLD) Packets: ACLD is considered the first fuzzy input variable over the range of 14-800 dropped packets/second. Through empirical analysis the value domain of this input variable is empirically divided into five fuzzy sets: Very Low, Low, Medium, High and Very High. These represent threat categories over the corresponding ranges 14-205 drops/second, 155-355 drops/second, 305-505 drops/second, 455-655 drops/second, and 605-800 drops/second, respectively. The initial design of the ACLD input variable with its triangular fuzzy sets in Matlab is depicted in Fig. 7.

2) SYN Dropped (SYND) Packets: SYND is considered the second fuzzy input variable over the range of 4-200 dropped packets/second. Similar to the specification to ACLD, through empirical analysis, the value domain of this input variable is divided into five fuzzy sets: Very Low, Low, Medium, High and Very High. These represent threat categories over the corresponding ranges 4-60 drops/second, 40-95 drops/second, 75-130 drops/second, 110-165 drops/second, and 145-200 drops/second, respectively. The initial design of the SYND input variable with its triangular fuzzy sets in Matlab is depicted in Fig. 8.

3) DOS Dropped (DOSD) Packets: DOSD is considered the third fuzzy input variable over the range of 4-400 dropped packets/second. Again, by empirical analysis, this input variable is divided into five fuzzy sets: Very Low, Low, Medium, High and Very High, representing threat categories over the corresponding ranges 4-120 drops/second, 80-190 drops/second, 150-260 drops/second, 220-330 drops/second, and 290-400 drops/second, respectively. The initial design of the DOSD input variable with its triangular fuzzy sets in Matlab is depicted in Fig. 9.

4) Threat Detection Rate (TDR): The fuzzy output variable, namely, the threat detection rate (TDR) is determined on the basis of the above three fuzzy input variables (ACLD, SYND and DOSD). Its value domain is also divided into five fuzzy sets: Very Low, Low, Medium, High and Very High, representing threat categories over the corresponding ranges 0-20%, 10-40%, 30-60%, 50-80% and 70-100%, respectively. The initial design of the TDR output variable with its triangular fuzzy sets in Matlab is depicted in Fig. 9.

5) Fuzzy Sparse Rule Base: Based on the above specification of both input and output variables and their corresponding fuzzy value domains, a fuzzy reasoning system that works by performing rule matching and firing can be built via following the Mamdani's inference method [7], as shown in Fig. 11. This system contains an original sparse rule base of 31 rules (that are empirically learned) as given in Fig. 12.

C. D-FRI System

As indicated above, the fuzzy inference system developed is based on a sparse rule base. Thus, it is likely that certain observations may not find any matching rules in this rule base. This implies that any threat detection over such observations will require an FRI. The D-FRI system performs such interpolation in the absence of any matching rules to generate an approximated result. Later, it stores all interpolated results for the purpose of dynamic rule promotion in future. When it accumulates a prescribed number of interpolated results, then its inherent dynamic learning mechanism generalises these results into rules which can be promoted and merged with the original sparse rule base, thereby improving both efficiency and accuracy in future inference. In the current study, a total of 283 interpolated results are accumulated and through generalising these results, a total of 7 rules are dynamically created and promoted, which are shown in Fig. 13.

IV. EXPERIMENTAL RESULTS

Experimental results on D-FRI-CiscoFirewall are presented in the following four subsections to illustrate how the proposed work helps improve the Cisco ASA Firewall operation.

A. Standard Cisco ASA Firewall Threat Detection

In this first set of experiments, results are recorded for the standard Cisco ASA Firewall under various simulated attack conditions. These are shown in Table II, where the default *syslog* message - *%ASA-4-733100* is generated and recorded in the log for all those attacks consisting of any value of ACLD, SYND and DOSD higher than the threshold *average rate*. The Cisco ASA Firewall threat detection feature only alerts by the

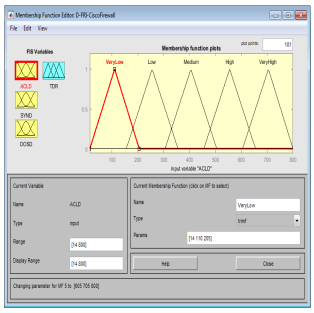

Fig. 7. Fuzzy input variable ACLD and its fuzzy sets

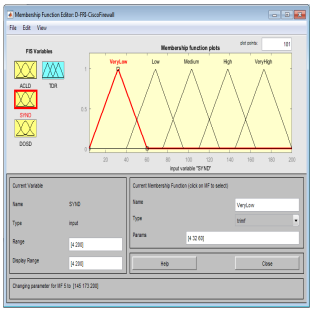

Fig. 8. Fuzzy input variable SYND and its fuzzy sets

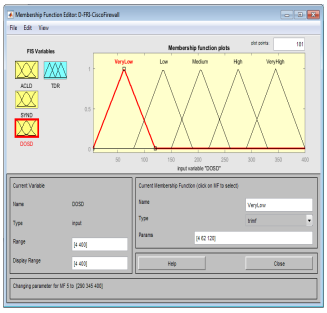

Fig. 9. Fuzzy input variable DOSD and its fuzzy sets

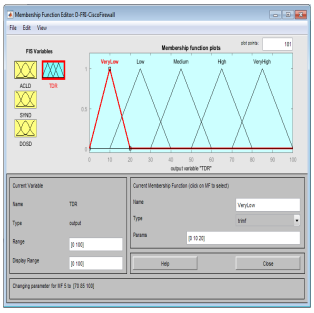

Fig. 10. Fuzzy output variable TDR and its fuzzy sets

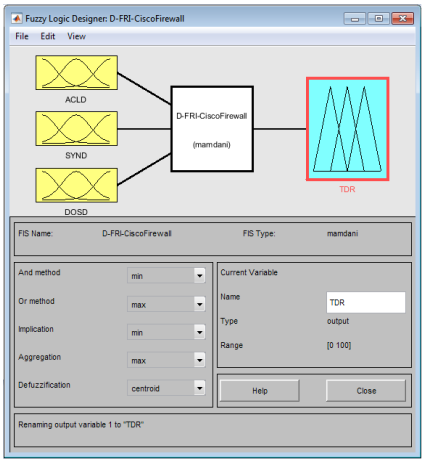

Fig. 11. Fuzzy inference system within D-FRI-CiscoFirewall

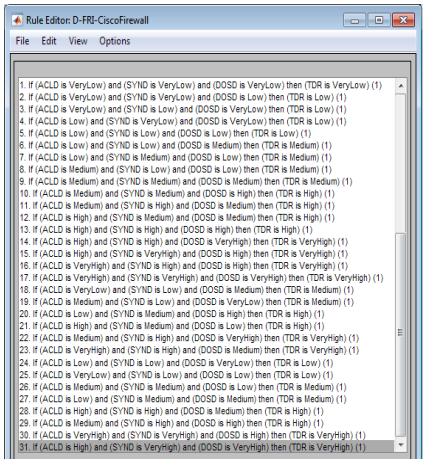

Fig. 12. Original sparse rule base in D-FRI-Cisco

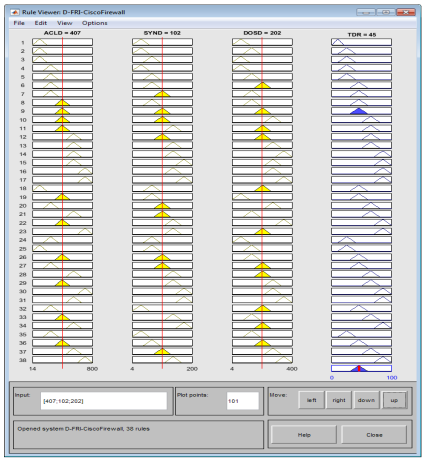

Fig. 13. D-FRI-Cisco sparse rule base with dynamically promoted rules

use of this standard *syslog* message for every threat. Note that reading a large number of *syslog* messages - *%ASA-4-733100* in the huge *syslog* file is a daunting task for anyone and necessitates expertise to understand it. Besides, it fails to offer more useful information, such as the relative analysis of a number of security events and the comprehensive threat detection rate for the entire system.

TABLE II. STANDARD CISCO ASA FIREWALL THREAT DETECTION OUTPUTS

Obs. No.	Standard Cisco ASA Firewall			
	Input Variables			Output
	ACLD	SYND	DOSD	Syslog Message
1	132	39	211	*%ASA-4-733100*
2	296	108	216	*%ASA-4-733100*
3	439	111	281	*%ASA-4-733100*
4	402	98	197	*%ASA-4-733100*
5	727	175	352	*%ASA-4-733100*
6	91	26	54	*%ASA-4-733100*
7	256	75	79	*%ASA-4-733100*

B. D-FRI-CiscoFirewall Threat Detection with Original Sparse Rules

The second set of experiments is to demonstrate the threat detection ability of D-FRI-CiscoFirewall for the same simulated attack conditions as with those specified in the first set. The results are shown in Table III, where the threat detection alerts are generated for the entire system together with the threat levels for selected security events. This is in addition to the default *syslog* message - *%ASA-4-733100* of the Cisco ASA Firewall. These results simplify the overall threat detection process for every firewall user, avoiding the otherwise required examination of the complex *syslog* and its messages. Undoubtedly, quick alerts and their understanding help expedite the action process. Therefore, the firewall administrator can act upon and exercise their planned action or close down the entire network for its immediate protection.

TABLE III. D-FRI-CISCO-FIREWALL THREAT DETECTION OUTPUTS BASED ON ORIGINAL SPARSE RULE BASE

Obs. No.	D-FRI-CiscoFirewall with Original Sparse Rules			
	Input Variables			Output Variable
	ACLD	SYND	DOSD	TDR
1	132	39	211	Threat Detection is LOW
2	296	108	216	Threat Detection is MEDIUM
3	439	111	281	Threat Detection is HIGH
4	402	98	197	Threat Detection is MEDIUM
5	727	175	352	Threat Detection is VERY HIGH
6	91	26	54	Threat Detection is VERY LOW
7	256	75	79	Threat Detection is LOW

C. D-FRI-CiscoFirewall Threat Detection with Dynamically Promoted Rules

This third set of experiments is carried out to demonstrate the effectiveness of performing dynamic actions in D-FRI-CiscoFirewall during the threat detection process, where a total of 283 interpolated rules are accumulated and after D-FRI generalisation, a total of 7 rules are dynamically created and promoted to become part of the (still sparse) rule base (as shown in Fig. 13). The inference results based on these dynamically promoted rules are presented in Table IV.

TABLE IV. D-FRI-CISCO-FIREWALL THREAT DETECTION OUTPUTS AFTER DYNAMICALLY PROMOTED RULES

Obs. No.	D-FRI-CiscoFirewall with Dynamically Promoted Rules			
	Input Variables			Output Variable
	ACLD	SYND	DOSD	TDR
1	151	40	219	Threat Detection is MEDIUM
2	412	144	133	Threat Detection is HIGH
3	597	189	195	Threat Detection is VERY HIGH
4	263	42	129	Threat Detection is LOW
5	398	74	187	Threat Detection is MEDIUM
6	579	109	280	Threat Detection is HIGH
7	711	146	365	Threat Detection is VERY HIGH

Note that once these interpolated results are promoted into the rule base, there is no need for future interpolation given the same or similar observations that fully or partially match these dynamically learned rules. This helps save the rule interpolation overheads otherwise incurred, making the overall inference system more efficient.

D. Accuracy of Dynamic Rules for D-FRI-CiscoFirewall

The fourth and final set of experiments is crucial to evaluate the real success of the proposed approach in general and the impact of D-FRI in particular, by checking the accuracy of the dynamically promoted rules. For this, the dynamically generated rules are compared against those rules that are directly translated from individual interpolated results without generalisation ($\epsilon_{\%dvi}$) and also, against the underlying ground truth rules that are provided in the simulated environment ($\epsilon_{\%dvt}$). Of course, for real-world applications, such ground truth rules are obviously not available, otherwise there is no need to resort to fuzzy rule interpolation in the first place.

The differences between the use of traditional transformation-based rule interpolation and that of the ground truth rules ($e_{\%ivt}$) are also provided. For all these performance indices, the percentage error $\epsilon_{\%} = \epsilon / range_y$ is computed in relation to the range of the consequent variable. Table V exhibits the averaged values and standard deviations for these indices. This result shows that the use of dynamically generated rules by the D-FRI operation leads to comparatively more accurate results than the employment of traditional rule interpolation and such results are closer to the use of ground truth rules.

TABLE V. ACCURACY COMPARISON BETWEEN DYNAMIC RULES AND DIRECTLY INTERPOLATED RULES AND GROUND TRUTH RULES

Metric	$\epsilon_{\%dvi}$	$\epsilon_{\%dvt}$	$\epsilon_{\%ivt}$
AVG	2.45	**1.36**	2.62
SD	2.76	**1.38**	2.75

V. CONCLUSION

This paper has presented the innovative D-FRI-CiscoFirewall system for automating threat detection with the Cisco ASA Firewall. D-FRI-CiscoFirewall utilises threat detection statistics, customising the detection process according to the organisational requirements. It performs a relative analysis of prioritised security events and predicts a comprehensive security status even when no matching rules are found. D-FRI-CiscoFirewall produces a dynamic rule base derived from the changing network conditions and traffic density, resulting in more accurate detection. In particular, the paper has demonstrated the successful use of the D-FRI approach in D-FRI-CiscoFirewall for selected and prioritised security events: drop due to Access Control List (ACLD), drop due to SYN attack (SYND) and drop due to Denial of Service attack (DOSD). For future, D-FRI-CiscoFirewall will be extended to cover other types of drop. Theoretically, it would be very interesting to investigate how backward FRI [10] and weighted FRI [11] may be integrated with the current work, to enhance the effectiveness of D-FRI-CiscoFirewall.

REFERENCES

[1] N. Naik, R. Diao, and Q. Shen, "Dynamic fuzzy rule interpolation and its application to intrusion detection," *IEEE Transactions on Fuzzy Systems*, 2017.

[2] Cisco.com. (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

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

[4] Cisco.com. (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

[5] 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.

[6] N. Naik, P. Jenkins, B. Kerby, J. Sloane, and L. Yang, "Fuzzy logic aided intelligent threat detection in cisco adaptive security appliance 5500 series firewalls," in *2018 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, 2018.

[7] 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.

[8] Z. Huang and Q. Shen, "Fuzzy interpolative reasoning via scale and move transformations," *Fuzzy Systems, IEEE Transactions on*, vol. 14, no. 2, pp. 340–359, 2006.

[9] 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

[10] S. Jin, R. Diao, C. Quek, and Q. Shen, "Backward fuzzy rule interpolation," *IEEE Transactions on Fuzzy Systems*, vol. 22, no. 6, pp. 1682–1698, 2014.

[11] F. Li, C. Shang, Y. Li, J. Yang, and Q. Shen, "Fuzzy rule-based interpolative reasoning supported by attribute rankingn," *IEEE Transactions on Fuzzy Systems*, vol. 26, no. 5, pp. 2758–2773, 2018.