A Framework for Security Components Anomalies Severity Evaluation and Classification

Kamel Karoui[1] , Fakher Ben Ftima[2] and Henda Ben Ghezala[3]
[1]RIADI, ENSI, University of Manouba, Manouba, Tunisia
kamel.karoui@insat.rnu.tn

[2]RIADI, ENSI, University of Manouba, Manouba, Tunisia
fakher.benftima@infcom.rnu.tn

[3]RIADI, ENSI, University of Manouba, Manouba, Tunisia
Henda.bg@cck.rnu.tn

ABSTRACT

Security components such as firewalls, IDS and IPS, are the most widely adopted security devices for network protection. These components are often implemented with several errors (or anomalies) that are sometimes critical. To ensure the security of their networks, administrators should detect these anomalies and correct them. Before correcting the detected anomalies, the administrator should evaluate and classify these latter to determine the best strategy to correct them. In this work, we propose a framework to assess and classify the detected anomalies using a three evaluation criteria: a quantitative evaluation, a semantic evaluation and multi-anomalies evaluation. The proposed process, convenient in an audit process, will be detailed by a case study to demonstrate its usefulness.

KEYWORDS

Anomaly severity evaluation, anomaly severity classification, semantic evaluation, quantitative evaluation, multi-anomalies evaluation.

1. INTRODUCTION

Rules in a security component can be misconfigured, which implies many conflicts. A misconfiguration or a conflict between rules means that the security component, may either:

- accept some malicious packets, which consequently create security holes.
-discard some legitimate packets, which consequently disrupt normal traffic.

Both cases could cause irreparable consequences. Unfortunately, it has been observed that most security components are implemented with anomalies. Depending on the nature of the anomaly, it can be critical, less critical or benign. Considering the impact of these anomalies on the network security, such errors cannot be tolerated [2].

There are several researches that have proposed for anomalies detection and correction but rare those who are interested in the anomalies severity and their impact on network security. The evaluation and classification of anomalies severity provide the administrator with:

-many correction scenarios
-a classification of rules to be corrected according to their criticality
-an overview of the security component vulnerabilities

DOI : 10.5121/ijnsa.2013.5405

In this paper, we propose firstly an evaluation metrics of the anomalies severity based on the following criteria:

-a quantitative criterion: to get an idea of the number of rules involved in the anomaly.
-a semantic criterion: to assess the impact of the misconfiguration on the services provided (HTTP,FTP,..)
-a multi-anomalies criterion: to study the impact of the composition of many anomalies together.

By combining the three metrics together, we can measure the impact of each anomaly on the security component rule base. For this, we will classify these anomalies severity importance according to their nature, namely; shadowing anomaly, generalization anomaly, redundancy anomaly and correlation anomaly. This classification will determine rules that cause the security component vulnerability.

The remaining parts of the paper are organized as follows: section 1 introduces related works in security component anomalies detection and correction. Section 2 schematizes the proposed approach model. Sections 3 to 5 detail the proposed process steps and section 6 concludes the paper.

2. RELATED WORKS

As presented in the introduction, a lot of research has been proposed for the security components analysis, misconfigurations' detection and correction. Most research focuses on the firewalls network policy; in [10], [7] and [6] the authors propose a model for firewalls properties analysis and anomalies detection. Also, the authors of [5] and [4] suggest another model to detect firewalls misconfigurations in central and distributed architectures. In [1], the authors analyze firewall rules using an expert system whereas the authors of [8] analyze firewalls with relational algebra. In [3], the authors put forward a model for IPsec and VPN verification. However, these security components (homogenous or heterogeneous) may conflict when they are installed together on a network. In this context, [2] propose a solution for firewalls and IDS misconfigurations detection.

In reviewing these few references, we note that there is no works that assessed the severity of anomalies before correcting them. The study of the severity can give the administrator more information about the vulnerability of the component. In addition, the classification step exploits this information by illustrating the impact of these errors on the network security by a set of diagrams. In this work, we will develop these two concepts; we begin by detailing our proposed approach in the following section, we will

3. THE PROPOSED APPROACH

In order to evaluate and classify the security component anomalies severity, we propose an approach composed of several steps schematized in figure 1. In the case study, we will apply our approach to firewalls. However, the approach should apply for all security components based on filtering attributes. Below, we will briefly present these steps:

-Step A: Security component anomalies detection
Usually, most security components' base rule contains some misconfigurations. This step consists in checking the security component' base rule to detect anomalies. For the firewall, we enumerate

four kinds of anomalies, namely; shadowing anomaly, generalization anomaly, redundancy anomaly and correlation anomaly. We will not detail this section because it is not the purpose of the paper. For more details, refer to [9]. In the next step, we will evaluate the severity of the detected anomalies (See step A in figure 1).

- Step B: The security component anomalies' severity importance evaluation

The detected anomalies in step A will be classified into several sub-sets:

- Shadowing anomalies sub-set: contains rules that are shadowed by other rules in the base rule.
-Generalization anomalies sub-set: contains rules that are generalized by other rules in the base rule.
-Redundancy anomalies sub-set: contains rules that are redundant to other rules in the base rule.
-Correlation anomalies sub-set: contains rules that are correlated to other rules in the base rule.

These sub-sets will allow us to evaluate each anomaly severity importance using a three metrics; a quantitative metric, a semantic metric and multi-anomalies metric (See step B in figure 1).

- Step C: Anomalies severity importance classification

The defined metrics in step B, will be exploited together in order to classify the anomalies severity. We will classify the severity importance according to the shadowing level degree, the generalization level degree, the redundancy level degree and the correlation level degree. (See step C in figure 1).

-Step D: Security component anomalies correction

This step consists in correcting the detected anomalies in step B. The correction strategy depends on the classification results returned in step C. We will not detail this section because it is not the purpose of the paper (see step D in figure 1).

In the process presented in figure 1, the gray colored part (steps A and D) is the part already made in several research works. The blue-colored part (steps B and C) is the part that we propose and detail in the following sections.

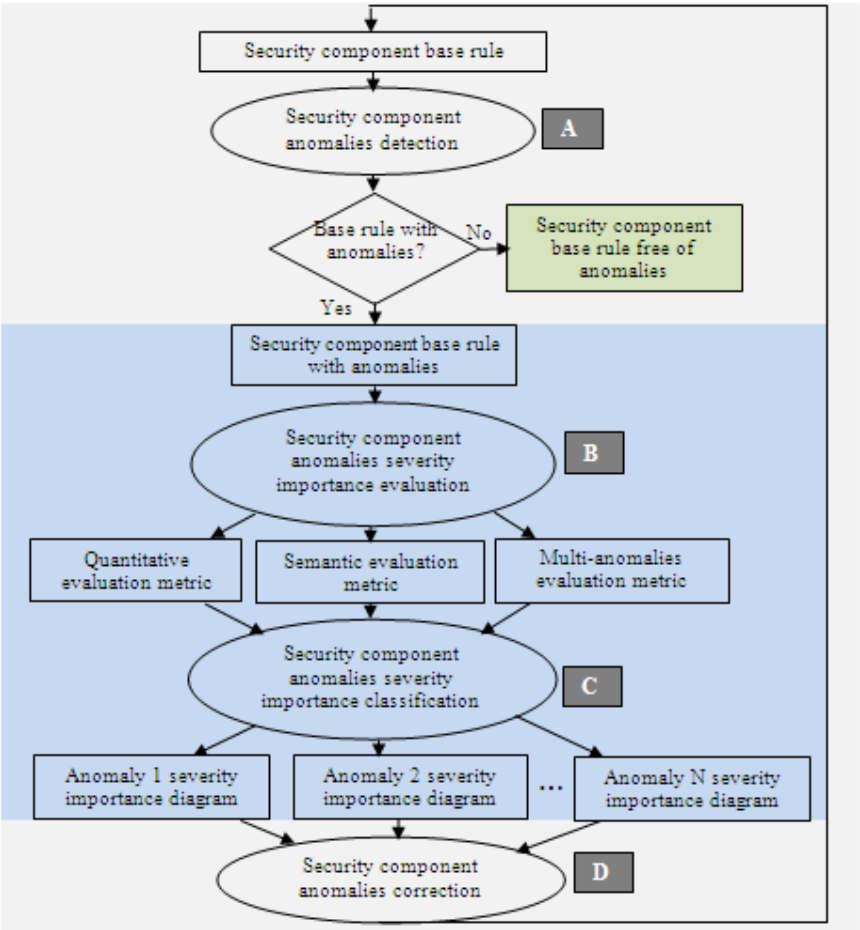

Figure 1. The proposed approach

4. FORMAL SECURITY COMPONENT'S BASE RULE VERIFICATION (STEP A)

Generally, security components are specified by a set of formal rules which can be filtering or alerting ones. A rule defines a decision (such as "deny", "alert", "accept", or "pass") that applies over a set of condition attributes (such as, "source address", "destination address", "source port", "destination port", "protocol", "attack class", etc.). Let's take a security component composed of a set Q of t rules ($r_i \in Q$ with $1 \leq i \leq t$). A rule r_i in the set Q is represented formally as follows:

$$\mathbf{r_i: r_i[A_1]\ r_i[A_2]\ldots.\ r_i[A_n]} \text{ where}$$

-A_1, A_2… A_{n-1} are the rule r_i attributes'. For example, in table 1, the attribute A_2=Protocol.
-$r_i[A_m]$ is the attribute A_m value with $(1 \leq m \leq n)$. For example, in table 1, $r_3[A_2]$=TCP.
- A_n is the attribute "Decision". For example, in table 1, A_7 is the decision attribute and $r_3[A_7]$=deny.

For more details about rules formalization, refer to [4].

An anomaly in a security component base rule can be the result of the following cases [5]:

-The existence of two or more rules that may match the same packet.
-The existence of a rule that can never be activated. We note that a rule r_i is activated if there is an IP packet that was accepted or rejected by applying the rule r_i.

There are four different anomalies that may exist among rules in a security component base rule, namely:

-Shadowing anomaly: a rule r_j is shadowed by a previous rule r_i when r_i matches all the packets that match r_j and the two rules have different decisions, such that the shadowed rule r_j will never be activated (see example in section 4.1).

-The generalization anomaly: The generalization anomaly is the reverse of the shadowing anomaly i.e. in a base rule Q, a rule r_j is a generalization of a preceding rule r_i if, on the one hand, the rule r_j can match all the packets that match the rule r_i and , on the other hand, the two rules have different decisions (see example in section 4.1).

-The redundancy anomaly: In a base rule Q, a rule r_j is redundant to a rule r_i if r_j performs the same decision on the same packets as r_i . In the way, if the redundant rule r_j is removed, the safety of the security component will not be affected (see example in section 4.1).

- The correlation anomaly: In a base rule Q, the rule r_j is correlated to r_i if, on the one hand, the first rule r_i matches some packets that match the second rule r_j , and the second rule r_j matches some packets that match the first rule r_i and, on the other hand, the two rules have different decisions (see example in section 4.1).

For more details about the security component anomalies, refer to [5].

4.1 Case study

Let's take a security component *Fw*, composed of a base rule Q. Each rule r_i belonging to Q has the following attributes: "Packet length", "Protocol", "Source address", "Destination address", "Source port", "Destination port" and "Decision".

Rules	Packet length (A_1)	Protocol (A_2)	Source address (A_3)	Src. Port (A_4)	Destination address (A_5)	Dest. Port (A_6)	Decision (A_7)
r_1	All	TCP	[140.192.10.1-140.192.10.100]	Any	[129.170.20.20-129.170.20.100]	Any	deny
r_2	All	TCP	[140.192.10.20-140.192.10.50]	Any	[129.170.20.20-129.170.20.70]	80	accept
r_3	All	TCP	[140.192.10.1-140.192.10.60]	Any	[129.170.20.20-129.170.20.100]	Any	deny
r_4	16	TCP	[140.192.10.1-140.192.10.100]	Any	[129.170.20.30-129.170.20.100]	80	accept
r_5	16	TCP	[140.192.10.20-140.192.10.50]	Any	[129.170.20.30-129.170.20.70]	80	deny
r_6	16	TCP	[140.192.10.20-140.192.10.50]	Any	[129.170.20.30-129.170.20.70]	80	accept
r_7	All	TCP	[140.192.10.20-140.192.10.50]	23	[129.170.20.30-129.170.20.70]	80	deny
r_8	16	TCP	[140.192.10.170-140.192.10.200]	Any	[129.170.20.30-129.170.20.70]	25	deny
r_9	All	TCP	[140.192.10.151-140.192.10.200]	Any	[129.170.20.20-129.170.20.70]	23	accept
r_{10}	All	TCP	[140.192.10.101-140.192.10.150]	Any	[129.170.20.30-129.170.20.70]	21	deny

Table 1. The security component *Fw* base rule

By analyzing the security component *Fw*, we note that there some anomalies detailed as follows:
-For the shadowing anomaly, we note that r_2 is shadowed by r_1. More precisely:

$(r_2[A_1]=r_1[A_1]) \wedge (r_2[A_2]=r_1[A_2]) \wedge (r_2[A_3] \subset r_1[A_3]) \wedge (r_2[A_4]=r_1[A_4]) \wedge$
$(r_2[A_5] \subset r_1[A_5]) \wedge (r_2[A_6] \subset r_1[A_6]) \wedge (r_2[A_7] \neq r_1[A_7])$
Also, in the same table, we note that (r_4 and r_6 are shadowed by r_1), (r_5 and r_7 are shadowed by r_2), (r_6 is shadowed by r_3) , (r_5 and r_7 are shadowed by r_4) and (r_6 is shadowed by r_5).

-For the generalization anomaly, we note that r_2 is generalized by r_3. More precisely:
$(r_2[A_1]=r_3[A_1]) \wedge (r_2[A_2]=r_3[A_2]) \wedge (r_2[A_3] \subset r_3[A_3]) \wedge (r_2[A_4]=r_3[A_4]) \wedge$
$(r_2[A_5] \subset r_3[A_5]) \wedge (r_2[A_6] \subset r_3[A_6]) \wedge (r_2[A_7] \neq r_3[A_7])$

-For the redundancy anomaly, we note that r_3 is redundant to r_1. More precisely:
$(r_3[A_1]=r_1[A_1]) \wedge (r_3[A_2]=r_1[A_2]) \wedge (r_3[A_3] \subset r_1[A_3]) \wedge (r_3[A_4]=r_1[A_4]) \wedge$
$(r_3[A_5]=r_1[A_5]) \wedge (r_3[A_6]=r_1[A_6]) \wedge (r_3[A_7]=r_1[A_7])$
Also, in the same table, we note that (r_5 and r_7 are redundant to r_1), (r_5 and r_7 are redundant to r_3), (r_6 is redundant to r_2) and (r_6 is redundant to r_4).

-For the correlation anomaly, we note that r_4 is correlated to r_3. More precisely:
$(r_3[A_1] \supset r_4[A_1]) \wedge (r_3[A_2]=r_4[A_2]) \wedge (r_3[A_3] \subset r_4[A_3]) \wedge (r_3[A_4]=r_4[A_4]) \wedge$
$(r_3[A_5] \supset r_4[A_5]) \wedge (r_3[A_6] \supset r_4[A_6]) \wedge (r_3[A_7] \neq r_4[A_7])$
Also, in the same table, we note that (r_7 is correlated to r_6) and (r_7 is correlated to r_4).

In the next section, we will first evaluate the severity importance of these anomalies in order to classify them.

5. THE SECURITY COMPONENT ANOMALIES SEVERITY IMPORTANCE EVALUATION (STEP B)

After detecting the security component anomalies (see section 4), we will gather them in four sub-sets that we will define in the next sub-section. Then, we will evaluate their criticality degree by a set of metrics.

5.1 Anomalies sub-sets definition

For each one of the anomalies' categories namely, "**S**hadowing", "**G**eneralization", "**R**edundancy" and "**C**orrelation", we associate respectively sub-sets **S**, **G**, **R** and **C** which contain rules belonging to that category. Let's take a security component composed of a set Q of t rules ($r_i \in Q$ with $1 \leq i \leq t$). We define these sub-sets as follows:

• The set of shadowing rules:
$$S = \left\{ r_i \in Q \middle| \exists r_j \in Q \middle| \forall 1 \leq m \leq (n-1),\ r_j[A_m] \subseteq r_i[A_m] \wedge r_j[A_n] \neq r_i[A_n] \text{ with } 1 \leq i < j \leq t \right\} \quad (1)$$
We note that |S| is the sub-set S cardinality i.e. the number of shadowed rules.
• The set of generalizing rules:
$$G = \left\{ r_j \in Q \middle| \exists r_i \in Q \middle| \forall 1 \leq m \leq (n-1),\ r_i[A_m] \subseteq r_j[A_m] \wedge r_j[A_n] \neq r_i[A_n] \text{ with } 1 \leq i < j \leq t \right\} \quad (2)$$
We note that |G| is the sub-set G cardinality i.e. the number of generalized rules.

• The set of redundant rules:

$$R=\left\{r_i\in Q\middle|\exists r_j\in Q\middle|\forall 1\le m\le (n-1), r_j[A_m]\ \subseteq r_i[A_m]\wedge r_i[A_n]=r_j[A_n] with\ 1\le i<j\le t\right\} \quad (3)$$

We note that |R| is the sub-set *R* cardinality i.e. the number of redundant rules.

• The set of correlated rules:

$$C=\left\{\begin{matrix} r_i\in Q\middle|\exists r_j\in Q\middle|\forall 1\le m\le (n-1),\left[(r_i[A_m]\ \subset r_j[A_m])\ \vee\ (r_i[A_m]\ \supset r_j[A_m])\vee(r_i[A_m]\ =r_j[A_m])\right]\wedge \\ r_i[A_n]\ne r_j[A_n] with\ 1\le i<j\le t \end{matrix}\right\} \quad (4)$$

We note that |C| is the sub-set *C* cardinality i.e. the number of correlated rules.
Now, we will define new sub-sets allowing us to evaluate the anomalies' impact of each rule belonging to the defined sub-sets (S, G, R and C) on the other rules, as follows:

• For each element r_i belonging to S, we define the set of shadowed rules:

$$S(r_i)=\left\{r_j\in Q\middle|\ \forall 1\le m\le (n-1),\ r_j[A_m]\ \subseteq r_i[A_m]\ \wedge r_j[A_n]\ne r_i[A_n] with\ 1\le i<j\le t\right\} \quad (5)$$

• For each element r_i belonging to G, we define the set of generalized rules:

$$G(r_i)=\left\{r_j\in Q\middle|\ \forall 1\le m\le (n-1),\ r_i[A_m]\ \subseteq r_j[A_m]\wedge r_j[A_n]\ne r_i[A_n] with\ 1\le i<j\le t\right\} \quad (6)$$

• For each element r_i belonging to R, we define the set of redundant rules:

$$R(r_i)=\left\{r_j\in Q\middle|\ \forall 1\le m\le (n-1), r_j[A_m]\ \subseteq r_i[A_m]\wedge r_i[A_n]=r_j[A_n] with\ 1\le i<j\le t\right\} \quad (7)$$

• For each element r_i belonging to C, we define the set of correlated rules:

$$C(r_i)=\left\{\begin{matrix} r_j\in Q\middle|\ \forall 1\le m\le (n-1),\left[(r_i[A_m]\ \subset r_j[A_m])\ \vee\ (r_i[A_m]\ \supset r_j[A_m])\vee(r_i[A_m]\ =r_j[A_m])\right]\wedge \\ r_i[A_n]\ne r_j[A_n] with\ 1\le i<j\le t \end{matrix}\right\} \quad (8)$$

5.1.1 Case study

Applying the four sub-sets (1),(2),(3) and (4) defined above, on the example in Table 1, we obtain the following results:

• S={r_1,r_2, r_3, r_4, r_5}. We can verify that rules in the sub-set *S* are rules that are shadowing other rules in the set Q.
• G={r_3}. We can verify that rules in the sub-set *G* are rules that are generalizing other rules in the set *Q*.
• R={r_1, r_2, r_3, r_4 }. We can verify that rules in the sub-set *R* are rules that are redundant to other rules in the set *Q*.
• C={r_3, r_4, r_6 }. We can verify that rules in the sub-set *C* are rules that are correlating other rules in the set *Q*.

Taking into account the defined sub-sets S, G, R and C, we will apply (5),(6),(7) and (8) on the example in Table 1.We obtain the following results:

- Rules subjected to the shadowing anomaly (see Table 1) as are classified follows:

$S(r_1)=\{r_2,r_4,r_6\}$ We can verify that rules in the sub-set $S(r_1)$ are rules that are shadowed by r_1 in the set *Q*.

$S(r_2)=\{r_5,r_7\}$ We can verify that rules in the sub-set $\mathbb{S}(r_2)$ are rules that are shadowed by r_2 in the set *Q*.
$S(r_3)=\{r_6\}$ We can verify that rules in the sub-set $\mathbb{S}(r_3)$ are rules that are shadowed by r_3 in the set *Q*.
$S(r_4)=\{r_5,r_7\}$ We can verify that rules in the sub-set $\mathbb{S}(r_4)$ are rules that are shadowed by r_4 in the set *Q*.
$S(r_5)=\{r_6\}$ We can verify that rules in the sub-set $\mathbb{S}(r_5)$ are rules that are shadowed by r_5 in the set *Q*.

-Rules subjected to the generalization anomaly (see Table 1) are classified as follows:
$G(r_3)=\{r_2\}$ We can verify that rules in the sub-set $\mathbb{G}(r_3)$ are rules that are generalized by r_3 in the set *Q*.

-Rules subjected to the redundant anomaly (see Table 1) are classified as follows:
$R(r_1)=\{r_3,r_5,r_7\}$ We can verify that rules in the sub-set $\mathbb{R}(r_1)$ are rules that are redundant to r_1 in the set *Q*.
$R(r_3)=\{r_5,r_7\}$ We can verify that rules in the sub-set $\mathbb{R}(r_3)$ are rules that are redundant to r_3 in the set *Q*.
$R(r_2)=\{r_6\}$ We can verify that rules in the sub-set $\mathbb{R}(r_2)$ are rules that are redundant to r_2 in the set *Q*.
$R(r_4)=\{r_6\}$ We can verify that rules in the sub-set $\mathbb{R}(r_4)$ are rules that are redundant to r_4 in the set *Q*.

-Rules subjected to the correlation anomaly (see Table 1) are classified as follows:
$C(r_3)=\{r_4\}$ We can verify that rules in the sub-set $\mathbb{C}(r_3)$ are rules that are correlated to r_3 in the set *Q*.
$C(r_6)=\{r_7\}$ We can verify that rules in the sub-set $\mathbb{C}(r_6)$ are rules that are correlated to r_6 in the set *Q*.
$C(r_4)=\{r_7\}$ We can verify that rules in the sub-set $\mathbb{C}(r_4)$ are rules that are correlated to r_4 in the set *Q*.

5.2 Anomalies severity importance evaluation

In this section, we will evaluate the anomalies severity regarding three criteria; namely quantitative, semantic and multi-anomalies.

5.2.1 Quantitative importance evaluation

The quantitative evaluation is a metric based on the number of rules involved in the anomaly. The cardinality of the four sub-sets (S, G, R and C) can give us some indications of these anomalies importance.

For that, we associate a quantitative coefficients M_S, M_G, M_R and M_C to each element r_i belonging respectively to the sub-set *S*, *G*, *R* and *C*. These coefficients express the quantitative importance of each type of error. They are defined as follows:

$M_S(r_i) = \frac{|S(r_i)|}{t-1}$ (9) ; $M_G(r_i) = \frac{|G(r_i)|}{t-1}$ (10); $M_R(r_i) = \frac{|R(r_i)|}{t-1}$ (11) and $M_C(r_i) = \frac{|C(r_i)|}{t-1}$(12) where *t* is the number of rules in the set *Q*.

5.2.2 Case study

In our case study, the shadowing anomaly coefficient (9) is defined as follows:

$M_S(r_1) = \frac{|S(r_1)|}{t-1} = \frac{3}{9} = 0,333$; $M_S(r_2) = \frac{|S(r_2)|}{t-1} = \frac{2}{9} = 0,222$; $M_S(r_3) = \frac{|S(r_3)|}{t-1} = \frac{1}{9} = 0,111$;

$M_S(r_4) = \frac{|S(r_4)|}{t-1} = \frac{2}{9} = 0,222$; $M_S(r_5) = \frac{|S(r_5)|}{t-1} = \frac{1}{9} = 0,111$

The generalization anomaly coefficient (10) is defined as follows:

$M_G(r_3) = \frac{|G(r_3)|}{t-1} = \frac{1}{9} = 0,111$

The redundancy anomaly coefficient (11) is defined as follows:

$M_R(r_1) = \frac{|R(r_1)|}{t-1} = \frac{3}{9} = 0,333$; $M_R(r_2) = \frac{|R(r_2)|}{t-1} = \frac{1}{9} = 0,111$; $M_R(r_3) = \frac{|R(r_3)|}{t-1} = \frac{2}{9} = 0,222$;

$M_R(r_4) = \frac{|R(r_1)|}{t-1} = \frac{1}{9} = 0,111$

Finally, the correlation anomaly coefficient (12) is defined as follows:

$M_C(r_3) = \frac{|C(r_3)|}{t-1} = \frac{1}{9} = 0,111$; $M_C(r_4) = \frac{|C(r_4)|}{t-1} = \frac{1}{9} = 0,111$; $M_C(r_6) = \frac{|C(r_6)|}{t-1} = \frac{1}{9} = 0,111$

Taking into account the quantitative evaluation criterion, the shadowing anomaly coefficient $M_S(r_1)$ is greater than the other shadowing anomaly coefficients seeing that r_1 shadows more rules. Thus, the shadowing error is more important and will have higher priority in the correction process. Generally, correcting the most important shadowing rule decreases the number of shadowed rules.

As long as, the redundancy anomaly coefficient $M_R(r_1)$ is greater than the other redundancy anomaly coefficients seeing that r_1 is redundant to more rules. Therefore, the redundancy error is also important and will have higher priority in the correction process.

As defined below, the quantitative coefficient M is based on the number of rules of each sub-set. Although it gives us a first indicator of the anomalies severity importance, nevertheless, some reserves can be expressed:

• The indicators $M_R(r_i)$ or $M_G(r_i)$ can be very bad (approximate to 1) but not really critical seeing that this rule can be rarely activated.
• In the same way, the indicators $M_S(r_i)$ or $M_C(r_i)$ can be very good (approximate to 0) but probably points out a serious problem if this rule is often activated.

To remedy to the previous reserves, we propose a complementary metric called semantic evaluation. This metric takes into account the semantic of the services involved in the anomaly and gives us an overview of the rule vulnerability degree.

5.2.3 Semantic importance evaluation

To propose such a metric, the administrator will order rules regarding one or more filtering attributes (except the attribute "Decision"). As an example, for an e-commerce website, the administrator will give importance to the port 8080. For an FTP server, it will give importance to the port 23 and 25.
Let choose for example the attribute "destination port" which is, generally, the most important service among the others attributes. In this case, the administrator must classify services offered by the network according to the importance of "destination port" number.

From this classification, we bind each rule to the service to which it is referred and associate an indicator relating to the importance of that service. Let's suppose that we have z services in the network and a rule r_i using to a service classified k^{th} by the administrator. We associate to r_i the value:

$$\boldsymbol{v(r_i) = z\text{-}k+1} \text{ with } 1 \leq k \leq t$$

If the attribute value is “ANY”, this means that this attribute can take any services value provided by the network. For this, it is assigned by the value of the best classified service plus one.

Based on $v(r_i)$, we define semantic evaluation coefficients M_S’, M_G’, M_R’ and M_C’ for respectively the defined sub-sets S, G, R and C as follows :

$$M'_S(r_i) = \frac{v(r_i)}{Max(v(r_i))+1} \quad (13)$$ where r_i belongs to the sub-set S

$$M'_G(r_i) = \frac{v(r_i)}{Max(v(r_i))+1} \quad (14)$$ where r_i belongs to the sub-set G

$$M'_R(r_i) = \frac{v(r_i)}{Max(v(r_i))+1} \quad (15)$$ where r_i belongs to the sub-set R

$$M'_C(r_i) = \frac{v(r_i)}{Max(v(r_i))+1} \quad (16)$$ where r_i belongs to the sub-set C

5.2.4 Case study

Based on the defined metrics (13), (14), (15) and (16), we suppose that the administrator has classified the services offered by the attribute "Destination Port ". We notice that, in our case study, the filtering rules use four destination ports (see Table 1) that are; the HTTP port (80), the FTP port (21), the TELNET port (23) and the SMTP port (25) classified by importance as follows:

1. HTTP (this service will have the value 4-1+1=4)
2. SMTP (this service will have the value 4-2+1=3)
3. TELNET (this service will have the value 4-3+1=2)
4. FTP (this service will have the value 4-4+1=1)

The service ANY, will have the value of the best classified service plus one. In our case, it will have the value 5.

In our case, the associated values to each rule representing a given service are the following:

$v(r_2)=v(r_4)=v(r_5)=v(r_6)=v(r_7)=4$ since r_2 , r_4 , r_5 , r_6 and r_7 are related to the HTTP port.

$v(r_9)=2$ since r_9 is related to the TELNET port.

$v(r_8)=3$ since r_8 is related to the SMTP port.

$v(r_{10})=1$ since r_{10} is related to the FTP port.

$v(r_1)=v(r_3)=5$ r_1 and r_3 are related to any port.

The four metrics sub-sets M_S', M_G', M_R' and M_C' are calculated as follows:

$$M_S'(r_1)=M_R'(r_1)=\frac{5}{6}=0,83\,;M_S'(r_2)=M_R'(r_2)=\frac{4}{6}=0,66\,;$$

$$M_S'(r_3)=M_G'(r_3)=M_R'(r_3)=M_C'(r_3)=\frac{5}{6}=0,83\,;\qquad M_S'(r_4)=M_R'(r_4)=M_C'(r_4)=\frac{4}{6}=0,66\,;$$

$$M_S'(r_5)=\frac{4}{6}=0,66\,;M_C'(r_6)=\frac{4}{6}=0,66$$

Taking into account the semantic evaluation criterion, we note that:

- Each rule with the destination port value "ANY" gains importance.
- There are rules involved in several errors. For example, rule r_3 has an impact on all anomalies categories.

In the next section, we will consider this criterion because it increases the errors severity.

5.2.5 Multi-anomalies importance evaluation

Sometimes, a rule is involved in several anomalies. We are talking about "multi-anomalies" categories. In the case of firewall anomalies, there are simple errors category, double errors category, triple errors category and quadruple errors category. For example, as presented in the sub-section 5.2.4, r_3 is involved in the shadowing error category, the generalization error category, the correlation error category and the redundancy error category. Also, r_2 is involved in the shadowing error category and the redundancy error category. These categories are detailed as follows:

- Simple error category: The simple error category is defined as follows:

$$SM=\left\{r_i\in(S\vee R\vee G\vee C)\wedge\left[\begin{array}{l} r_i\notin(S\cap R)\wedge r_i\notin(S\cap G)\wedge r_i\notin(S\cap C)\\ \wedge r_i\notin(R\cap G)\wedge r_i\notin(R\cap C)\wedge r_i\notin(G\cap C)\end{array}\right]\right\} \quad (17)$$

- Double errors category: The double error category is defined as follows:

$$DB = \left\{ \begin{array}{l} \left[r_i \in (S \cap G) \vee (S \cap R) \vee (S \cap C) \vee (G \cap R) \vee (G \cap C) \vee (R \cap C) \right] \\ \wedge \left[r_i \notin (S \cap G \cap R) \wedge r_i \notin (S \cap G \cap C) \wedge r_i \notin (S \cap R \cap C) \wedge r_i \notin (C \cap R \cap G) \right] \end{array} \right\} \quad (18)$$

- Triple errors category: The triple error category is defined as follows:

$$TR = \left\{ r_i \in \left[(S \cap G \cap R) \vee (S \cap G \cap C) \vee (S \cap R \cap C) \vee (G \cap R \cap C) \right] \wedge r_i \notin (S \cap G \cap R \cap C) \right\} \quad (19)$$

- Quadruplet errors category: The quadruplet error category is defined as follows:

$$QD = \{ S \cap G \cap R \cap C \} \quad (20)$$

In order to show the impact of the multi-anomalies categories, the administrator will associate a weight to each category of error. In the case of firewalls, if a rule r_i belongs to the SM category, it will associate to it a coefficient $M''_S(r_i) = M''_G(r_i) = M''_C(r_i) = M''_R(r_i) = 0,25$. If a rule r_i belongs to the DB category, it will associate to it a coefficient $M''_S(r_i) = M''_G(r_i) = M''_R(r_i) = M''_C(r_i) = 0,5$. If a rule r_i belongs to the TR category, it will associate to it a coefficient $M''_S(r_i) = M''_G(r_i) = M''_R(r_i) = M''_C(r_i) = 0,75$ and finally, if a rule r_i belongs to the QD category, it will associate to it a coefficient $M''_S(r_i) = M''_G(r_i) = M''_C(r_i) = M''_R(r_i) = 1$.

5.2.6 Case study

Based on (1), (2), (3) and (4), rules involving anomalies are r_1, r_2 , r_3 , r_4 , r_5 and r_6. Applying (17), (18), (19) and (20), in our case study, we have:

- $r_5 \in SM = \{S\}$, it will have a coefficient $M''_S(r_5) = 0,25$
- $r_6 \in SM = \{C\}$, it will have a coefficient $M''_C(r_6) = 0,25$
- $r_1 \in DB = \{S \cap R\}$, it will have a coefficient $M''_S(r_1) = M''_R(r_1) = 0,5$
- $r_2 \in DB = \{S \cap R\}$, it will have a coefficient $M''_S(r_2) = M''_R(r_2) = 0,5$
- $r_4 \in TR = \{S \cap R \cap C\}$, it will have a coefficient $M''_S(r_4) = M''_R(r_4) = M''_C(r_4) = 0,75$
- $r_3 \in QD = \{S \cap G \cap R \cap C\}$, it will have a coefficient $M''_S(r_3) = M''_G(r_3) = M''_C(r_3) = M''_R(r_3) = 1$

6. CLASSIFICATION OF THE ANOMALIES IMPORTANCE (STEP C)

In section 5, we have proposed, for each rule, three metrics M, M' and M''. Gathering these three metrics together give us an interesting measure ***MM'M"*** that we can incorporate either in an audit process or for assessing security component vulnerability.

In this section, we will exploit this measure and classify the anomalies severity importance relatively to the shadowing anomaly importance. The purpose of this classification is to schematize the impact of the shadowing anomaly severity in a rule. Also, this classification will determine the vulnerable services and sources of attack rules. The exploitation of these results will allow the administrator to decide the order of rules correction and review the security of important services. For a significant evaluation, we propose a classification based on acceptable thresholds. In the next section, we will classify only the shadowing anomaly. The same study can

be made for other types of anomalies i.e. the generalization, the redundancy and the correlation anomalies.

6.1 The shadowing anomaly importance classification

In this section, we suppose that the administrator has defined acceptable shadowing thresholds SM_S, SM'_S and SM''_S for respectively M_S, M'_S and M''_S metrics. According to M_S, M'_S and M''_S values, we propose the following notations:

- M_S^+ if the value $M_S \leq SM_S$ and M_S^- if the value $M_S > SM_S$
- $M_S'^+$ if the value $M'_S \leq SM'_S$ and $M_S'^-$ if the value $M'_S > SM'_S$
- $M_S''^+$ if the value $M''_S \leq SM''_S$ and $M_S''^-$ if the value $M''_S > SM''_S$

In this way, we can classify the shadowing importance degree compared to the associated SM_S, SM'_S and SM''_S values. The shadowing anomaly importance degree in a rule can belong to one of the eight following classes:

$M_S^+M_S'^+M_S''^+$, $M_S^-M_S'^+M_S''^+$, $M_S^+M_S'^-M_S''^+$, $M_S^+M_S'^+M_S''^-$, $M_S^-M_S'^+M_S''^-$, $M_S^-M_S'^-M_S''^+$, $M_S^+M_S'^-M_S''^-$, $M_S^-M_S'^-M_S''^-$

Figure 2, gives a classification of the eight shadowing anomaly importance classes in a rule from the worst one ($M_S^-M_S'^-M_S''^-$) to the best one ($M_S^+M_S'^+M_S''^+$).

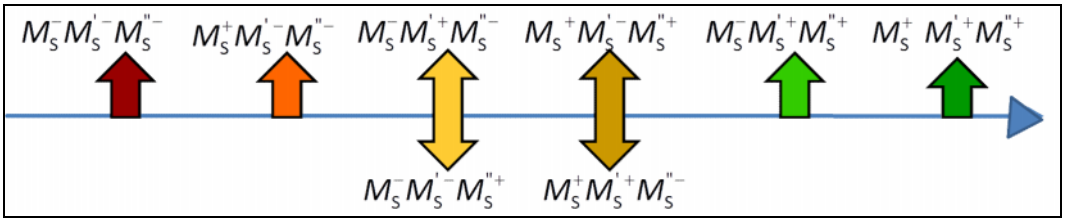

Figure 2. Classification of the shadowing anomaly importance classes

The ideal is that the rule belongs to the class $M_S^+M_S'^+M_S''^+$ i.e. the three metrics are lower than their respective thresholds SM_S, SM'_S and SM''_S. A rule belonging to the class $M_S^-M_S'^-M_S''^-$ is a critical rule since all its metrics are higher than their respective thresholds SM_S, SM'_S and SM''_S.

In figure 2, we notice that the measure classes $M_S^+M_S'^-M_S''^+$ and $M_S^+M_S'^+M_S''^-$ (as far as $M_S^-M_S'^+M_S''^-$ and $M_S^-M_S'^-M_S''^+$) are classified with the same rank. From our point of view, the semantic measure M'_S and the multi-anomalies measure M''_S are equivalent considering that they have generally the same importance. However, the administrator can give more importance to one of these two metrics and thus change the classification.

6.1.1 Case study

Based on the shadowing evaluation metrics defined above, we suppose that the administrator has fixed the thresholds values as follows: $SM_S = 0,2$; $SM'_S = 0,7$ and $SM''_S = 0,6$. If we take the shadowing rule r_1 values: $M_S(r_1) = 0,333$; $M'_S(r_1) = 0,83$ and $M''_S(r_1) = 0,5$ (see sections 5.2.2, 5.2.4 and 5.2.6) , this latter belongs to the class $M_S^- M'^-_S M''^+_S$ (see figure 3). This class is 5th according to the proposed classification in figure 2, which implies that the rule r_1 is critical.

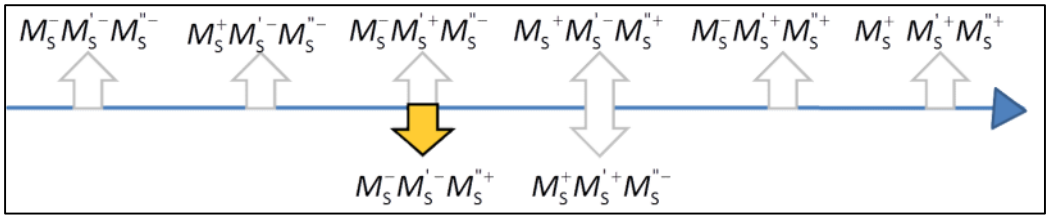

Figure 3. The rule r_1 shadowing anomaly importance representation

To further specify the impact of the shadowing rule r_1, we will illustrate its evaluations values relatively to the acceptable thresholds defined above in a three-dimensional benchmark composed of three axes: the axis M_s, the axis M'_s and the axis M''_s. In figure 4, the thresholds values defined above represent the vertexes of the green triangle. The shadowing r_1 evaluation values $M_S(r_1)$, $M'_S(r_1)$ and $M''_S(r_1)$ represent the vertexes of the red triangle.

Any red triangle included/coinciding in/to the green triangle indicates that its metrics values are acceptables. Exceeding any side of the triangle indicates that the corresponding measure is critical.

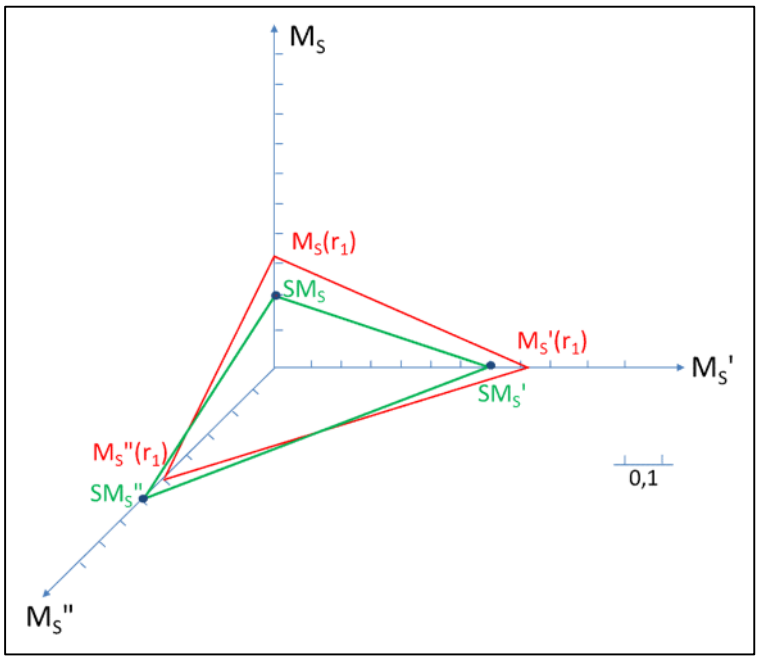

Figure 4. The rule r_1 shadowing anomaly evaluation metrics representation

In our case study, the vertexes of the red triangle represent the rule r_1 evaluation values. We note that these latter exceed those of the green triangle on the side of axes M_s and M'_s. Based on results returned in sections 5.2.2 and 5.2.4, this is explained as follows:
-From the side of the axis M_s, the quantitative measure M_s (r_1) exceeds the threshold SM_s, this is due to the large number of rules masked by r_1.
-From the side of the axis M'_s, the semantic measure $M'_s(r_1)$ exceeds the threshold S M'_s. This is due to the value ANY in the "destination port" attribute, that accepts all incoming flow and therefore, this port can be easily attacked.

7. CONCLUSION

In this paper, we evaluated the severity importance of anomalies with 3 manners; a quantitative evaluation, a semantic evaluation and a multi-anomalies evaluation. The quantitative evaluation showed us the number of rules involved in each type of anomaly. However, this first metric lack of semantic i.e. it does not display the impact of the anomaly on the security component base rules. As a complementary metric, we have defined the semantic metric. This metric allows us to determine the degree of vulnerability of each service involved in the anomaly. In addition, we noted that there are rules involved in more than one anomaly. Therefore, we proceeded to a "multi-anomalies" assessment to show the impact of anomalies combination on the rule. In addition, we exploited this information by classifying the impact of these errors on the network security by a set of diagrams.

REFERENCES

[1] P. Eronen, and J. Zitting, 2001. An Expert System for Analyzing Firewall Rules. Proceedings of 6th Nordic Workshop on Secure IT-Systems.

[2] J. Garcia-Alfaro, F.Cuppens, and N. Cuppens-Boulahia, Analysis of Policy Anomalies on Distributed Network Security Setups. Proceedings of the 11th European Symposium on research in computer security (ESORICS 2006), Hamburg, Germany.

[3] H. Hamed, E. Al-Shaer, and W. Marrero, Modeling and Verification of IPsec and VPN Security Policies. Proc. 13th IEEE Int'l Conf. Network Protocols (ICNP '2005), pp. 259-278.

[4] E. Al-Shaer, H.Hamed, R. Boutaba, M. Hasan, Conflict classification and analysis of distributed firewall policies, IEEE Journal on Selected Areas in Communications (JSAC) 2005, pp. 2069–2084.

[5] E. Al-Shaer, and H. Hamed, Discovery of Policy Anomalies in Distributed Firewalls, Proc. IEEE INFOCOM '2004, pp. 2605-2615.

[6] A.X. Liu, and M. Gouda, Complete Redundancy Detection in Firewalls, Proc. 19th Ann. IFIP Conf. Data and Applications Security (2005), pp. 196-209.

[7] M. Gouda, and A.X. Liu, A Model of Stateful Firewalls and Its Properties, Proc. IEEE Int'l Conf. Dependable Systems and Networks (DSN '2005), pp. 320-327.

[8] SP. Pornavalai, and T. Chomsiri, Analyzing Firewall Policy with Relational Algebra and its Application. Australian Telecommunication Networks and Applications Conference (ATNAC 2004), Australia.

[9] F. Ben Ftima, K. Karoui and H. Ben Ghezala, A multi-agent framework for anomalies detection on distributed firewalls using data mining techniques. Springer Verlag "Data Mining and Multi-agent Integration", 2009. ISBN: 978-1-4419-0523-9, pp267-278.[10]A.X. Liu, Firewall Policy Verification and Troubleshooting, Proc. IEEE Int'l Conf. Comm. (ICC) 2008.