

#OWASP = 22

Per ottimizzare il processo di posizionamento delle regole owasp bisogna aggregare tutti i flussi di indirizzi diversi con stesse regole, ove non venga escluso alcun flusso:

source	destination	owasp
10.0.0.1	20.0.0.1	ow1
10.0.0.2	20.0.0.1	ow2
10.0.0.3	20.0.0.1	ow3

In questo caso non posso aggregare niente e avrò tre flussi distinti.

source	destination	owasp
10.0.0.1	20.0.0.1	ow1
10.0.0.2	20.0.0.1	ow2
10.0.0.3	20.0.0.1	ow2

Aggregazione non possibile, non possiamo usare 10.0.0.\* 20.0.0.1 ow2 in quanto implicherebbe protezione sul primo flusso con ow2.

source	destination	owasp
10.0.0.1	20.0.0.1	ow1 ow2 ow3
10.0.0.2	20.0.0.1	ow2
10.0.0.3	20.0.0.1	ow2 ow3 ow4

Aggregazione possibile ma #elementi invariato:

source	destination	owasp
10.0.0.1	20.0.0.1	ow1 ow3
10.0.0.*	20.0.0.1	ow2
10.0.0.3	20.0.0.1	ow3 ow4

source	destination	owasp
10.0.0.1	20.0.0.1	ow1
10.0.0.2	20.0.0.1	ow1
10.0.0.3	20.0.0.1	ow1 ow2 ow3

Aggregazione possibile:

source	destination	owasp
10.0.0.*	20.0.0.1	ow1
10.0.0.3	20.0.0.1	ow2 ow3

Un modello con questo tipo di aggregazioni implica che su ogni flusso debbano esserci tutte le regole specificate e NON debbano essercene altre non richieste.

Si definisca  $O_s$  il set di regole OWASP attivabili nel contesto di un dato flusso di un firewall. Ogni  $o \in O_s$  è formato dalla coppia  $(O_i, a)$ , dove  $O_i$  rappresenta la precisa regola owasp e  $a$  l'azione da eseguire che può essere *true* nel caso la regola debba essere attivata oppure *false* nel caso la regola non debba essere attivata.

La relazione matematica tra le regole attivate e le altre è la seguente:

$$\forall (O_i, a), a = true \Rightarrow \bigwedge_{j \neq i} (O_j, \neg a)$$

Pertanto l'utilità di tali aggregazioni è limitata a pochi specifici casi, in cui

tutti i flussi o la maggior parte abbiano le stesse e sole regole owasp, ove si ridurrebbe effettivamente la quantità di elementi “owasp\_rules” all’interno dei firewall allocati

Sia  $F_o$  l’insieme di flussi che collegano un client o una sottorete ad uno specifico server, per ogni  $o \in O_s$  con  $a=true$ , se non esiste alcun flusso  $f$  appartenente ad  $F_o$  che non contiene  $o$ , allora  $o$  può essere aggregato in  $O_s$ .

$\forall o \in O_s : (\nexists f \in F : o \notin f \cap a(o) = true) \Rightarrow Soft(agggregatable(o) = true)$