PROJET SISE-OPSIE 2022

SISE : Hamza Fassi - Pierre Le Galeze - Sami Ait Tilat

OPSIE : Bachir Oufaquir - Badereddine Touati

```
knitr::opts_chunk$set(echo = TRUE)
```

```
src_fw <- read.table("logs_fw-3.csv",sep=";",header=1)
```

```
#install.packages("scales")
library(dplyr)
```

```
## Warning: le package 'dplyr' a été compilé avec la version R 4.1.2
```

```
##
## Attachement du package : 'dplyr'
```

```
## Les objets suivants sont masqués depuis 'package:stats':
##
##     filter, lag
```

```
## Les objets suivants sont masqués depuis 'package:base':
##
##     intersect, setdiff, setequal, union
```

```
library(ggplot2)
```

```
## Warning: le package 'ggplot2' a été compilé avec la version R 4.1.2
```

```
library(scales)
```

```
## Warning: le package 'scales' a été compilé avec la version R 4.1.2
```

Migration et préparation des données

```
src_fw <- src_fw %>%
  mutate(Status = case_when(
    dstport==20 ~ "FTP ",
    dstport==21 ~ "FTP ",
    dstport==22 ~ "SSH ",
    dstport==23 ~ "Telnet",
    dstport==80 ~ "HTTP",
    dstport==3306 ~ "MYSQL"

  ))
```

Classement des règles les plus utilisées

```
regle <- src_fw %>%
  count(policyid)
head(regle[order(-regle$n),],10)
```

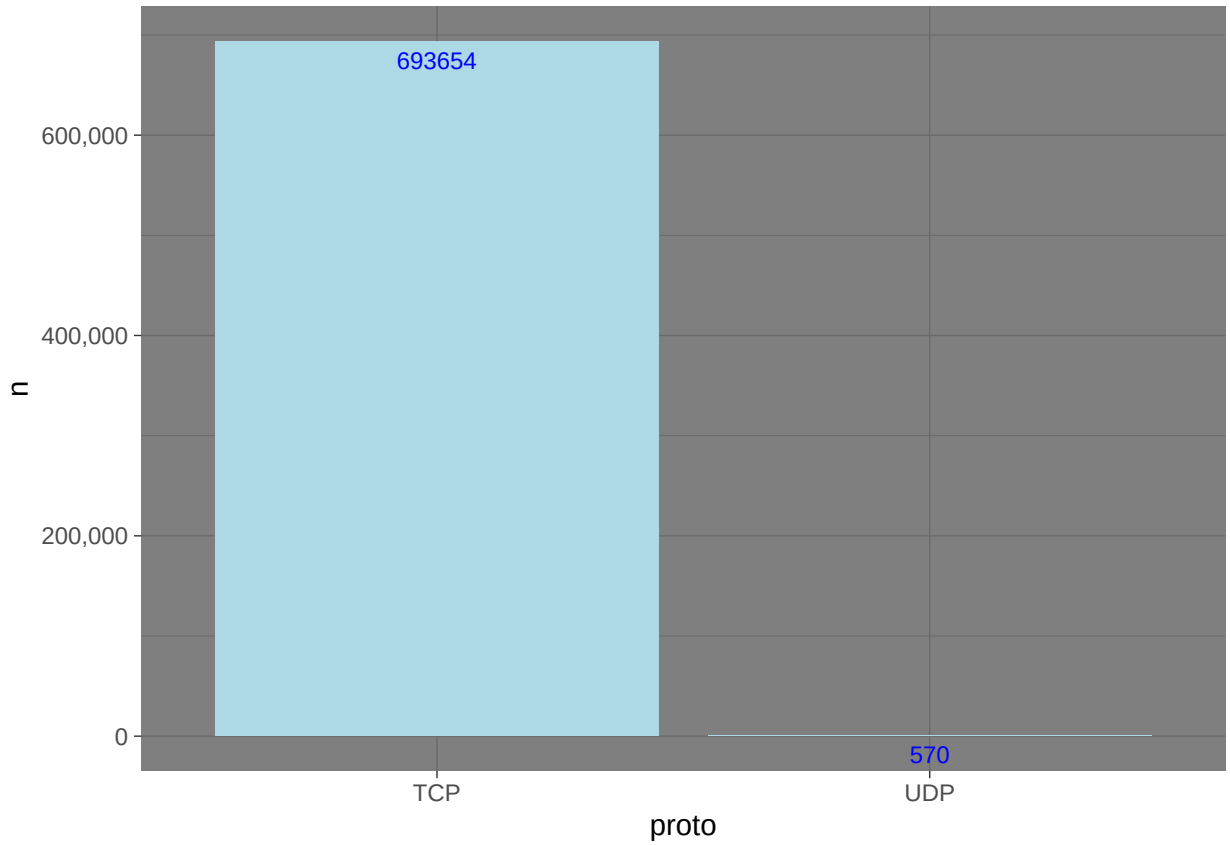
```
##    policyid      n
## 12      999 313289
## 1         1 126337
## 3         3  85273
## 6         6  64802
## 7         7  51973
## 10       17  39302
## 4         4   6391
## 9        16   3611
## 5         5   1954
## 8        13    730
```

Classement des règles les plus utilisées

```
proto <- src_fw %>%
  count(proto)
```

Histogramme du Classement des règles les plus utilisées

```
ggplot(data=proto, aes(x=proto, y=n)) +
  geom_bar(stat="identity",fill="lightblue" )+
  theme_dark()+
  scale_y_continuous(labels = comma)+
  geom_text(aes(label=n), vjust=1.6, colour="blue", size =3)
```



Top dix des règles les plus utilisées avec le protocole Udp

```
src_fwUDP <- src_fw[which(src_fw$proto == "UDP"), ]
portUDP <- src_fwUDP %>%
  count(dstport)
B <- head(portUDP[order(-portUDP$n),],10)
B
```

```
##    dstport  n
## 27    5060 50
## 5      123 35
## 8      389 34
## 17    1900 33
## 2       19 26
## 3       53 26
## 7      161 25
## 44   11211 25
## 51   27015 25
## 1       17 24
```

Top dix des règles les plus utilisées avec le protocole TCP

```
src_fwTCP <- src_fw[which(src_fw$proto == "TCP"), ]
portTCP <- src_fwTCP %>%
  count(dstport)
A <- head(portTCP[order(-portTCP$n),],5)
A
```

```
##      dstport     n
## 446      445 96115
## 23        22 92530
## 81        80 50578
## 444      443 15915
## 8081    8080  9151
```

Rapprochement des règles (rule id) par rapport aux ports de destination et les actions

Rapprochement des règles pour le cas où : Proto = “TCP”

```
for (i in unique(src_fwTCP$policyid)){
  print(paste("Règle :",i))
  subset=subset(src_fwTCP,policyid==i)
  print("Port de destination:")
  res=head(sort(table(subset$dstport),decreasing=T),10)
  print(names(res))
  print("Fréquence associées :")
  print(res)
}
```

```
## [1] "Règle : 999"
## [1] "Port de destination:"
##  [1] "8080" "8088" "465"  "1433" "3074" "3478" "1197" "81"   "139"  "6379"
## [1] "Fréquence associées :"
##
## 8080 8088  465 1433 3074 3478 1197   81  139 6379
## 8122 3833 3638 3201 2121 2121 1769 1707 1592 1374
## [1] "Règle : 1"
## [1] "Port de destination:"
##  [1] "445"  "80"   "22"   "3389" "3390" "3391" "3392" "3128" "3399" "443"
## [1] "Fréquence associées :"
##
##   445    80    22  3389  3390  3391  3392  3128  3399   443
## 10908  1313  1223   621   348   285   241   238   232   226
## [1] "Règle : 17"
## [1] "Port de destination:"
## [1] "22"
## [1] "Fréquence associées :"
```

```
##    22
## 39302
## [1] "Règle : 7"
## [1] "Port de destination:"
## [1] "22"
## [1] "Fréquence associées :"
##    22
## 51973
## [1] "Règle : 3"
## [1] "Port de destination:"
## [1] "445" "135"
## [1] "Fréquence associées :"
##
##   445   135
## 85100   173
## [1] "Règle : 6"
## [1] "Port de destination:"
## [1] "80"  "443"
## [1] "Fréquence associées :"
##
##    80   443
## 49146 15656
## [1] "Règle : 4"
## [1] "Port de destination:"
## [1] "23"
## [1] "Fréquence associées :"
##   23
## 6391
## [1] "Règle : 5"
## [1] "Port de destination:"
## [1] "3389"
## [1] "Fréquence associées :"
## 3389
## 1954
## [1] "Règle : 18"
## [1] "Port de destination:"
## [1] "20000"
## [1] "Fréquence associées :"
## 20000
##   189
## [1] "Règle : 2"
## [1] "Port de destination:"
##  [1] "80"   "445"  "23"   "443"  "22"   "465"  "8080" "5555" "85"   "2005"
## [1] "Fréquence associées :"
##
##   80  445   23  443   22  465 8080 5555   85 2005
##  119  107   38   33   32   12   10    2    1    1
## [1] "Règle : 13"
## [1] "Port de destination:"
## [1] "3306"
## [1] "Fréquence associées :"
## 3306
##  730
## [1] "Règle : 16"
```

```
## [1] "Port de destination:"
## [1] "3074" "8080" "3478" "465"  "1197"
## [1] "Fréquence associées :"
##
## 3074 8080 3478  465 1197
##  852  832  821  802  304
```

#Rapprochement des règles pour le cas où : Proto = “TCP” et action= “DENY”.

```
src_fwTCPDENY <- src_fwTCP[which(src_fwTCP$action == "DENY"), ]
for (i in unique(src_fwTCPDENY$policyid)){
  print(paste("Règle :",i))
  subset=subset(src_fwTCPDENY,policyid==i)
  print("Port de destination:")
  res=head(sort(table(subset$dstport),decreasing=T),10)
  print(names(res))
  print("Fréquence associées :")
  print(res)
}
```

```
## [1] "Règle : 999"
## [1] "Port de destination:"
##  [1] "8080" "8088" "465"  "1433" "3074" "3478" "1197" "81"   "139"  "6379"
## [1] "Fréquence associées :"
##
## 8080 8088  465 1433 3074 3478 1197   81  139 6379
## 8122 3833 3638 3201 2121 2121 1769 1707 1592 1374
## [1] "Règle : 1"
## [1] "Port de destination:"
##  [1] "445"  "80"   "22"   "3389" "3390" "3391" "3392" "3128" "3399" "443"
## [1] "Fréquence associées :"
##
##   445    80    22  3389  3390  3391  3392  3128  3399   443
## 10908  1313  1223   621   348   285   241   238   232   226
## [1] "Règle : 17"
## [1] "Port de destination:"
## [1] "22"
## [1] "Fréquence associées :"
##    22
## 39302
## [1] "Règle : 3"
## [1] "Port de destination:"
## [1] "445" "135"
## [1] "Fréquence associées :"
##
##   445   135
## 85100   173
## [1] "Règle : 4"
## [1] "Port de destination:"
## [1] "23"
## [1] "Fréquence associées :"
##   23
## 6391
```

```
## [1] "Règle : 5"
## [1] "Port de destination:"
## [1] "3389"
## [1] "Fréquence associées :"
## 3389
## 1954
## [1] "Règle : 18"
## [1] "Port de destination:"
## [1] "20000"
## [1] "Fréquence associées :"
## 20000
##   189
## [1] "Règle : 2"
## [1] "Port de destination:"
##  [1] "80"   "445"  "23"   "443"  "22"   "465"  "8080" "5555" "85"   "2005"
## [1] "Fréquence associées :"
##
##   80  445   23  443   22  465 8080 5555   85 2005
##  119  107   38   33   32   12   10    2    1    1
## [1] "Règle : 13"
## [1] "Port de destination:"
## [1] "3306"
## [1] "Fréquence associées :"
## 3306
##  730
## [1] "Règle : 16"
## [1] "Port de destination:"
## [1] "3074" "8080" "3478" "465"  "1197"
## [1] "Fréquence associées :"
##
## 3074 8080 3478  465 1197
##  852  832  821  802  304
```

Rapprochement des règles pour le cas où : Proto = “TCP” et action= “PERMIT”.

```
src_fwTCPPERMIT <- src_fwTCP[which(src_fwTCP$action == "PERMIT"), ]
for (i in unique(src_fwTCPPERMIT$policyid)){
  print(paste("Règle :",i))
  subset=subset(src_fwTCPPERMIT,policyid==i)
  print("Port de destination:")
  res=head(sort(table(subset$dstport),decreasing=T),10)
  print(names(res))
  print("Fréquence associées :")
  print(res)
}
```

```
## [1] "Règle : 7"
## [1] "Port de destination:"
## [1] "22"
## [1] "Fréquence associées :"
```

```
##    22
## 51973
## [1] "Règle : 6"
## [1] "Port de destination:"
## [1] "80"  "443"
## [1] "Fréquence associées :"
##
##    80   443
## 49146 15656
```

Rapprochement des règles pour le cas où : Proto = “UDP” et action =“DENY”.

```
src_fwUDPDENY <- src_fwUDP[which(src_fwUDP$action == "DENY"), ]

for (i in unique(src_fwUDPDENY$policyid)){
  print(paste("Règle :",i))
  subset=subset(src_fwUDPDENY,policyid==i)
  print("Port de destination:")
  res=head(sort(table(subset$dstport),decreasing=T),10)
  print(names(res))
  print("Fréquence associées :")
  print(res)
}
```

```
## [1] "Règle : 1"
## [1] "Port de destination:"
##  [1] "5060"  "123"   "389"   "1900"  "19"    "53"    "161"   "11211" "27015"
## [10] "17"
## [1] "Fréquence associées :"
##
##  5060   123   389  1900    19    53   161 11211 27015    17
##    49    35    34    33    26    26    25    25    25    24
## [1] "Règle : 2"
## [1] "Port de destination:"
## [1] "1027" "6881" "1434" "5060" "8080" "8081"
## [1] "Fréquence associées :"
##
## 1027 6881 1434 5060 8080 8081
##    2    2    1    1    1    1
```

Rapprochement des règles pour le cas où : Proto = “UDP”

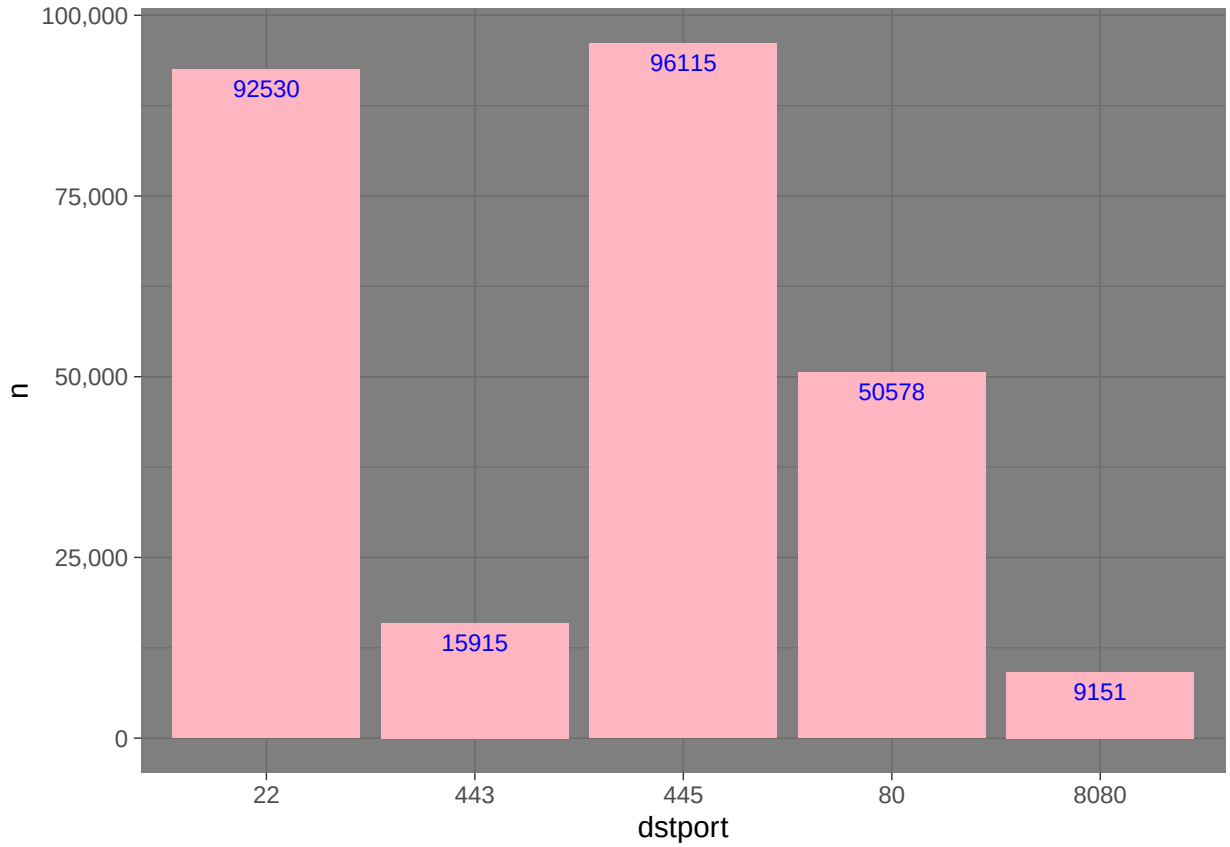
```
for (i in unique(src_fwUDP$policyid)){
  print(paste("Règle :",i))
  subset=subset(src_fwUDP,policyid==i)
  print("Port de destination:")
  res=head(sort(table(subset$dstport),decreasing=T),10)
```

```
  print(names(res))
  print("Fréquence associées :")
  print(res)
}
```

```
## [1] "Règle : 1"
## [1] "Port de destination:"
##  [1] "5060"  "123"   "389"   "1900"  "19"    "53"    "161"   "11211" "27015"
## [10] "17"
## [1] "Fréquence associées :"
##
##  5060   123   389  1900    19    53   161 11211 27015    17
##    49    35    34    33    26    26    25    25    25    24
## [1] "Règle : 2"
## [1] "Port de destination:"
## [1] "1027" "6881" "1434" "5060" "8080" "8081"
## [1] "Fréquence associées :"
##
## 1027 6881 1434 5060 8080 8081
##    2    2    1    1    1    1
```

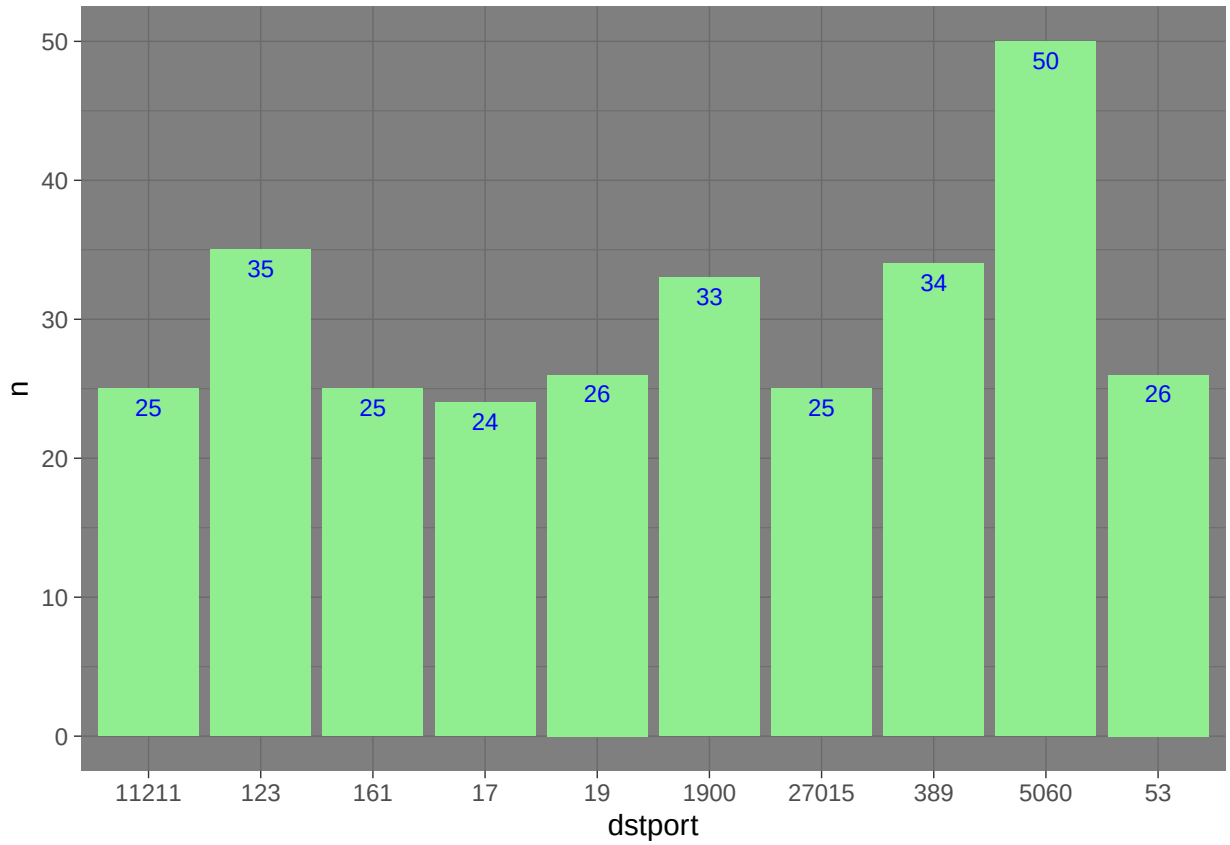
Graphe des top 5 des régles les plus utilisees avec le protocole TCP

```
A$dstport <- as.character(A$dstport)
ggplot(data=A, aes(x=dstport, y=n)) +
  geom_bar(stat="identity",fill="lightpink" )+
  theme_dark()+
  scale_y_continuous(labels = comma)+
  geom_text(aes(label=n), vjust=1.6, colour="blue", size =3)
```



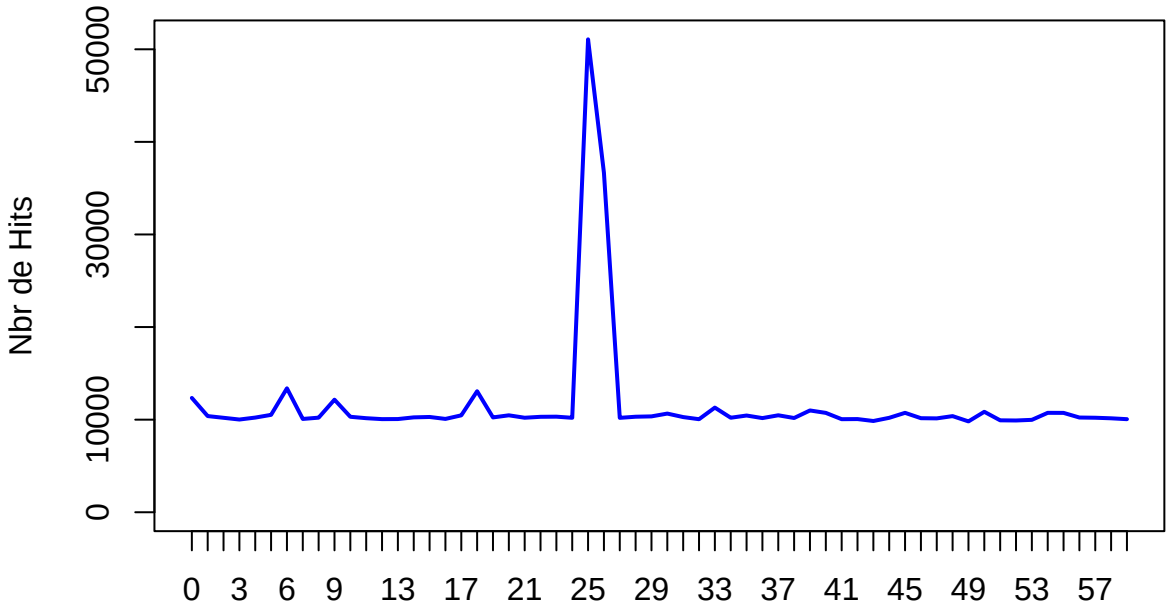
Graphe des Top dix des règles les plus utilisées avec le protocole Udp

```
B$dstport <- as.character(B$dstport)
ggplot(data=B, aes(x=dstport, y=n)) +
  geom_bar(stat="identity",fill="lightgreen" )+
  theme_dark()+
  scale_y_continuous(labels = comma)+
  geom_text(aes(label=n), vjust=1.6, colour="blue", size =3)
```



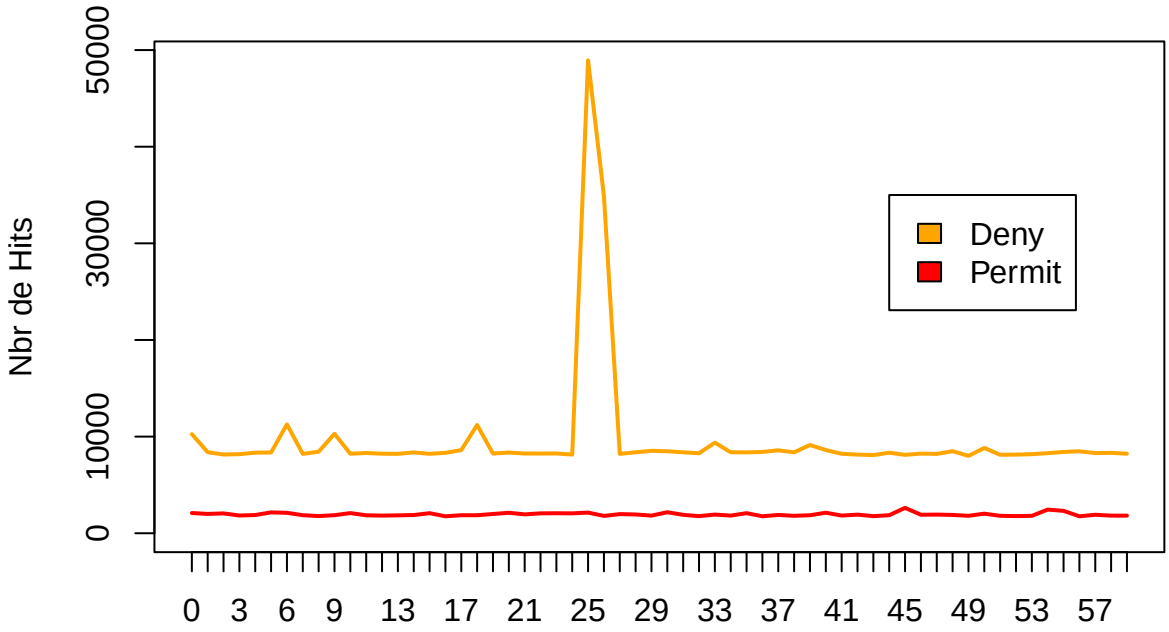
L'exemple ci-dessous montre une courbe représentant le trafic réseau dans son ensemble

```
src_fw$datetime <-strptime(src_fw$datetime, "%Y-%m-%d %H:%M:%S")
plot(table(src_fw$datetime$min),type="l", col="blue", ylab = "Nbr de Hits")
```



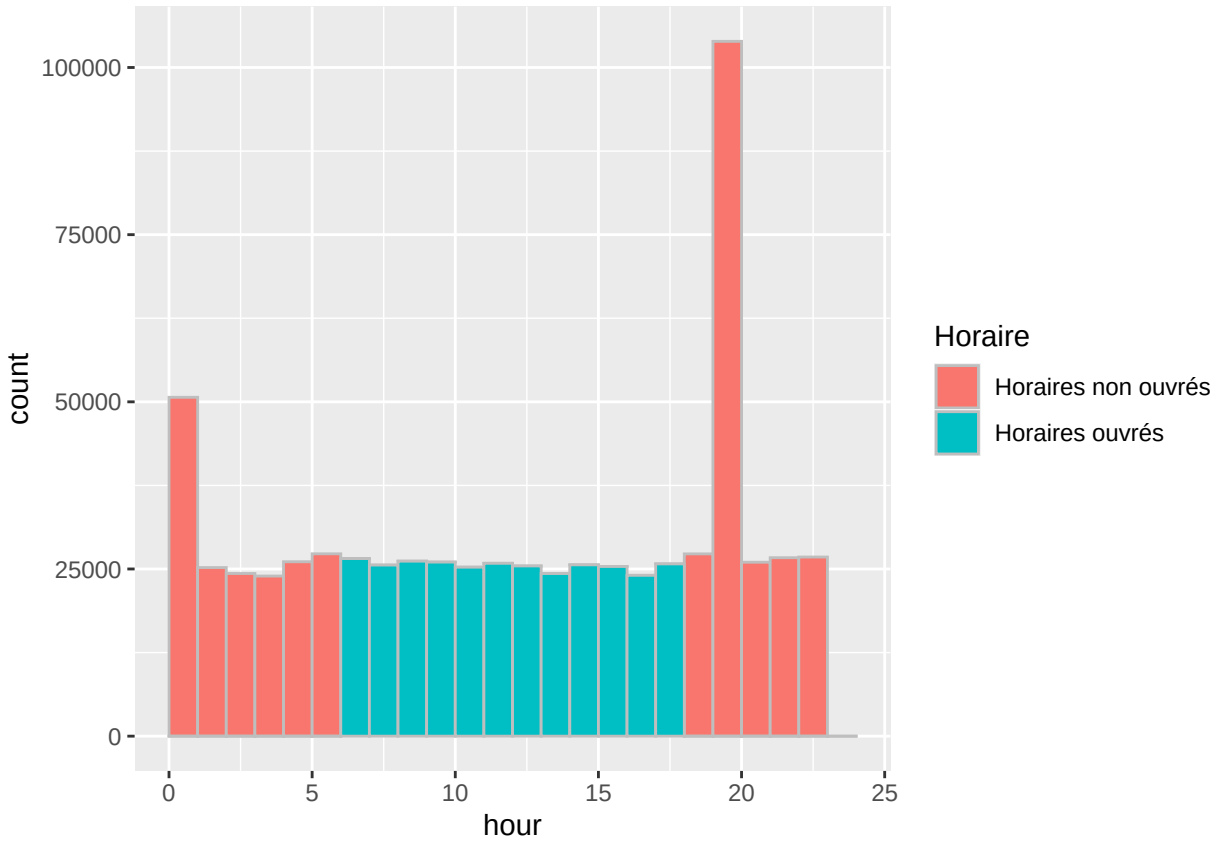
L'exemple ci-dessous permet de comparer les flux réjetés et autorisées en TCP. Les flux rejetés semblent stables

```
src_fwPermit <- src_fw[which(src_fw$action == "PERMIT"), ]
src_fwDeny<- src_fw[which(src_fw$action == "DENY"), ]
plot(table(src_fwDeny$datetime$min),type="l", col=" orange", ylab = "Nbr de Hits")
lines(table(src_fwPermit$datetime$min),col="red",type="l")
legend(44, 35000, legend=c("Deny", "Permit"),
       fill = c("orange","red")
)
```



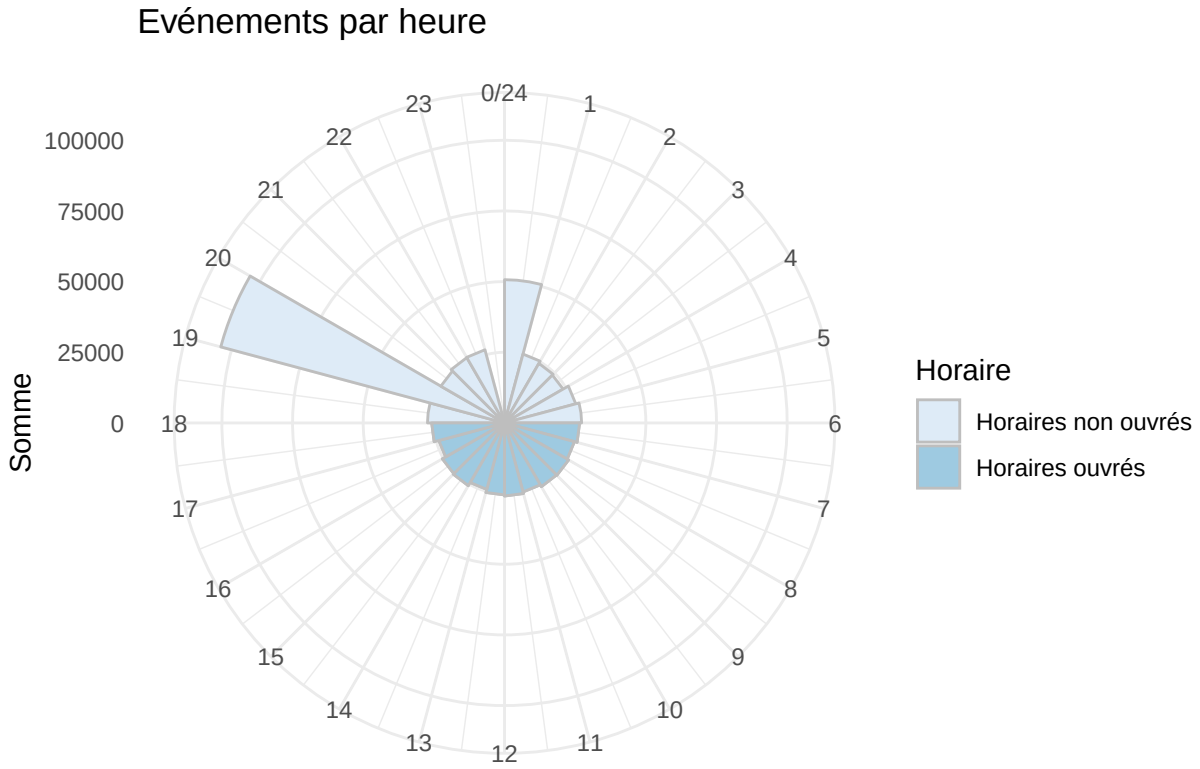
Visualisation des accès nocturnes

```
df2 <- data.frame(datetime =src_fw$datetime,hour=src_fw$datetime$hour )
df2$Horaire <- df2$hour %in% seq(7,18)
df2$Horaire[df2$Horaire=='TRUE']<-"Horaires ouvrés"
df2$Horaire[df2$Horaire=='FALSE']<-"Horaires non ouvrés"
ggplot(df2,aes(x=hour,fill=Horaire)) + geom_histogram(breaks=seq(0,24),colour="grey")
```



Ou encore le graphe ci-dessous :

```
ggplot(df2,aes(x=hour,fill=Horaire)) + geom_histogram(breaks=seq(0,24),colour="grey")+
  coord_polar(start=0)+theme_minimal()+scale_fill_brewer()+ylab("Somme")+ggtitle("Evénements par heure")
  scale_x_continuous("",limits =c(0,24),breaks=seq(0,24),labels=seq(0,24))
```


Evénements par heure
Somme
100000
75000
50000
25000
0
0/24
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
Horaire
Horaires non ouvrés
Horaires ouvrés