Justificación FireWall

FERTSPA STUDIOS

2019

ESI-BUCEO

MONTEVIDEO

Decidimos que nuestro FireWall sería uno restrictivo ya que este a pesar de ser más difícil de configurar, se adapta mejor a lo que ofrecemos como empresa. Gracias a que el mismo es restrictivo mantendremos controlado como los distintos operarios utilizan la conexión a internet y además mantendremos más seguros nuestra red de ataques externos. Por último, solo queda decir que en nuestro FireWall solo habilitaremos los puertos necesarios para el funcionamiento de la red y de todo lo que el programa necesita.

```
#!/bin/bash
#Ver 1.5 - Fertspa
#
#Release notes: se agrega script de Firewall
##

#Flush de reglas para evitar inconvenientes a la hora de aplicar reglas nuevas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

#Utilizaremos protocolo restrictivo
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -P PREROUTING DROP
iptables -t nat -P POSTROUTING DROP

#Dejamos localhost y nuestra ip
iptables -A INPUT -s 192.168.1.100 -j ACCEPT
verificar
/sbin/iptables -A INPUT -i lo -j ACCEPT
verificar

#Habilitamos puerto de SSH para administración del servidor
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
verificar

#Habilitamos puerto 9088 para Informix
iptables -A INPUT -p tcp --dport 9088 -j ACCEPT
verificar

#Fin de reglas
verificar()
{
        if [ "$?" -eq "0" ]
                echo -e "Las reglas se aplicaron exitosamente\n"
        else
                echo -e "Hubo un error de sintaxis al aplicar las reglas\n"
        fi
}
##Fin de script ----------------
```