開発技術全般 - 報告書 #1094
CentOS7でiptablesではなくfirewalldを使った方法

2017/08/18 18:28 - 匿名ユーザー

ステータス:	新規	**開始日:**	2017/08/18
優先度:	通常	**期日:**	
担当者:		**作業時間の記録:**	0.00時間
カテゴリ:			

説明

セキュリティ対策をiptablesでやろうとしてもCentOS7では上手く出来ませんでした。
そこでfirewalldを使った方法です。

「参考サイト」
https://www.imd-net.com/column/13339/

（firewalldの状態を確認、起動。unmaskはmaskしてた場合の解除）
$ systemctl status firewalld
$ systemctl unmask firewalld
$ systemctl enable firewalld
$ systemctl start firewalld

（http,https通信を許可）

$ firewall-cmd --add-service=http --zone=public --permanent
$ firewall-cmd --add-service=https --zone=public --permanent
$ systemctl restart firewalld

（SSH通信を特定のIPだけ許可する）

・SSHサーバーのポートを永続的に閉じる。
$ firewall-cmd --permanent --remove-service=ssh

・sshd_configで指定したポート22番、特定のIPを永続的に許可する。
（上はアイハーツのグローバルIP、下はnagiosのチェックのため）
$ firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv4" source address="153.156.40.213" port protocol="tcp" port="22" accept"
$ firewall-cmd --permanent --zone=public --add-rich-rule="rule family="ipv4" source address="49.212.24.211" port protocol="tcp" port="22" accept"

・再起動
$ firewall-cmd --reload

履歴

#1 - 2017/12/15 17:47 - 匿名ユーザー

https://qiita.com/MATO/items/e8ae2b528fe9ddc4c25a

#2 - 2017/12/27 10:20 - 匿名ユーザー

・ポートの開放

```
$ firewall-cmd --zone=public --add-port=8000/tcp --permanent
$ firewall-cmd --zone=public --add-port=9000/tcp --permanent

$ firewalld-cmd --reload
```