目次

Firewall の設定 (ufw)

Ubuntu Linux標準のFirewall設定ツール ufw[1] が使用できます[2]
標準の状態ではFirewallを有効にしていませんので、例として

- SSH(TCP/22)へのアクセスだけ有効
- 他のアクセスはすべてDROP

という設定をする方法を紹介します。

ufw の設定

現在の状態の確認

デフォルトではFirewallは無効になっています。
コマンドで確認してみます。

```
user1@plum:~$ sudo ufw status
[sudo] password for user1:
Status: inactive
user1@plum:~$
```

iptables がどのように設定されているかについても、あわせて確認してみます。

```
user1@plum:~$ sudo iptables-save
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:05:50 2014
*nat
:PREROUTING ACCEPT [1247:244112]
:INPUT ACCEPT [38:5046]
:OUTPUT ACCEPT [1:76]
:POSTROUTING ACCEPT [1:76]
COMMIT
# Completed on Mon Mar 31 11:05:50 2014
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:05:50 2014
*mangle
:PREROUTING ACCEPT [1728:287458]
:INPUT ACCEPT [519:48392]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [327:37342]
:POSTROUTING ACCEPT [327:37342]
COMMIT
# Completed on Mon Mar 31 11:05:50 2014
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:05:50 2014
*filter
:INPUT ACCEPT [526:48756]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [334:38266]
```

```
COMMIT
# Completed on Mon Mar 31 11:05:50 2014
user1@plum:~$
```

“filter” の部分を見てわかるとおり、INPUT/FORWARD/OUTPUT がすべて “ACCEPT” になっており、
確かに Firewall は無効であることが確認できます。

フィルタ設定の追加

フィルタの設定を追加する前に ufw を有効化してしまうと、sshでの接続が不可能となり、なにも操作できなくなってしまいます。
まずは、下記の通り設定をします。

- INPUTのデフォルトポリシー ⇒ DENY (設定されていないもの: アクセス拒否)
- ssh ⇒ アクセス許可

```
user1@plum:~$ sudo ufw default DENY
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
user1@plum:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
user1@plum:~$
```

ufw の状態を確認してみます。

```
user1@plum:~$ sudo ufw status
Status: inactive
user1@plum:~$
```

有効化していませんので、まだ “inactive” のままです。

ufw の有効化

sshでアクセスできるようルールを追加しましたので、ufw を有効化してみます。

```
user1@plum:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)?
y
Firewall is active and enabled on system startup
user1@plum:~$
```

ufw の状態を確認します。

```
user1@plum:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
22                         ALLOW       Anywhere (v6)

user1@plum:~$
```

22番ポートへのアクセスが許可されているようです。

先ほどと同様に、iptables がどのように設定されたかを確認してみます。

```
user1@plum:~$ sudo iptables-save
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:22:36 2014
*nat
:PREROUTING ACCEPT [2375:465583]
:INPUT ACCEPT [69:9297]
:OUTPUT ACCEPT [1:76]
:POSTROUTING ACCEPT [1:76]
COMMIT
# Completed on Mon Mar 31 11:22:36 2014
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:22:36 2014
*mangle
:PREROUTING ACCEPT [3492:558411]
:INPUT ACCEPT [1199:103509]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [775:93716]
:POSTROUTING ACCEPT [775:93716]
COMMIT
# Completed on Mon Mar 31 11:22:36 2014
# Generated by iptables-save v1.4.18 on Mon Mar 31 11:22:36 2014
*filter
:INPUT DROP [5:272]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-logging-allow - [0:0]
:ufw-logging-deny - [0:0]
```

```
:ufw-not-local - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-skip-to-policy-forward - [0:0]
:ufw-skip-to-policy-input - [0:0]
:ufw-skip-to-policy-output - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
:ufw-user-forward - [0:0]
:ufw-user-input - [0:0]
:ufw-user-limit - [0:0]
:ufw-user-limit-accept - [0:0]
:ufw-user-logging-forward - [0:0]
:ufw-user-logging-input - [0:0]
:ufw-user-logging-output - [0:0]
:ufw-user-output - [0:0]
-A INPUT -j ufw-before-logging-input
-A INPUT -j ufw-before-input
-A INPUT -j ufw-after-input
-A INPUT -j ufw-after-logging-input
-A INPUT -j ufw-reject-input
-A INPUT -j ufw-track-input
-A FORWARD -j ufw-before-logging-forward
-A FORWARD -j ufw-before-forward
-A FORWARD -j ufw-after-forward
-A FORWARD -j ufw-after-logging-forward
-A FORWARD -j ufw-reject-forward
-A OUTPUT -j ufw-before-logging-output
-A OUTPUT -j ufw-before-output
-A OUTPUT -j ufw-after-output
-A OUTPUT -j ufw-after-logging-output
-A OUTPUT -j ufw-reject-output
-A OUTPUT -j ufw-track-output
-A ufw-after-input -p udp -m udp --dport 137 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 138 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp -m tcp --dport 139 -j ufw-skip-to-policy-input
-A ufw-after-input -p tcp -m tcp --dport 445 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 67 -j ufw-skip-to-policy-input
-A ufw-after-input -p udp -m udp --dport 68 -j ufw-skip-to-policy-input
-A ufw-after-input -m addrtype --dst-type BROADCAST -j ufw-skip-to-policy-
input
-A ufw-after-logging-forward -m limit --limit 3/min --limit-burst 10 -j LOG
--log-prefix "[UFW BLOCK] "
-A ufw-after-logging-input -m limit --limit 3/min --limit-burst 10 -j LOG --
log-prefix "[UFW BLOCK] "
-A ufw-before-forward -j ufw-user-forward
-A ufw-before-input -i lo -j ACCEPT
-A ufw-before-input -m state --state RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-input -m state --state INVALID -j ufw-logging-deny
```

```
-A ufw-before-input -m state --state INVALID -j DROP
-A ufw-before-input -p icmp -m icmp --icmp-type 3 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 4 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 12 -j ACCEPT
-A ufw-before-input -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A ufw-before-input -p udp -m udp --sport 67 --dport 68 -j ACCEPT
-A ufw-before-input -j ufw-not-local
-A ufw-before-input -d 224.0.0.251/32 -p udp -m udp --dport 5353 -j ACCEPT
-A ufw-before-input -d 239.255.255.250/32 -p udp -m udp --dport 1900 -j
ACCEPT
-A ufw-before-input -j ufw-user-input
-A ufw-before-output -o lo -j ACCEPT
-A ufw-before-output -m state --state RELATED,ESTABLISHED -j ACCEPT
-A ufw-before-output -j ufw-user-output
-A ufw-logging-allow -m limit --limit 3/min --limit-burst 10 -j LOG --log-
prefix "[UFW ALLOW] "
-A ufw-logging-deny -m state --state INVALID -m limit --limit 3/min --limit-
burst 10 -j RETURN
-A ufw-logging-deny -m limit --limit 3/min --limit-burst 10 -j LOG --log-
prefix "[UFW BLOCK] "
-A ufw-not-local -m addrtype --dst-type LOCAL -j RETURN
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT
-A ufw-track-output -p tcp -m state --state NEW -j ACCEPT
-A ufw-track-output -p udp -m state --state NEW -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 22 -j ACCEPT
-A ufw-user-input -p udp -m udp --dport 22 -j ACCEPT
-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT
BLOCK] "
-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Mon Mar 31 11:22:36 2014
user1@plum:~$
```

すこし長いので□sshがアクセス許可されている部分だけ抜き出してみます。

```
-A ufw-user-input -p tcp -m tcp --dport 22 -j ACCEPT
-A ufw-user-input -p udp -m udp --dport 22 -j ACCEPT
```

このとおり、22番ポートへのアクセスが許可されていることがわかります。

1)

https://wiki.ubuntu.com/UncomplicatedFirewall
[2)]

v2.2.0 からは□FirewallD に移行します