【iptables遮断への変更手順書】

firewalld 遮断方式のお客様は本手順にて、iptables 遮断への変更を実施してください。

【入れ替え対象のスクリプト】

・firewall-drop.sh

【前提条件】

本手順は入れ替え対象のスクリプトが/var/ossec配下のディレクトリにインストールされているものとして記載しております。
別ディレクトリにインストールされている場合は、適宜読み替えの上ご利用ください。
また、コマンドの実行は、管理者権限で実行してください。

【変更手順】

1. iptables-servicesパッケージをインストール

yum install iptables-services

2. ossecを停止

/var/ossec/bin/ossec-control stop

3. ossecの停止を確認

/var/ossec/bin/ossec-control status

[停止している状態]
ossec-logcollector not running...
ossec-syscheckd not running...
ossec-agentd not running...
ossec-execd not running...

4. 攻撃遮断くんが追加したIPアドレスの削除を確認

iptables -nL
tail -f /var/ossec/logs/active-responses.log

以下のように該当IPアドレスがdeleteされていることを確認してください。

2020年 12月 15日 火曜日 20:14:48 JST
/var/ossec/active-response/bin/host-deny.sh delete - xxx.xxx.xxx.xxx
1608030830.236950 200105

2020年 12月 15日 火曜日 20:14:48 JST
/var/ossec/active-response/bin/firewall-drop.sh delete - xxx.xxx.xxx.xxx
1608030830.236950 200105

5. firewalldのルールを保存

iptables -S | tee ~/firewalld_iptables_rules
ip6tables -S | tee ~/firewalld_ip6tables_rules

6. firewalldの停止を実施

systemctl stop firewalld

7. firewalldの停止を確認

systemctl status firewalld

8. firewalldを無効化

systemctl disable firewalld
systemctl mask firewalld

9. iptablesのルールをクリア

```
# iptables -t nat -F
# iptables -t mangle -F
# iptables -F
# iptables -X
# ip6tables -t nat -F
# ip6tables -t mangle -F
# ip6tables -F
# ip6tables -X
```

※iptables-servicesのパッケージのインストール時にINPUT,FORWARDを拒否する設定が含まれるため、不要なルールを削除する必要があります

10. iptablesへのルール移行

【firewalldからiptablesにルールの移行をする必要がない場合】

以下のルールのみ追加してください。

```
# iptables -I INPUT -s 127.0.0.1 -j ACCEPT
# iptables -I FORWARD -s 127.0.0.1 -j ACCEPT
```

【firewalldからiptablesにルールを全て移行したい場合】

[firewalldのルールを全て移行する場合 (IPv4)]

```
# vi ~/firewalld_iptables_rules
```

ファイルの先頭と末尾に以下の文字列を記載してください。

```
~~~
*filter
<手順5で取得したルールの内容>
COMMIT
~~~
```

```
# iptables-restore < ~/firewalld_iptables_rules
# iptables -I INPUT -s 127.0.0.1 -j ACCEPT
# iptables -I FORWARD -s 127.0.0.1 -j ACCEPT
```

[firewalldのルールを全て移行する場合 (IPv6)]
vi ~/firewalld_ip6tables_rules

ファイルの先頭と末尾に以下の文字列を記載してください。
~~~
*filter
<手順5で取得したルールの内容>
COMMIT
~~~

ip6tables-restore < ~/firewalld_ip6tables_rules

11. iptablesの状態を確認

iptables -nL

[iptablesの状態]
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 127.0.0.1 0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 127.0.0.1 0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
target prot opt source destination

12. iptablesへルールを保存

/usr/libexec/iptables/iptables.init save
/usr/libexec/iptables/ip6tables.init save

13. iptablesを起動

systemctl start iptables
systemctl start ip6tables

14. iptablesの起動を確認

systemctl status iptables
systemctl status ip6tables

15. iptablesを有効化

systemctl enable iptables
systemctl enable ip6tables

16. スクリプトの入れ替えを実施

ファイルのハッシュ値が、以下ハッシュ値と同一であることを確認してください。
sha256sum /var/ossec/active-response/bin/firewall-drop.iptables.sh

〈ハッシュ値〉
07791bdc54a0bcf131f74c6410688e8785031a814b16fba47a210494e2d0da91

cp -pi /var/ossec/active-response/bin/firewall-drop.sh
/var/ossec/active-response/bin/firewall-drop.sh.bak

cp -pi /var/ossec/active-response/bin/firewall-drop.iptables.sh
/var/ossec/active-response/bin/firewall-drop.sh

※firewall-drop.iptables.shが存在しない場合は、以下の方法でスクリプトを取得してください。

(1) 以下リンクの「③ セットアップ」「4. 添付ファイル を、以下のディレクトリに上書き」の添付ファイルをクリック
https://shadan-kun.com/ja/installation_linux#firewalld

※ダウンロードされたスクリプトは、firewall-drop.shの名称となるため、コピーする際はご注意ください

(2) 添付ファイルが正しいか、取得したファイルのハッシュ値が、以下ハッシュ値と同一であることを確認

sha256sum firewall-drop.sh
※ハッシュ値：8595b4dd9f17edcf50d50aae0c4c6e69cd4f7af14306b4274161b5426db9c1ed

17. ossecを起動

/var/ossec/bin/ossec-control start

18. ossecの起動を確認

/var/ossec/bin/ossec-control status

[起動している状態]
ossec-logcollector is running...
ossec-syscheckd is running...
ossec-agentd is running...
ossec-execd is running...

19. 遮断動作確認

疑似攻撃により遮断動作を確認します。

19-1. テスト検知用URLへアクセス

http://<お客様サイトドメイン>/cybersecuritycloud/waftest
https://<お客様サイトドメイン>/cybersecuritycloud/waftest

19-2. 管理画面の検知履歴から検知を確認

ルールID:209999(攻撃種別:その他)
※検知履歴表示:管理画面サイドメニュー[検知/レポート] > [検知履歴]

19-3. 検知後のアクセスが遮断されることを確認
クライアントからの遮断確認方法:ブラウザ等でタイムアウトを確認

※中間機器やアプリケーションの設定等により遮断動作が異なる場合があります
(例:AWSのALBでは403エラーレスポンスを受け、クライアントへ502エラーレスポンスを返します)
※遮断時間は約10分となります

19-4. iptables へ DROP 文が追加されていることを確認 (以下、☆部分)

iptables -nL

Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 127.0.0.1 0.0.0.0/0
DROP all -- 1.1.1.1 0.0.0.0/0 ☆DROP文が127.0.0.1配下に追加されていること
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 127.0.0.1 0.0.0.0/0
DROP all -- 1.1.1.1 0.0.0.0/0 ☆DROP文が127.0.0.1配下に追加されていること
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 ctstate RELATED,ESTABLISHED

19-5. 10 分程確認し、ログに add と delete が記述されていることを確認

tail -f /var/ossec/logs/active-responses.log

以上で、iptablesへの変更は完了です。