# ネットワーク開発演習　９...ファイアーウォール（iptables）

# １.実習の計画

# (1) ポリシーの設計

# (2) シェルスクリプトの基本構造をつくる

(3) IPマスカレード

(4) ユーザチェーンを追加する

# 2. ポリシーの設計

# EXT →　DMZ

# http, ssh, dns

# DMZ →　EXT

# http, dns

# INT →　EXT

# http,dns

# INT →　DMZ

# http,ssh

# DMZ → INT

# http, ssh

# EXT →　INT

# http, dns

3. シェルスクリプトの基本構造をつくる

ルータ１とルータ２に

(1) fw.sh というファイル名で作成してみる

-----

#!/bin/bash

# 既存のルールを削除する

sudo iptables -F

sudo iptables -F -t nat

# 既存のユーザチェーンを削除する

sudo iptables -X

# 設定を確認する

sudo iptables -L

sudo iptables -L -t nat

---

(2) ファイルに実行権限を与える

chmod a+x fw.sh

(3) スーパーユーザで実行

$ sudo ./fw.sh

(4) fw.sh

#!/bin/bash

#変数の定義（EXTは後で否定する)

# インターフェース０

ET0="\_\_\_\_\_\_\_\_\_\_"

# インターフェース１

ET1="\_\_\_\_\_\_\_\_\_\_"

INT="192.168.20.0/24"

DMZ="192.168.10.0/24"

EXT="192.168.0.0/16"

EXT2="192.168.1.0/24"

# ルータ１のグローバル側のIPアドレス

IP="192.168.1.n"

WWW="192.168.10.2:80"

SSH="192.168.10.3:22"

# ルータの設定

# sudo sysctl -w net.ipv4.ip\_forward=1

# ルータ１のルーティングテーブル

sudo route add -net 192.168.20.0 netmask 255.255.255.0 gw 192.168.10.1 $ET1

sudo route add default gw 192.168.1.254 $ET0

# ルータ2のルーティングテーブル

sudo route add default gw 192.168.10.254 $ET0

#初期化

sudo iptables -F -t nat

sudo iptables -F

sudo iptables -X

#IPマスカレード（ルータ１もルータ２も）

sudo iptables -A POSTROUTING -t nat -s $INT -j MASQUERADE –o eth0

#静的NAT（ルータ１だけ）

sudo iptables -A PREROUTING -t nat -p tcp -d $IP --dport 80 -i eth0 -j DNAT --to $WWW

sudo iptables -A PREROUTING -t nat -p tcp -d $IP --dport 22 -i eth0 -j DNAT --to $SSH

４. ユーザチェーンを作成する

**(1) 文法**

sudo **iptabels -N ユーザチェーン名**

(2) **パケットの流れとユーザチェーン**

◆EXT →　DMZ

ユーザチェーン名　ext-dmz

sudo iptables -N ext-dmz

◆DMZ →　EXT

ユーザチェーン名　dmz-ext

sudo iptables -N dmz-ext

◆INT →　EXT

ユーザチェーン名　int-ext

sudo iptables -N int-ext

EXT→　INT

ユーザチェーン名　ext-int

sudo iptables -N ext-int

INT →　DMZ

ユーザチェーン名　int-dmz

sudo iptables -N int-dmz

DMZ →　INT

ユーザチェーン名　dmz-int

sudo iptables -N dmz-int

**５．FORWARDチェーンの定義**

(1) ルータ１ （！は、それ以外という意味になる）

#EXT →　DMZ

sudo iptables -A FORWARD -s $EXT2 -d $DMZ –i eth0 -o eth1 -j ext-dmz

sudo iptables -A FORWARD ! -s $EXT -d $DMZ –i eth0 -o eth1 -j ext-dmz

#DMZ →　EXT

sudo iptables -A FORWARD -s $DMZ -d $EXT2 –i eth1 -o eth0 -j dmz-ext

sudo iptables -A FORWARD -s $DMZ ! -d $EXT –i eth1 -o eth0 -j dmz-ext

#INT →　EXT

sudo iptables -A FORWARD -s $INT ! -d $EXT –i eth1 -o eth0 -j int-ext

sudo iptables -A FORWARD -s $INT -d $EXT2 –i eth1 -o eth0 -j int-ext

#EXT →　INT

#sudo iptables -A FORWARD -s $EXT2 -d $INT –i eth0 -o eth1 -j ext-int

#INT →　DMZ

#sudo iptables -A FORWARD -s $INT -d $DMZ –i eth0 -o eth1 -j int-dmz

#DMZ →　INT

# なし

(2) ルータ２

#EXT →　DMZ

#DMZ →　EXT

#INT →　EXT

sudo iptables -A FORWARD -s $INT -d $EXT2 –i eth1 -o eth0 -j int-ext

sudo iptables -A FORWARD -s $INT -! d $EXT –i eth1 -o eth0 -j int-ext

#EXT →　INT

sudo iptables -A FORWARD -s $EXT2 -d $INT –i eth0 -o eth1 -j ext-int

sudo iptables -A FORWARD ! -s $EXT -d $INT –i eth0 -o eth1 -j ext-int

#INT →　DMZ

sudo iptables -A FORWARD -s $INT -d $DMZ –i eth1 -o eth0 -j int-dmz

#DMZ →　INT

sudo iptables -A FORWARD -s $DMZ -d $INT –i eth0 -o eth1 -j dmz-int

(3) HTTPとHTTPSを通過させる（ルータ１、ルータ２）

# 外部からDMZのwebサーバへのアクセスを許す

sudo iptables –A dmz-ext -p tcp --sport 80 -j ACCEPT

sudo iptables –A ext-dmz -p tcp --dport 80 -j ACCEPT

sudo iptables –A dmz-ext -p tcp --sport 443 -j ACCEPT

sudo iptables –A ext-dmz -p tcp --dport 443 -j ACCEPT

# 内部から外部のwebサーバへのアクセスを許す

sudo iptables –A int-ext -p tcp --dport 80 -j ACCEPT

sudo iptables –A ext-int -p tcp --sport 80 -j ACCEPT

sudo iptables –A int-ext -p tcp --dport 443 -j ACCEPT

sudo iptables –A ext-int -p tcp --sport 443 -j ACCEPT

# DMZから外部のwebサーバへのアクセスを許す

sudo iptables –A dmz-ext -p tcp --dport 80 -j ACCEPT

sudo iptables –A ext-dmz -p tcp --sport 80 -j ACCEPT

sudo iptables –A dmz-ext -p tcp --dport 443 -j ACCEPT

sudo iptables –A ext-dmz -p tcp --sport 443 -j ACCEPT

# DNS

sudo iptables –A dmz-ext -p tcp –dport 53 -j ACCEPT

sudo iptables –A ext-dmz -p tcp –sport 53 -j ACCEPT

sudo iptables –A int-ext –p udp –dport 53 -j ACCEPT

sudo iptables –A ext-int –p udp –sport 53 -j ACCEPT

# SSH

# 外部からDMZのSSHサーバへのアクセスを許す

sudo iptables -A ext-dmz -p tcp --dport 22 -j ACCEPT

sudo iptables -A dmz-ext -p tcp --sport 22 -j ACCEPT

# 内部ネットワークからDMZのSSHサーバへのアクセスを許す

sudo iptables -A int-dmz -p tcp --dport 22 -j ACCEPT

sudo iptables -A dmz-int -p tcp --sport 22 -j ACCEPT

(4)定義の最後に書くルール（これでアクセス不可能になる！）

# その他は通過させない （ルータ１もルータ２も）

sudo iptables -A FORWARD -j DROP

6. 最終確認

(1) 確認用PCから

ルータ１の外部のIPアドレスを指定して、wwwとSSHにアクセスできること

(2) 内部PCから、外部のwebが見れること

(3) 内部PCから、DMZのWWW とSSHにアクセスできること