情報学群実験4C　第6回レポート
ネットワークセキュリティ

学籍番号 1190319
楠田 健太
グループ4

平成29年7月30日

1　目的

LAN をインターネットへ接続することよって，LAN が悪意をもつユーザからの危険に晒される可能性が浮上する．具体的には，情報の漏洩や改ざんが挙げられる．それらを防ぐために，インターネットセキュリティ技術の一つであるパケットフィルタリングファイアーウォールを実現する．

また，外部ネットワークから IP アドレスの構成を秘匿しつつ，通信を制限可能な簡易的なファイアウォールを実装し，セキュリティの向上を実現する．

2　内容

まず始めに，パケットフィルタリングファイアーウォールの実装を行なう．サーバ以外のコンピュータについては外部のネットワークとの通信を全て遮断し，サーバのコンピュータについては，外部のネットワークと DNS，メールの送受信，Web 送受信のみが行えるようにする．

次に，ローカルサーバでポートフォワーディングを設定後，ルータで NAPT を設定，適用することによって，IP アドレスの構成を秘匿しつつ，簡易的なファイアーウォールを実装する．

最後に，動作確認を行なう．

3　要素技術

3.1　アプリケーションゲートウェイ

アプリケーションゲートウェイ (アプリケーションゲートウェイファイアーウォール) は，共通してプロキシファイアーウォールと呼ばれる．OSI 参照モデルのレイヤ 3，4，5，7 の情報をフィルタに通す (図 1 参照)．アプリケーションゲートウェイはアプリケーションレイヤにおいて適用されるため，ファイアーウォールの操作とフィルタリングのほとんどがソフトウェアで行われる．これにより，パケットフィルタリングファイアーウォールやステイトフルファイアーウォール以上の操作を提供することが可能である [1].

アプリケーションゲートウェイはアプリケーション数を制限して適用したり，一つのアプリケーションのみに適用する場合がある．e-mail，Web サービス，DNS，Telnet，FTP，Usenet news，LDAP，finger 等の共通のアプリケーションについても適用される．

アプリケーションゲートウェイは下記に示すように，パケットフィルタリングファイアーウォールやステイトフルファイアーウォール以上に多くの利点を備える．

- 機器ではなく，個人ごとに信頼性を証明する．
- 攻撃者の改ざんや DoS 攻撃などの活動に対して手間を与える．
- アプリケーションデータに対してモニターやフィルタリングが可能である．
- 詳細なログの取得が可能である．

利点を持つと同時に，下記に示すような制限がかかる．

- ソフトウェア上でパケットに処理を行なう．

- 比較的少数のアプリケーションに対して適用させる．
- クライアントに対して特別なソフトウェアを求める場合がある．

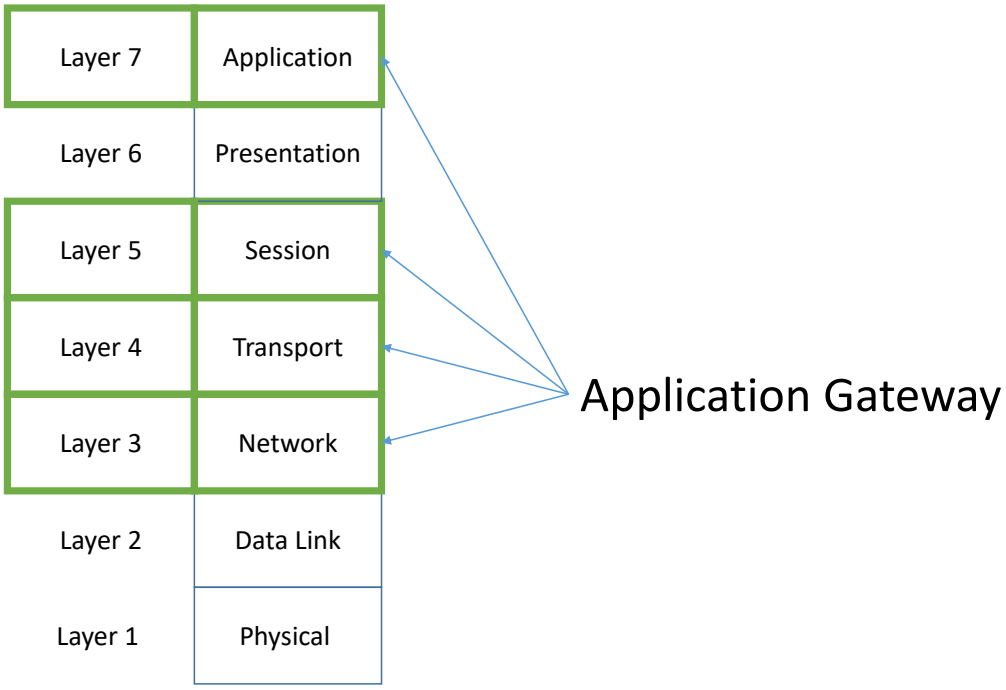

図 1: Application Gateway Firewalls and the OSI Reference Model

3.2 パケットフィルタ

パケットフィルタ (パケットフィルタリングファイアーウォール) は最もシンプルなファイアーウォールの一つである．これは主にパケットのコンテンツをフィルタを通すルーターの機能のことである．パケットフィルタリングファイアーウォールは レイヤ 3 (ネットワーク層) と レイヤ 4 (トランスポート層) で機能する (図 2 参照) ．例えば，Cisco router では基本的なアクセスリストを適用した場合，レイヤ 3 で情報をフィルタに通すことが可能であり，拡張したアクセスリストを適用した場合，レイヤ 3 とレイヤ 4 の両方において情報をフィルタに通すことが可能である [1].

パケットフィルタリングファイアーウォールは下記の種類の情報をフィルターに通すことが可能である．

- 出発点と到着点のレイヤ 3 アドレス
- レイヤ 3 のプロトコル情報

- レイヤ 4 のプロトコル情報
- 通信を送受信するインタフェース

例えば，Cisco router では 特定の ICMP メッセージ (レイヤ 3) や，出発点と到着点の IP アドレス (レイヤ 3) ，また TCP ポート番号 (レイヤ 4) などの情報をフィルタに通すために利用可能である (表 1 参照) 。

パケットフィルタリングファイアーウォールは主に下記の 2 つの利点を持つ.

- とても速い速度でプロセスを実行可能である.
- レイヤ 3 とレイヤ 4 の セグメントヘッダ のほぼすべての分野で簡単に照合を行なうことが可能であり，セキュリティポリシーの実行において多様性を提供可能である.

また，上記の利点があるにも関わらず，下記に示すような欠点を持つ.

- 設定が複雑になりかねない.
- アプリケーションレイヤ (レイヤ 7) への攻撃を防ぐことができない.
- ある種類の TCP/IP プロトコルの感受性が強くなってしまう.
- ログを取る機能に制限がある.

表 1: TCP/IP Packet Filtering information

Layer	Filtered Information
3	IP addresses
3	TCP/IP protocols，such as IP，ICMP，OSPF，TCP，UDP，and others
3	IP precedence (type of service [ToS]) information
4	TCP and UDP port numbers
4	TCP control flags，such as SYN，ACK，FIN，PSH，RST，and others

3.3 NAT (NAPT)

NAPT (Network Address Port Translation) とは，同じ LAN 内の異なるホストについて，インターネットから見たときに同じ IP アドレスでポート番号だけが異なって識別される技術のことである．この技術によって，JPNIC などのプロバイダから割り当てられた 1 つの IP アドレスで，複数の PC がインターネットと通信が可能となる [2].

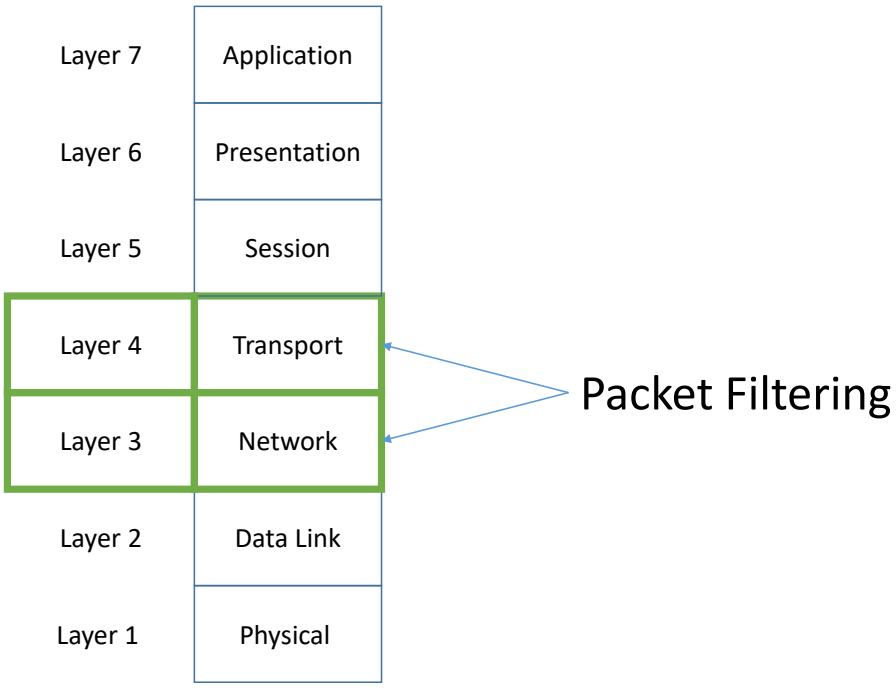

図 2: Packet Filtering Firewalls and the OSI Reference Model

3.4 ポートフォワーディング

ポートフォワーディングとは，インターネットから特定のポート番号宛てにパケットが届いた際に，あらかじめ設定しておいた LAN 側の機器にパケットを転送する機能である．NAPT の場合，LAN 側からインターネット向けにパケットが送信されると，送信元の IP アドレスとポート番号を付け替えて，変換テーブルに記録することでアドレス変換を行なう [3].

SSH コネクションを経由する部分が経由する部分が暗号化されるため，セキュリティを確保した柔軟な通信が可能となる [4].

下記に例を示す (図 3 参照) .

TCP/IP において扱うポートの番号と名前を下記に示す.

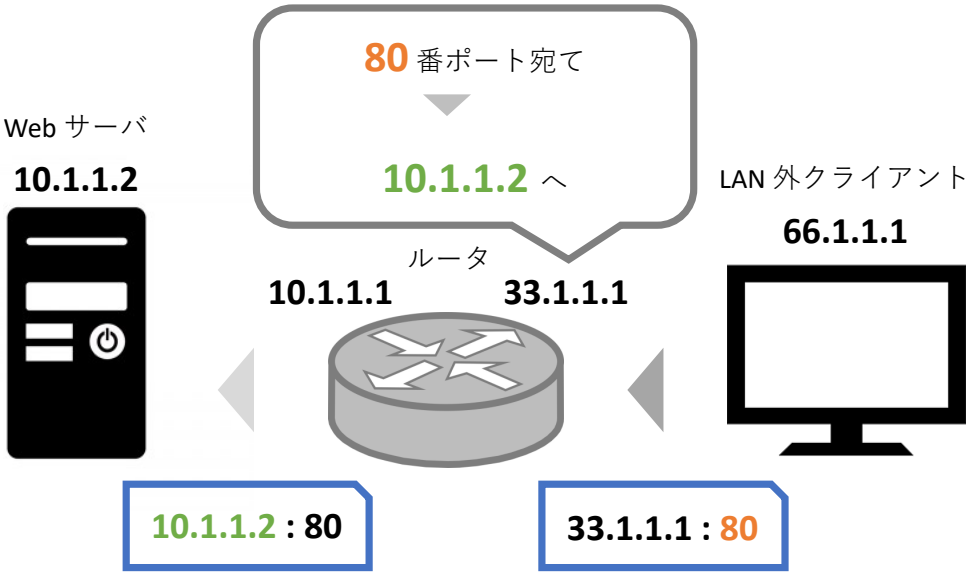

図 3: Port Forwarding

表 2: TCP Port Names (1/2)

Name	Port Number	Description
bgp	179	Border Gateway Protocol
chargen	19	Character generator
cmd	514	Remote commands
daytime	13	Daytime
discard	9	Discard
domain	53	domain Name System zone transfers
echo	7	Echo
exec	512	Remote commands/shell (rsh)
finger	79	Finger
ftp	21	File Transfer Protocol control channel
ftp-data	20	FTP data channel
gopher	70	Gopher
hostname	101	NIC host name server
ident	113	Ident protocol
irc	194	Internet Relay Chat
klogin	543	Kerberos login

表 3: TCP Port Names (2/2)

kshell	544	Kerberos shell
login	513	Remote login (rlogin)
lpd	515	Remote printing
nntp	119	Network News Transport Protocol
pim-auto-rp	496	PIM Auto Rendezvous Point
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
smtp	25	Simple Mail Transport Protocol
sunrpc	111	Sun remote-procedure call
syslog	514	Logging to a syslog server
tacacs	49	TAC access control system server connection
talk	517	Talk
telnet	23	Telnet
time	37	Time
uucp	540	UNIX-to-UNIX copy program
whois	43	Nickname
www	80	World Wide Web (HTTP)
	0 to 65,535	Valid port numbers

4 作業記録

以下に，実際に行った作業の手順を説明する．

4.1 パケットフィルタの設定

クライアント PC (Windows 7) を用いて，自グループの LAN (172.21.14.0) の入り口のルータ (192.168.0.14 - 172.21.14.1) にてパケットフィルタを設定する．また，フィルタの設定内容は下記のように設定する．

表 4: ルータ (192.168.0.14 - 172.168..0.1) におけるパケットフィルタ設定内容

サーバ	許可	DNS メール (MTA) 送受信 ウェブ送受信
サーバ以外の端末	不可	外部とのすべての通信

具体的には，下記の手順で進める．

1. Windows 7 とルータをシリアルケーブルで接続する．

2. Windows 7 の putty を起動する．

3. デスクトップにて，マウスを右クリックし，新規作成＞テキストエディタを選択する．

4. 名前を「access_list」に変更し，ダブルクリックして編集に移る．

5. 以下のように設定内容を入力する．

アクセスリストの設定内容 (1/2)

(100 番のリスト：外側インターフェース向け)
no access-list 100

(インターネットからサーバへの DNS 問い合わせを許可)
access-list 100 permit udp any host 172.21.14.2 eq 53
access-list 100 permit tcp any host 172.21.14.2 eq 53

(インターネットからサーバへの SMTP 接続を許可)
access-list 100 permit tcp any host 172.21.14.2 eq 25

(インターネットからサーバへの HTTP (SSL) 接続を許可)
access-list 100 permit tcp any host 172.21.14.2 eq 80
access-list 100 permit tcp any host 172.21.14.2 eq 443

(インターネットからルータへの着信を許可，さらにブロードキャストも許可)
access-list 100 permit ip any host 192.168.0.14
access-list 100 permit ip any host 192.168.0.255
access-list 100 permit ip any host 255.255.255.255

(インターネットからルータへの OSPF，マルチキャスト着信を許可)
access-list 100 permit ip any host 244.0.0.5
access-list 100 permit ip any host 244.0.0.6

(インターネットからサーバへの DNS 問い合わせ，SMTP 接続，HTTP (s) 接続，に対する応答パケットの許可)
access-list 100 permit udp any eq 53 host 172.21.14.2
access-list 100 permit tcp any eq 53 host 172.21.14.2
access-list 100 permit tcp any eq 25 host 172.21.14.2
access-list 100 permit tcp any eq 80 host 172.21.14.2
access-list 100 permit tcp any eq 443 host 172.21.14.2

アクセスリストの設定内容 (2/2)

```
(101 番のリスト：内側インターフェース向け)
no access-list 101

(サーバからインターネットへの DNS 問い合わせを許可)
access-list 101 permit udp host 172.21.14.2 any eq 53
access-list 101 permit tcp host 172.21.14.2 any eq 53

(サーバからインターネットへの SMTP 接続を許可)
access-list 101 permit tcp host 172.21.14.2 any eq 25

(サーバからインターネットへの HTTP (SSL) 接続を許可)
access-list 101 permit tcp host 172.21.14.2 any eq 80
access-list 101 permit tcp host 172.21.14.2 any eq 443

(サーバからインターネットへの DNS 問い合わせ，SMTP 接続，HTTP (s) 接続，に
対する応答パケットの許可)
access-list 101 permit udp host 172.21.14.2 eq 53 any
access-list 101 permit tcp host 172.21.14.2 eq 53 any
access-list 101 permit tcp host 172.21.14.2 eq 25 any
access-list 101 permit tcp host 172.21.14.2 eq 80 any
access-list 101 permit tcp host 172.21.14.2 eq 443 any
```

6. メニュー画面からコマンドプロンプトを起動する．
7. 上記のアクセスリストを右クリック＞コピーし，コマンドプロンプト上にて右クリック＞貼り付けを実行する．
8. 下記のコマンドを実行し，設定したアクセスリストを適用する．

アクセスリストの適用

```
router4(config)# interface FastEthernet()
router4(config-if)# ip access-group 100 in
router4(config-if)# end
router4# conf term
router4(config)# interface FastEthernet1
router4(config-if)# ip access-group 101 in
router4(config-if)# end
```

9. サーバ PC で下記のコマンドを実行して，設定した内容の動作確認を行なう．

ポート番号を指定した動作確認

```
telnet 172.21.14.2 53 (DNS)
telnet 172.21.14.2 25 (SMTP)
telnet 172.21.14.2 80 (HTTP)
telnet 172.21.14.2 443 (HTTPS)
```

以上でパケットフィルタの設定は完了である．

4.2 ポートフォワーディング

下記のコマンドを実行し，ポートフォワーディングの設定を行なう．

ポートフォワーディング

```
router4(config)# in nat inside source static tcp 172.21.14.2 80 192.168.0.14 80
router4(config)# in nat inside source static tcp 172.21.14.2 443 192.168.0.14 443
router4(config)# in nat inside source static tcp 172.21.14.2 25 192.168.0.14 25
router4(config)# in nat inside source static tcp 172.21.14.2 53 192.168.0.14 53
router4(config)# in nat inside source static udp 172.21.14.2 53 192.168.0.14 53
```

4.3 NAPT (オーバーロードつきダイナミック PAT) の設定

NAPT を設定することによって，外側のネットワークから接続を要求された際にポートを指定し，ホストを識別する．

具体的には，下記のような手順で進める．

1. 下記のコマンドを実行し，設定されてある現在のアクセスリストを解除する．

   アクセスリストの解除

   ```
   router4 ＞ en
   router4 ＞ conf term
   router4 ＞ no access-list 100
   router4 ＞ no access-list 101
   ```

2. 下記のコマンドを実行し，プールの設定を行なう．

   プールの設定

   ```
   router4(config)# ip nat pool group4 192.168.0.14 192.168.0.14 prefix 24
   ```

3. 下記のコマンドを実行し，アクセスリストの設定を行なう．

   アクセスリストの設定

   ```
   router4(config)# in nat inside source list 1 pool group4 overload
   ```

4. 下記のコマンドを実行し，NAT の定義を行なう．

NAT の定義

```
router4(config)# in nat inside source list 1 pool group4 overload
```

5. 下記のコマンドを実行し，インターフェースの設定を行なう．

インターフェースの設定

```
router4(config)# interface FastEthernet 1
router4(config-if)# ip nat inside
router4(config-if)# exit
router4(config)# interface FastEthernet 0
router4(config-if)# ip nat outside
router4(config-if)# exit
```

4.4 動作確認

クライアント の Web ブラウザから 下記の URL を入力し，アクセスすることで，設定した IP アドレスが画面に表示されているかを確認する．

NAPT の動作確認

```
http://192.168.0.2/index.cgi
```

5 考察

アプリケーションゲートウェイファイアーウォールのプロキシサーバを介した通信を行なうことによって IP アドレスの匿名性を保つことが可能である．では，なぜ NAPT とポートフォワーディングを併せて利用することによって匿名性を高める必要があるのだろうか．わたしは，プロキシサーバを介しているとしても，プライベートアドレスをあてずっぽうに宛先に指定することによって，アクセスされる確率が高いためであると考える．したがって，NAPT とポートフォワーディングを併せて活用することによって，レイヤ 4 のポート番号もホストへのアクセスのキーとする必要がある．その結果， IP アドレスの匿名性を高い精度で保ちつつ，プライベート IP アドレスとグローバル IP アドレスを複数対 1 で対応付けて通信を行なうことが可能となる．

参考文献

[1] Richard A. Deal,“ Cisco Router Firewall security ”，Cisco Press，2004.

[2] 日置慎治,“ 初めての情報ネットワーク 1 第 7 章 ADSL，NAT，NAPT ”，NPO CCC-TIES，2013.

[3] 中島章,“ 図解入門よくわかる最新ネットワーク技術の基本と仕組み ”，秀和システム，2016.

[4] 竹下隆史，松山公保，荒井透，苅田幸雄，“マスタリング TCP/IP 入門編 第 5 版”，オーム社，2014.

[5] シスコシステムズ，“シスコ ネットワーキングアカデミー CCNA 受講ガイド，”ソフトバンクパブリッシング株式会社，2005.