# Computer Networks: Assignment 5

17 April 2017

## Solving and submitting your assignment

Requirements about the delivery of this assignment:

- Submit via Blackboard (`http://blackboard.ru.nl`);
- Upload one pdf file for written answers and all supplemental files in a single zip file;
- The file should take the name of your student number, for example student *s0123456* should submit a file named *s0123456.pdf.*
- Write both your name and student number into the document (and only your student number in the filename).

**Deadline:** Wednesday, May 3, 20:00 p.m. sharp!

**Goals:** After completing these exercises successfully you should be able to:

- understand the concept of a firewall
- be able to setup basic filtering rules with *iptables*
- grasp how security notions are implemented in IPSec and SSL
- interpret SSL traffic

**Marks:** You will be graded with marks from 0 to 3 where 0 means not serious, 1 means serious but insufficient, 2 means sufficient and 3 means good. You can have at most 1 assignment graded 0. To get 1 or more, you MUST attempt to solve ALL exercises, even if the provided solution is not correct/complete. In other words, leaving an exercise out automatically turns your grade to 0. In your solution, please explain all answers clearly and concisely.

## 1 Firewalls and iptables

Assume the internal network 200.123.123/24. Communication with the outside is done over a stateless firewall implemented in the gateway router. This firewall is as restrictive as possible but accomplishes the following:

- Allows external users to access the company's website at 200.123.123.2 (it is enough to consider only HTTP);

- Allows internal users to send and receive TLS/SSL encrypted mail using SMTP and IMAP respectively by connecting to the external mail server 1.2.3.4;
- Allows internal users to *ping* external hosts using ICMP packets;
- But otherwise blocks all inbound and outbound traffic.

a) *iptables* is a Linux command used to set up firewalls. Give corresponding *iptables* commands for implementing the stateless firewall. You can abstract away from the actual network interfaces. Useful resources are the *iptables* manual page and this walkthrough.

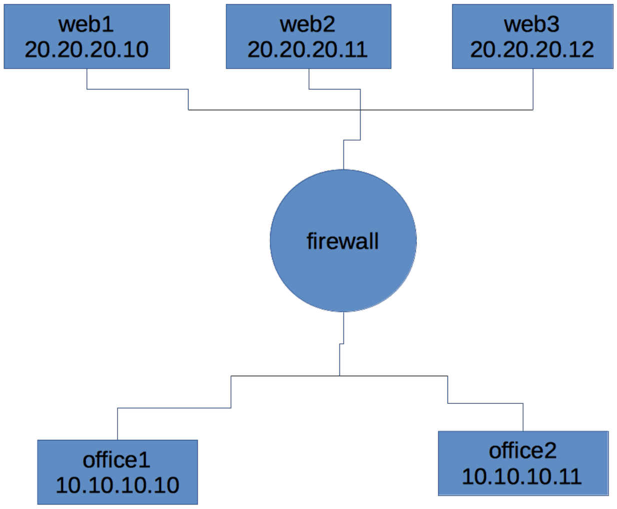
b) Give an access control list (ACL) for the router implementing this firewall *(hint: you can use the* iptables `--list` *option to print out the ACL for the firewall you have just implemented).*

c) Now say the firewall also supports stateful filtering. Strengthen the filter for one of the rules by also using stateful information and give the corresponding *iptables* commands for this filter. Then explain how the filter better enforces the rule, that is what scenarios are handled by this filter, but not by the original filter.

## 2 Firewall practice with netkit

Using the included netkit lab and following the network diagram in Figure 3 implement firewall rules that are as restrictive as possible but which accomplish the following

- 10.10.10.10 and 10.10.10.11 Can send http (and https) traffic to 20.20.20.0/24
- 10.10.10.10 can send only TLS encrypted mail (SMTP and IMAP) traffic to 20.20.20.11
- 10.10.10.10 and 10.10.10.11 can ping and traceroute to all 20.20.20.0/24 machines

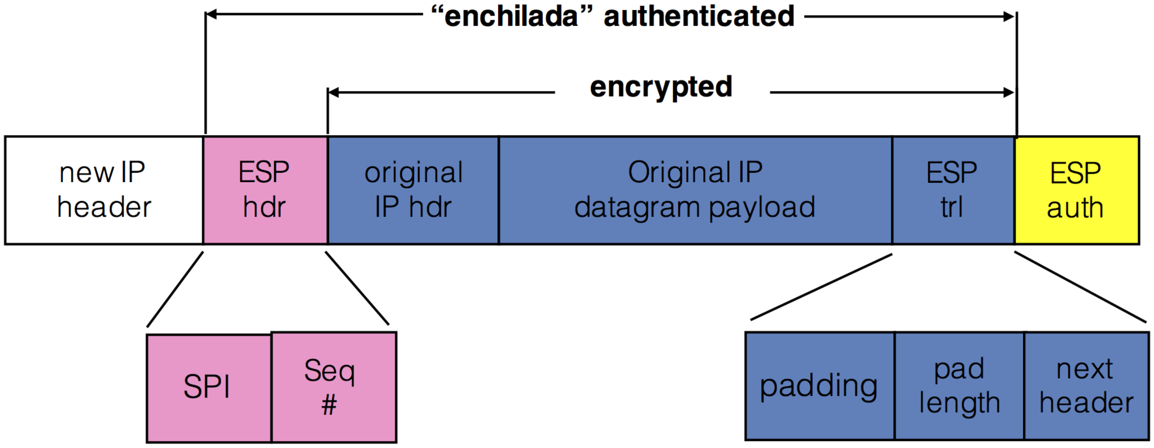


For this exercise you will only need to alter the iptables rules which are set in the firewall startup script. Example rules have been set to block all traffic on the firewall. *iptables* is already set to run on VM boot, but has a blank ruleset. All three 20.20.20.0/24 machines are running a web server which you can test access to from the 10.10.10.0/24 machines with links 20.20.20.X

Please turn in a copy of your firewall rules.

## 3 IPsec

The ESP protocol of the IPSec protocol suite provides integrity and confidentiality. To that end, it uses a specific ESP frame.



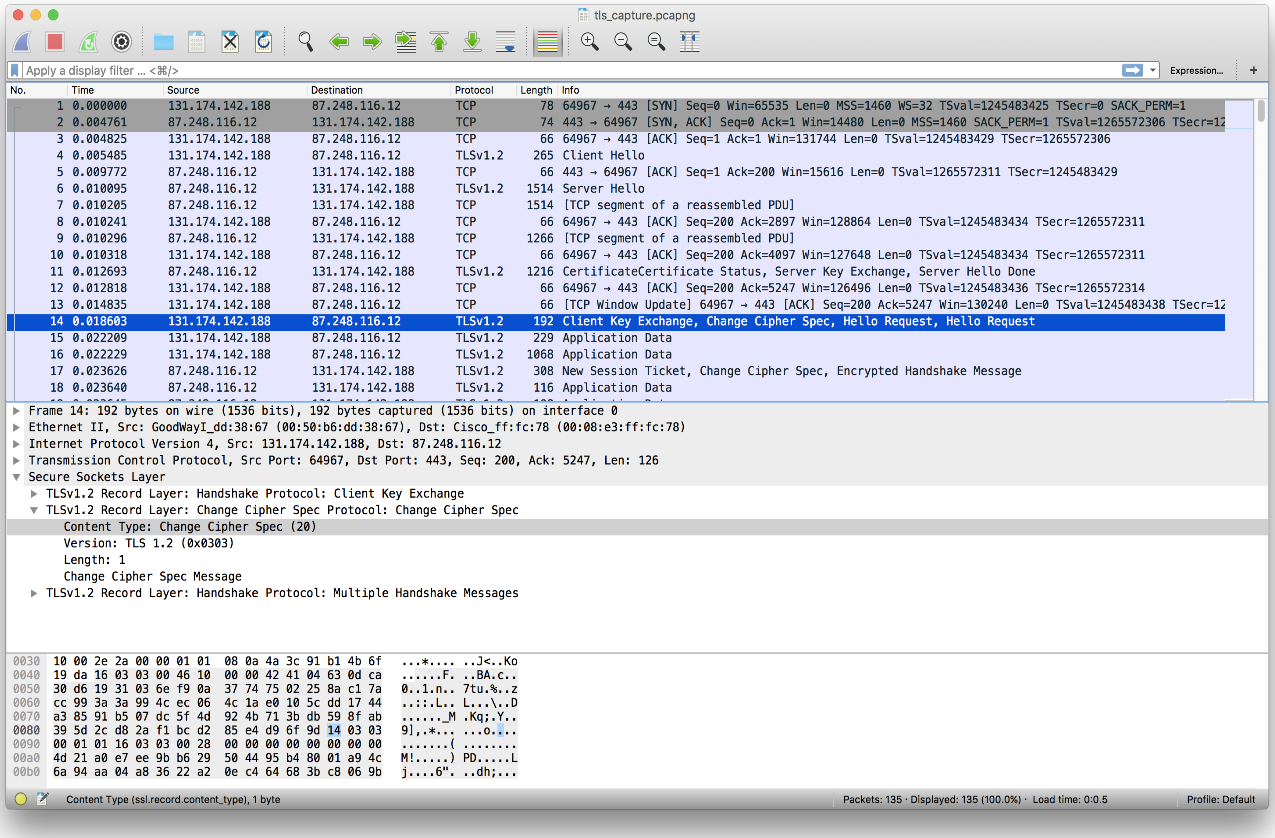
a) Use the above figure to explain each step of constructing an ESP frame.

b) How are the two mentioned security goals are achieved?

c) How does the protocol defend against replay attacks?

d) Say a security association (SA) was established. What IP addresses remain visible to the open network from the packets exchanged between the SA entities? What is the visible IP protocol number on these packets?

# 4 Understanding and Interpreting SSL Wireshark Capture



tls_capture.pcapng

```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  131.174.142.188 87.248.116.12   TCP        78 64967 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1245483425 TSecr=0 SACK_PERM=1
   2 0.004761  87.248.116.12   131.174.142.188 TCP        74 443 → 64967 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=1265572306 TSecr=12
   3 0.004825  131.174.142.188 87.248.116.12   TCP        66 64967 → 443 [ACK] Seq=1 Ack=1 Win=131744 Len=0 TSval=1245483429 TSecr=1265572306
   4 0.005485  131.174.142.188 87.248.116.12   TLSv1.2   265 Client Hello
   5 0.009772  87.248.116.12   131.174.142.188 TCP        66 443 → 64967 [ACK] Seq=1 Ack=200 Win=15616 Len=0 TSval=1265572311 TSecr=1245483429
   6 0.010095  87.248.116.12   131.174.142.188 TLSv1.2  1514 Server Hello
   7 0.010205  87.248.116.12   131.174.142.188 TCP      1514 [TCP segment of a reassembled PDU]
   8 0.010241  131.174.142.188 87.248.116.12   TCP        66 64967 → 443 [ACK] Seq=200 Ack=2897 Win=128864 Len=0 TSval=1245483434 TSecr=1265572311
   9 0.010296  87.248.116.12   131.174.142.188 TCP      1266 [TCP segment of a reassembled PDU]
  10 0.010318  131.174.142.188 87.248.116.12   TCP        66 64967 → 443 [ACK] Seq=200 Ack=4097 Win=127648 Len=0 TSval=1245483434 TSecr=1265572311
  11 0.012693  87.248.116.12   131.174.142.188 TLSv1.2  1216 CertificateCertificate Status, Server Key Exchange, Server Hello Done
  12 0.012818  131.174.142.188 87.248.116.12   TCP        66 64967 → 443 [ACK] Seq=200 Ack=5247 Win=126496 Len=0 TSval=1245483436 TSecr=1265572314
  13 0.014835  131.174.142.188 87.248.116.12   TCP        66 [TCP Window Update] 64967 → 443 [ACK] Seq=200 Ack=5247 Win=130240 Len=0 TSval=1245483438 TSecr=12
  14 0.018603  131.174.142.188 87.248.116.12   TLSv1.2   192 Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
  15 0.022209  131.174.142.188 87.248.116.12   TLSv1.2   229 Application Data
  16 0.022229  131.174.142.188 87.248.116.12   TLSv1.2  1068 Application Data
  17 0.023626  87.248.116.12   131.174.142.188 TLSv1.2   308 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  18 0.023640  87.248.116.12   131.174.142.188 TLSv1.2   116 Application Data
```

```
▶ Frame 14: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits) on interface 0
▶ Ethernet II, Src: GoodWayI_dd:38:67 (00:50:b6:dd:38:67), Dst: Cisco_ff:fc:78 (00:08:e3:ff:fc:78)
▶ Internet Protocol Version 4, Src: 131.174.142.188, Dst: 87.248.116.12
▶ Transmission Control Protocol, Src Port: 64967, Dst Port: 443, Seq: 200, Ack: 5247, Len: 126
▼ Secure Sockets Layer
  ▶ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  ▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
      Content Type: Change Cipher Spec (20)
      Version: TLS 1.2 (0x0303)
      Length: 1
      Change Cipher Spec Message
  ▶ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
```

```
0030  10 00 2e 2a 00 00 01 01  08 0a 4a 3c 91 b1 4b 6f   ...*.... ..J<..Ko
0040  19 da 16 03 03 00 46 10  00 00 42 41 04 63 0d ca   ......F. ..BA.c..
0050  30 d6 19 31 03 6e f9 0a  37 74 75 02 25 8a c1 7a   0..1.n.. 7tu.%..z
0060  cc 99 3a 3a 99 4c ec 06  4c 1a e0 10 5c dd 17 44   ..::.L.. L...\..D
0070  a3 85 91 b5 07 dc 5f 4d  92 4b 71 3b db 59 8f ab   ......_M .Kq;.Y..
0080  39 5d 2c d8 2a f1 bc d2  85 e4 d9 6f 9d 14 03 03   9],.*... ...o....
0090  00 01 01 16 03 03 00 28  00 00 00 00 00 00 00 00   .......( ........
00a0  4d 21 a0 e7 ee 9b b6 29  50 44 95 b4 80 01 a9 4c   M!.....) PD.....L
00b0  6a 94 aa 04 a8 36 22 a2  0e c4 64 68 3b c8 06 9b   j....6". ..dh;...
```

Content Type (ssl.record.content_type), 1 byte

Packets: 135 · Displayed: 135 (100.0%) · Load time: 0:0.5

Profile: Default

Figure 1: SSL Wireshark capture

a) Is Wireshark packet 14 sent by client or server?

b) What is the server's IP address and port number?

c) Assuming no loss and no retransmissions, what will be the sequence number of the next TCP segment sent by the client?

d) How many SSL records does Wireshark packet 14 contain?

e) Does packet 14 contain a Master Secret or an Encrypted Master Secret or neither?

f) The client encrypted handshake message takes into account how many SSL records?

g) The server encrypted handshake message takes into account how many SSL records?

# 5 SSL & MiTM

Suppose Alice and Bob are communicating over an SSL session. Suppose an attacker, Eve, who does not have any of the shared keys, inserts a bogus TCP segment into a packet stream with correct TCP checksum and sequence numbers (and correct IP addresses and port numbers).

a) Will SSL at the receiving side accept the bogus packet and pass the payload to the receiving application? Why or why not?

b) Assume Eve, a woman-in-the-middle, can wreak havoc in an SSL session by interchanging TCP segments. Can Eve do something similar by deleting a TCP segment? What does she need to do to succeed at the deletion attack? What effect will it have?