PAN9 CYBERSECURITY GATEWAY

Lab 5: Analyzing Packet Captures

Document Version: 2020-01-24

Contents

Introduction

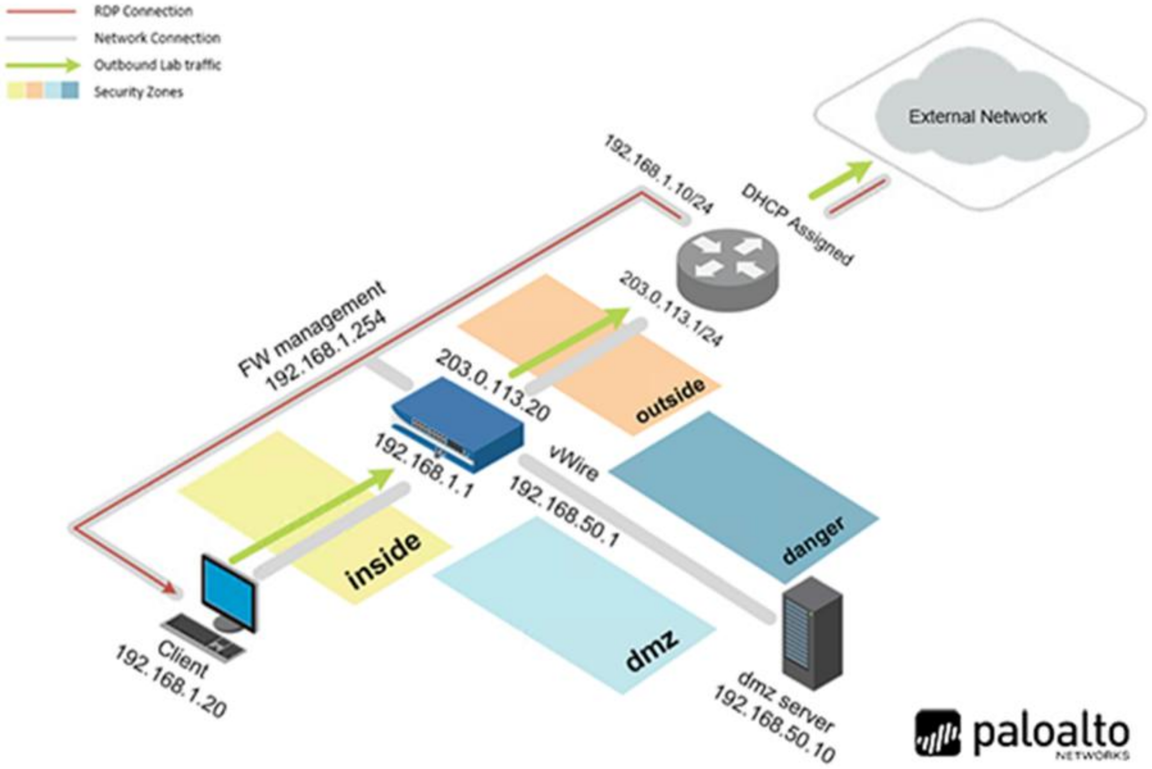
In this lab, you will utilize the Palo Alto Networks Firewall to create a packet capture and save it to the Client. Then, you will use Wireshark to explore capture files and examine the data within the packet.

Objective

In this lab, you will perform the following tasks:

- Create a Packet Capture within the Palo Alto Networks Firewall
- Analyze PCAP Files with Wireshark

Lab Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

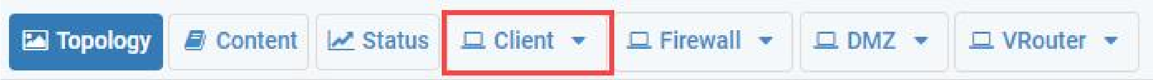
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Client	192.168.1.20	lab-user	Train1ng$
DMZ	192.168.50.10	root	Pal0Alt0
Firewall	192.168.1.254	admin	Train1ng$

5 Lab: Analyzing Packet Captures

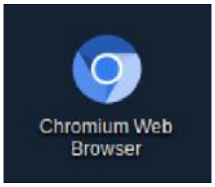
5.0 Load Lab Configuration

In this section, you will load the Firewall configuration file.

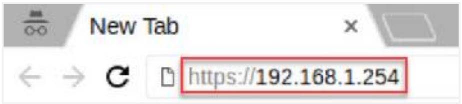
1. Click on the **Client** tab to access the Client PC.



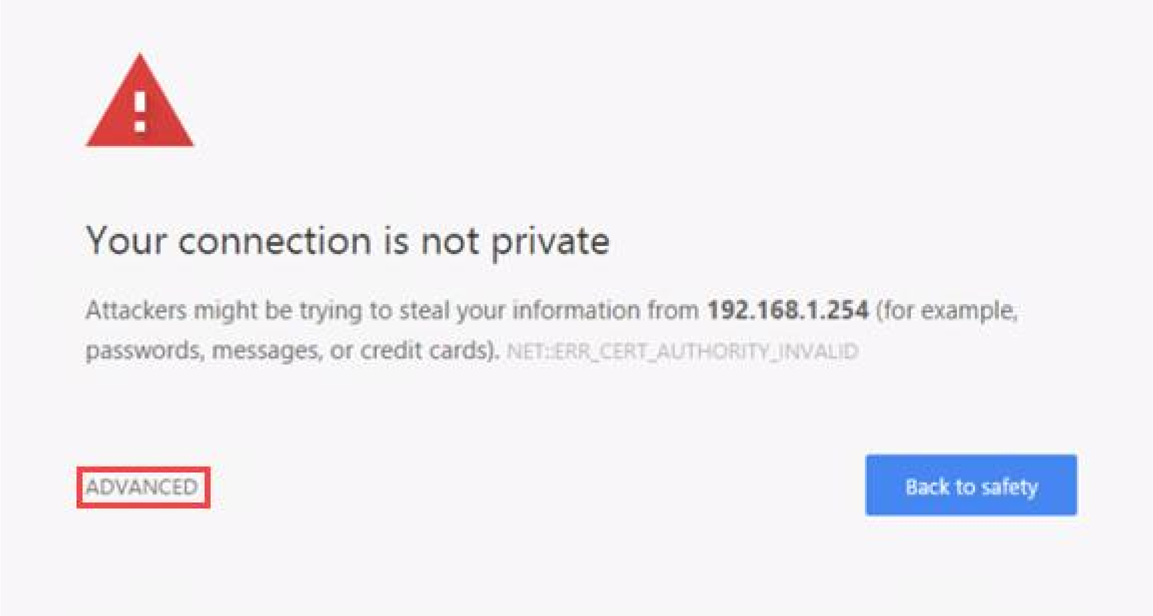
2. Log in to the Client PC with the username `lab-user` and password `Train1ng$`.
3. Double-click the **Google Chrome** icon located on the Desktop.



4. In the *Chromium* address field, type `https://192.168.1.254` and press **Enter**.



5. You will see a "*Your connection is not private"* message. Click on the **ADVANCED** link.

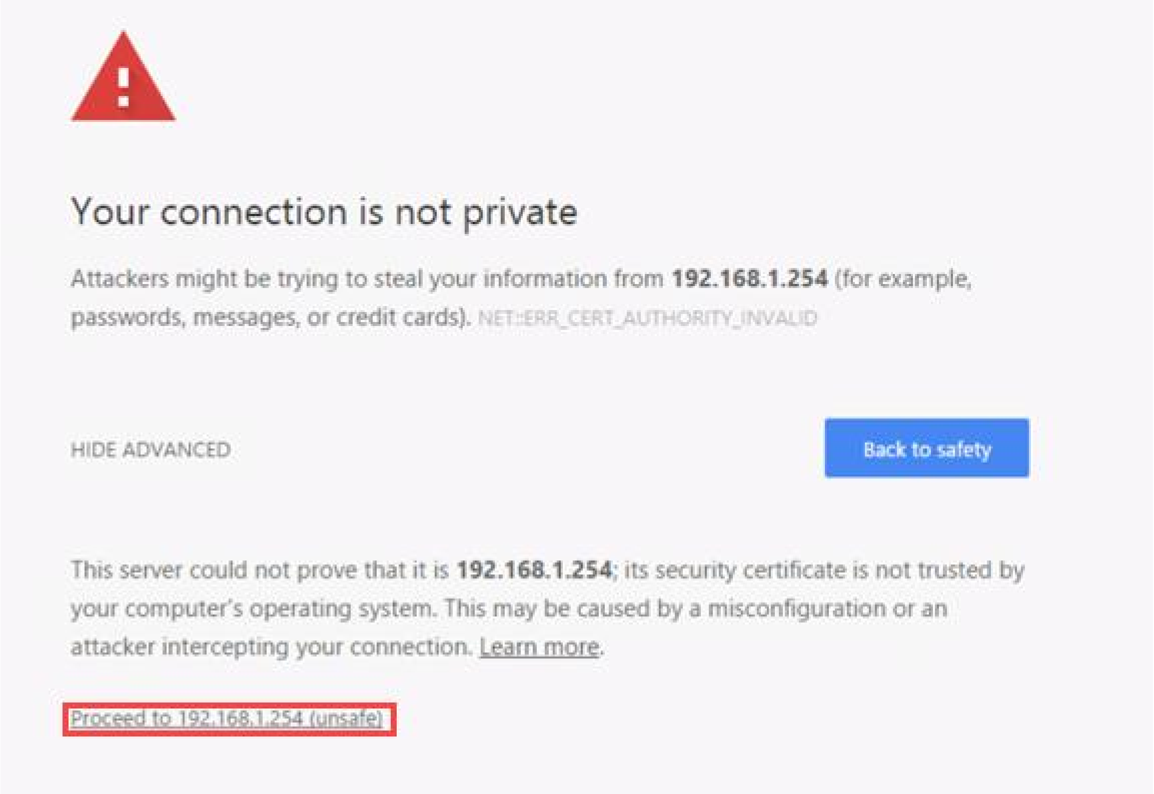


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

If you experience the “Unable to connect” or “502 Bad Gateway” message while attempting to connect to the specified IP above, please wait an additional 1-3 minutes for the Firewall to fully initialize. Refresh the page to continue.

6. Click on **Proceed to 192.168.1.254 (unsafe)**.

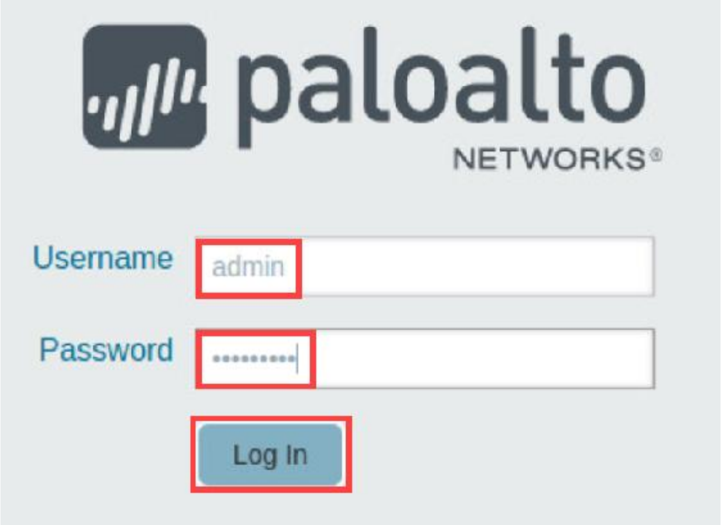


Your connection is not private

Attackers might be trying to steal your information from **192.168.1.254** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

This server could not prove that it is **192.168.1.254**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

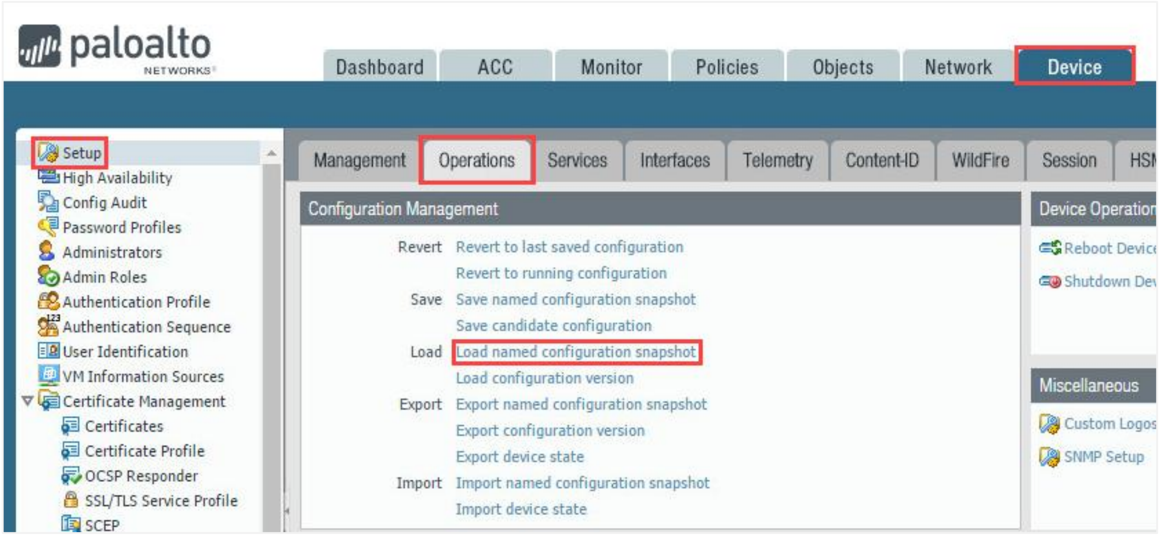
7. Log in to the Firewall web interface as username **admin**, password `Train1ng$`.



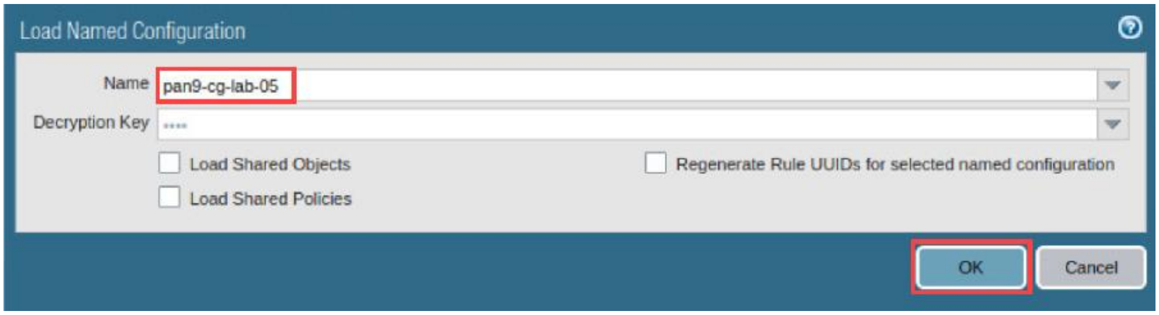
Username: admin

Password: ••••••••••

8. In the web interface, navigate to **Device > Setup > Operations** and click on **Load named configuration snapshot** underneath the *Configuration Management* section.



9. In the *Load Named Configuration* window, select **pan9-cg-lab-05** from the *Name* dropdown box and click **OK**.


Load Named Configuration

Name pan9-cg-lab-05

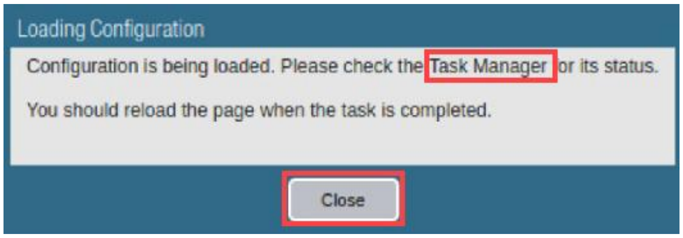
Decryption Key ••••

□ Load Shared Objects

□ Regenerate Rule UUIDs for selected named configuration

□ Load Shared Policies

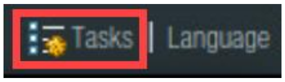
10. In the Loading Configuration window, a message will show *Configuration is being loaded. Please check the Task Manager for its status. You should reload the page when the task is completed.* Click **Close** to continue.


Loading Configuration

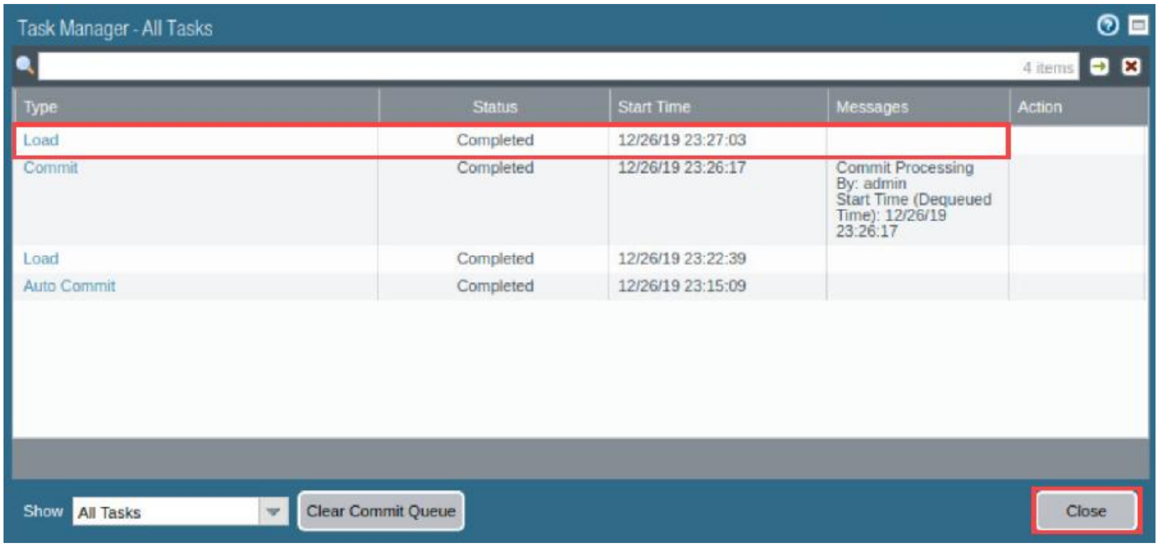
Configuration is being loaded. Please check the Task Manager for its status.

You should reload the page when the task is completed.

11. Click the **Tasks** icon located at the bottom-right of the web interface.

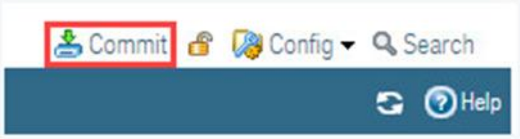


12. In the *Task Manager – All Tasks* window, verify the *Load* type has successfully completed. Click **Close**.

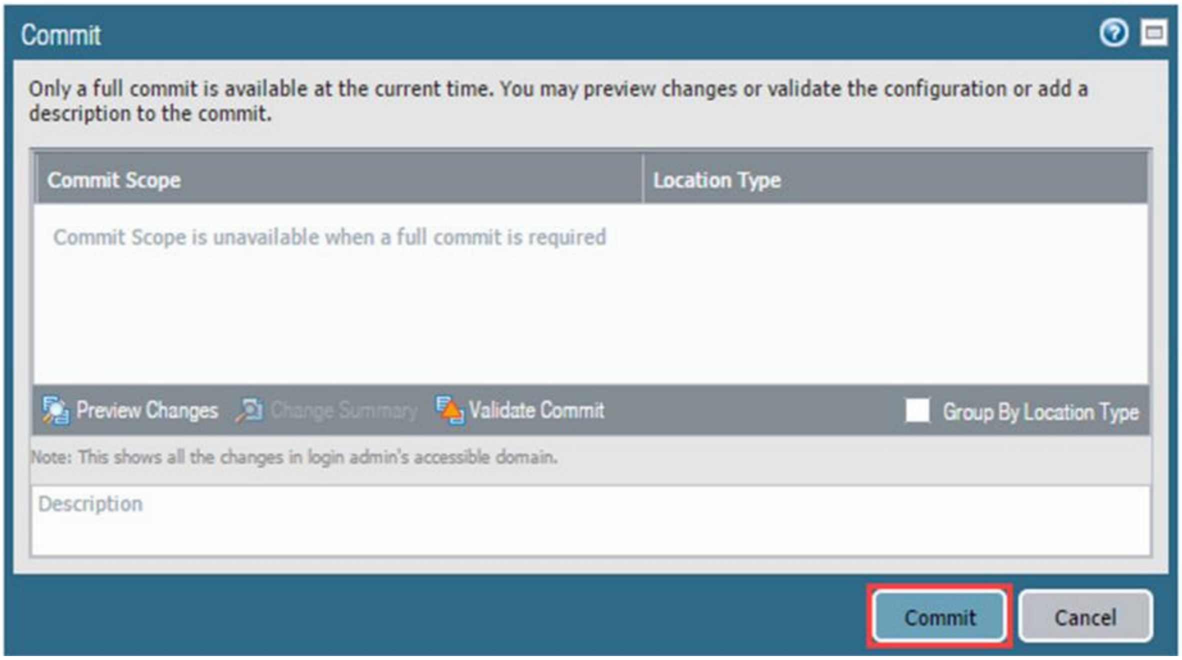


Type	Status	Start Time	Messages	Action
Load	Completed	12/26/19 23:27:03		
Commit	Completed	12/26/19 23:26:17	Commit Processing By: admin Start Time (Dequeued Time): 12/26/19 23:26:17	
Load	Completed	12/26/19 23:22:39		
Auto Commit	Completed	12/26/19 23:15:09		

13. Click the **Commit** link located at the top-right of the web interface.



14. In the *Commit* window, click **Commit** to proceed with committing the changes.

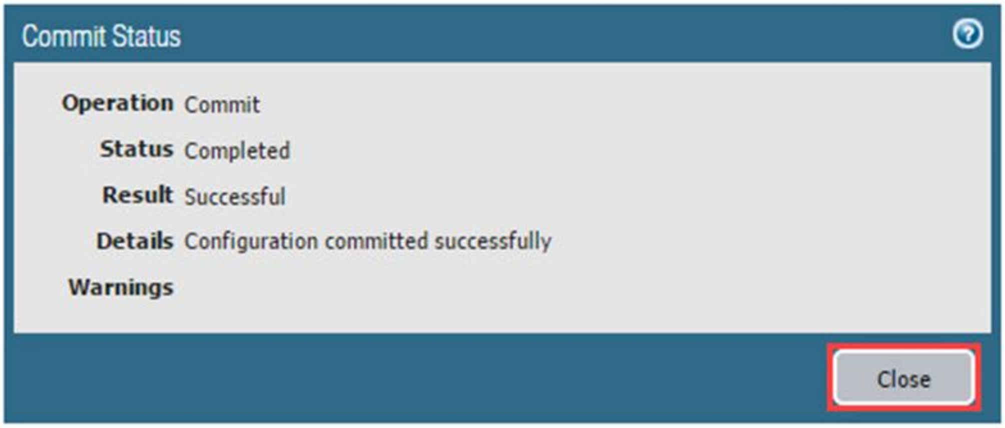


Only a full commit is available at the current time. You may preview changes or validate the configuration or add a description to the commit.

Commit Scope	Location Type
Commit Scope is unavailable when a full commit is required	

Note: This shows all the changes in login admin's accessible domain.

15. When the commit operation successfully completes, click **Close** to continue.



Commit Status

Operation Commit

Status Completed

Result Successful

Details Configuration committed successfully

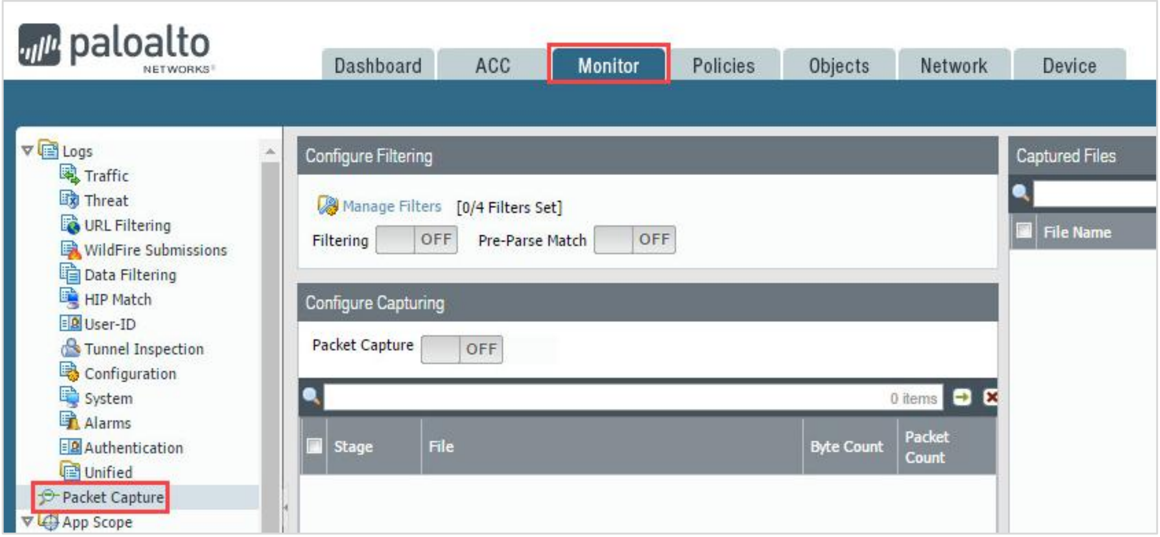
Warnings

The commit process takes changes made to the Firewall and copies them to the running configuration, which will activate all configuration changes since the last commit.

5.1 Create a Packet Capture within the Palo Alto Networks Firewall

In this section, you will create a packet capture on the Firewall and download it to the Client for inspection. This will capture all traffic going through the Firewall.

1. Navigate to **Monitor** > **Packet Capture.**



Configure Filtering

Manage Filters [0/4 Filters Set]

Filtering OFF Pre-Parse Match OFF

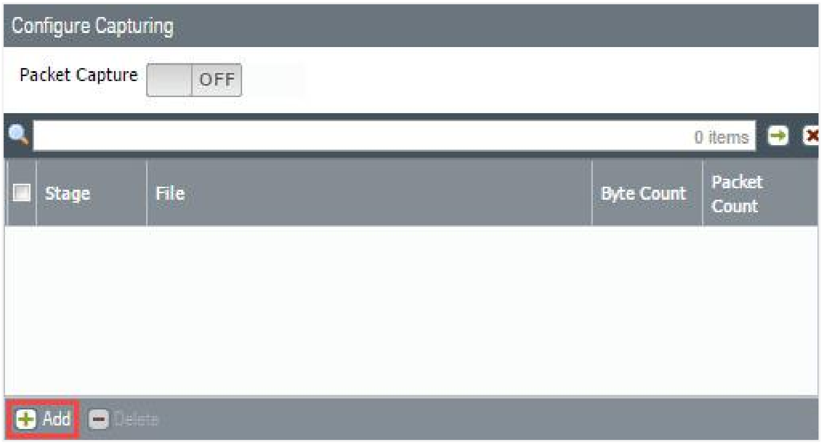
Configure Capturing

Packet Capture OFF

0 items

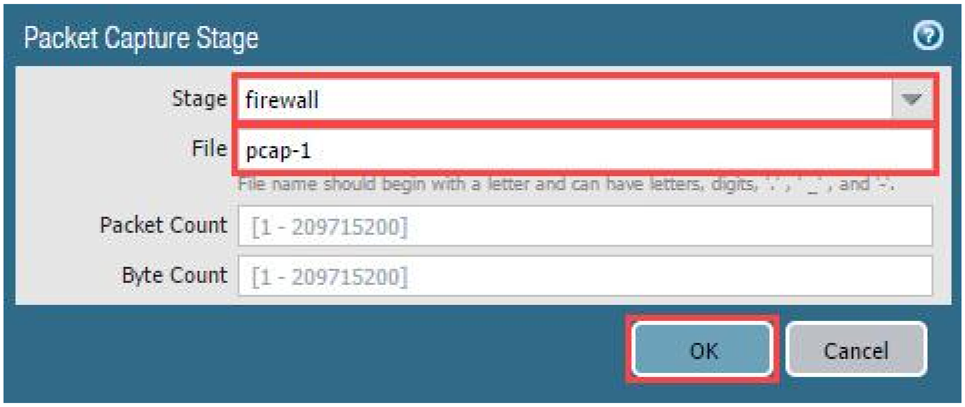
Stage	File	Byte Count	Packet Count

2. In the *Configure Capturing* section, click **Add** to create a Packet Capture Stage.



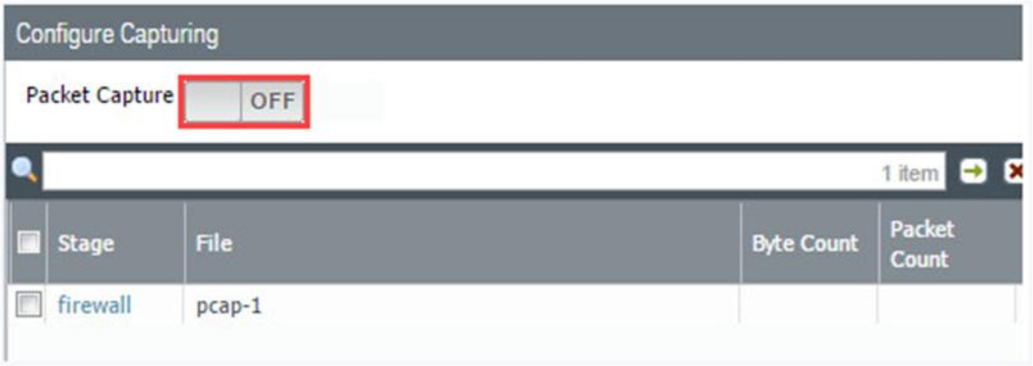
☐	Stage	File	Byte Count	Packet Count

3. In the *Packet Capture Stage* window, select **firewall** from the Stage dropdown. Then, in the File field, type `pcap-1`**.** Finally, click **OK**.



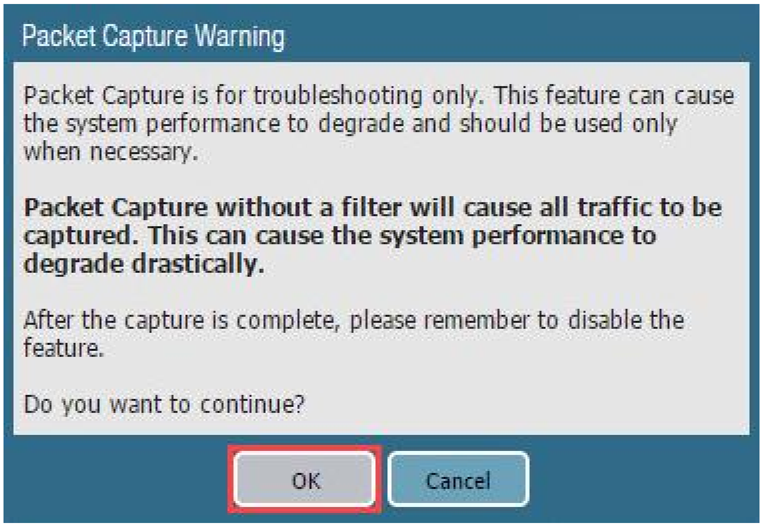
Stage: firewall
File: pcap-1
File name should begin with a letter and can have letters, digits, '.', '_', and '-'.
Packet Count: [1 - 209715200]
Byte Count: [1 - 209715200]

4. In the *Configure Capturing* section, click **OFF** to turn Packet Capture on.



☐	Stage	File	Byte Count	Packet Count
☐	firewall	pcap-1		

5. On the *Packet Capture Warning* window, click **OK** to continue.



Packet Capture Warning

Packet Capture is for troubleshooting only. This feature can cause the system performance to degrade and should be used only when necessary.

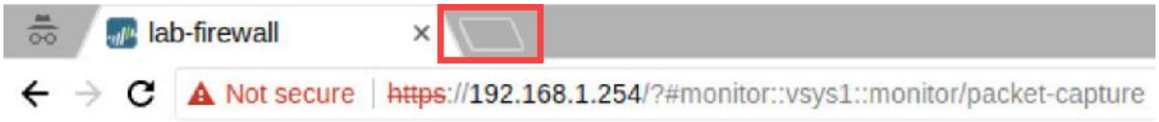
Packet Capture without a filter will cause all traffic to be captured. This can cause the system performance to degrade drastically.

After the capture is complete, please remember to disable the feature.

Do you want to continue?

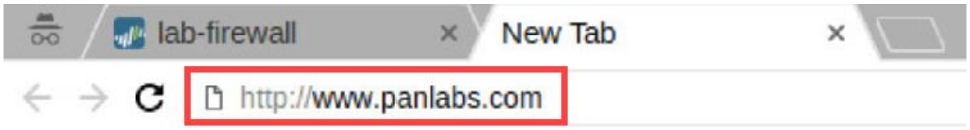
As noted in the *Packet Capture Warning* window, you would want to exercise caution using this feature in a live environment as it may impact the performance of the firewall.

6. With Packet Capturing turned on, click on the **New tab** button.

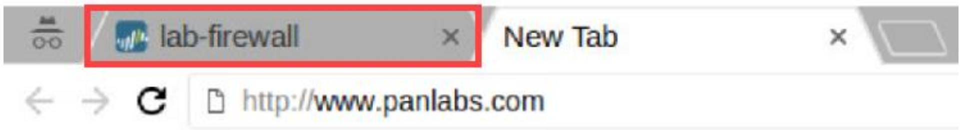


lab-firewall
Not secure
~~https~~://192.168.1.254/?#monitor::vsys1::monitor/packet-capture

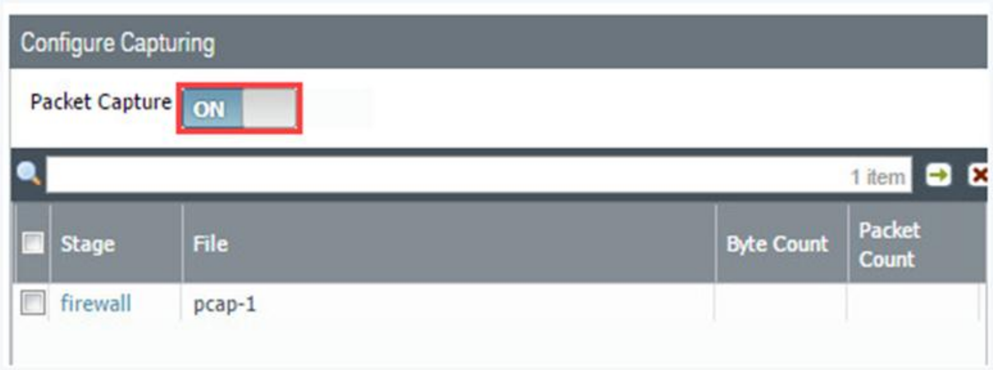
7. In the *address bar*, type `http://www.panlabs.com` and press **Enter**.



8. Click on the **lab-firewall** tab in the upper-left to switch back to the *Firewall administrator* page.



9. In the *Configure Capturing* section, click **ON** to turn Packet Capture off.



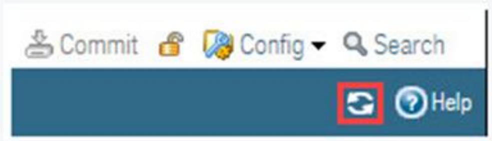
Configure Capturing

Packet Capture: ON

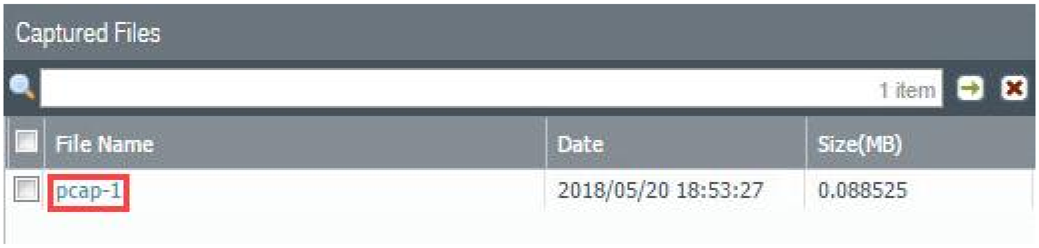
1 item

□	Stage	File	Byte Count	Packet Count
□	firewall	pcap-1		

10. Click the **Refresh** icon in the upper-right of the *Firewall administrator* page to refresh the *Captured Files* section.



11. In the *Captured Files* section, download the packet capture by clicking the **pcap-1** filename in the *File Name* column.

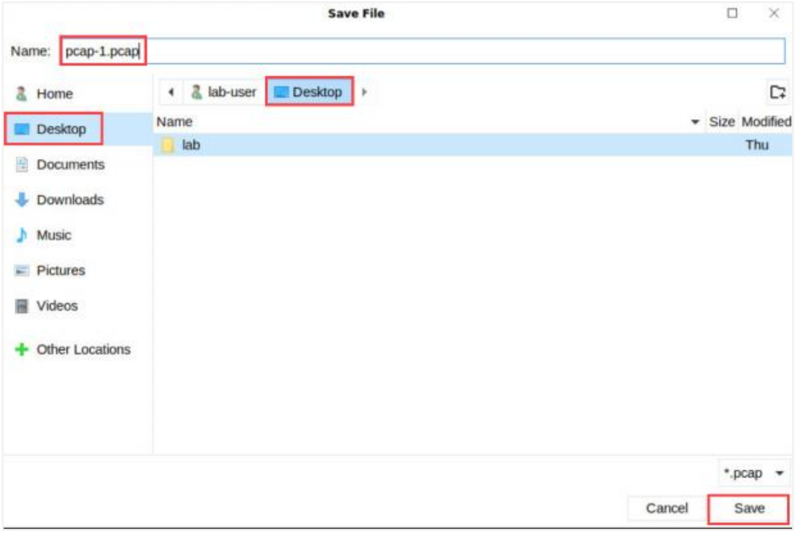


Captured Files

1 item

□	File Name	Date	Size(MB)
□	pcap-1	2018/05/20 18:53:27	0.088525

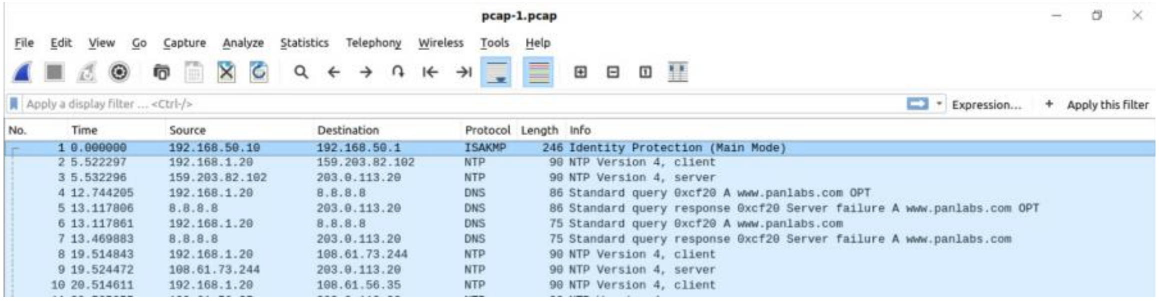
12. When the *Save File* window opens, save the **pcap-1.pcap** file to the client Desktop.



Save File

Name: pcap-1.pcap

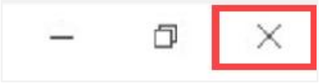
13. On the client desktop, double-click on the **pcap-1.pcap,** and it will open in Wireshark.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.50.10	192.168.50.1	ISAKMP	246	Identity Protection (Main Mode)
2	5.522297	192.168.1.20	159.203.82.102	NTP	90	NTP Version 4, client
3	5.532296	159.203.82.102	203.0.113.20	NTP	90	NTP Version 4, server
4	12.744205	192.168.1.20	8.8.8.8	DNS	86	Standard query 0xcf20 A www.panlabs.com OPT
5	13.117806	8.8.8.8	203.0.113.20	DNS	86	Standard query response 0xcf20 Server failure A www.panlabs.com OPT
6	13.117861	192.168.1.20	8.8.8.8	DNS	75	Standard query 0xcf20 A www.panlabs.com
7	13.469883	8.8.8.8	203.0.113.20	DNS	75	Standard query response 0xcf20 Server failure A www.panlabs.com
8	19.514843	192.168.1.20	108.61.73.244	NTP	90	NTP Version 4, client
9	19.524472	108.61.73.244	203.0.113.20	NTP	90	NTP Version 4, server
10	20.514611	192.168.1.20	108.61.56.35	NTP	90	NTP Version 4, client

14. You may explore the packet capture. In the next section you will analyze a capture in detail. You may close Wireshark by clicking the **X** in the upper-right.

15. Close *Chromium* in the upper-right.

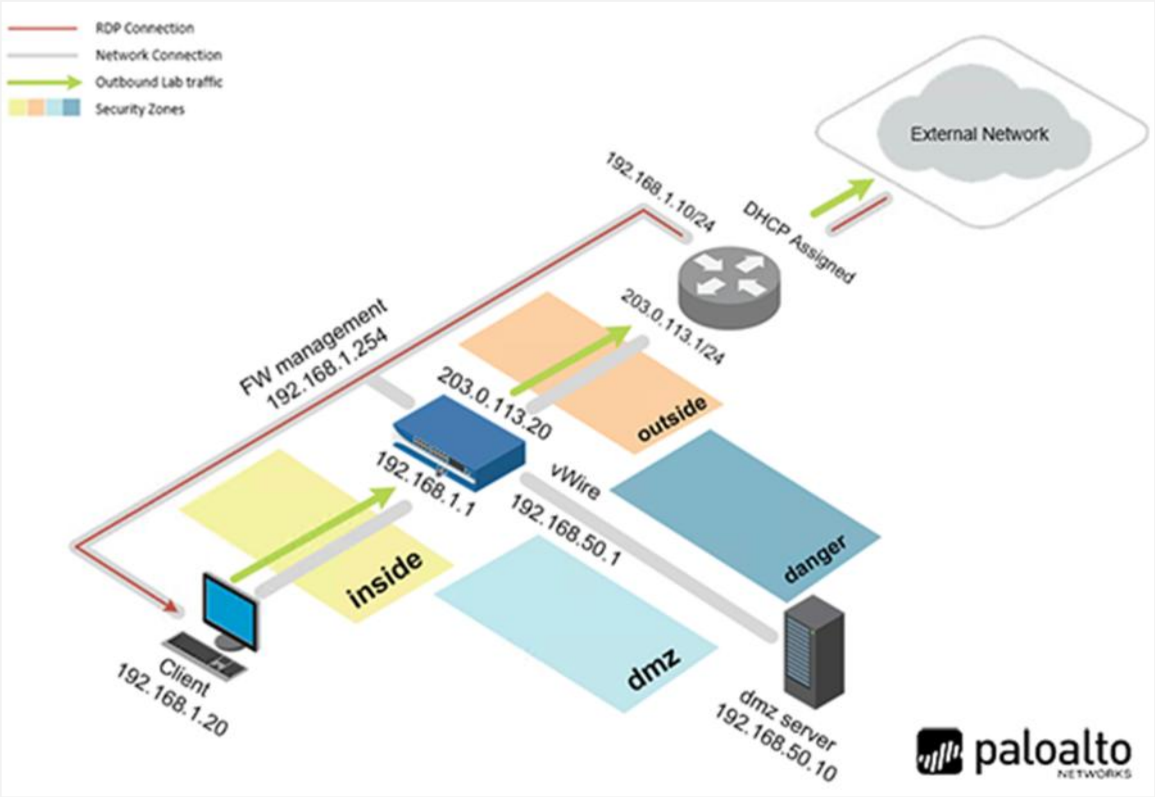


5.2 Analyze PCAP Files with Wireshark

In this section, you will analyze the traffic capture on the Firewall. Due to the amount of traffic captured, you will use filters to locate packets more easily.

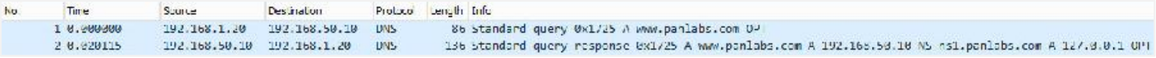
> Due to the nature of the lab environment, you will analyze packet captures from a previously saved session.

1. Before you analyze packets, please review the lab topology. Note the Client and DMZ server.



2. On the Desktop, double-click on **capture.pcap** to open a previous capture in Wireshark.

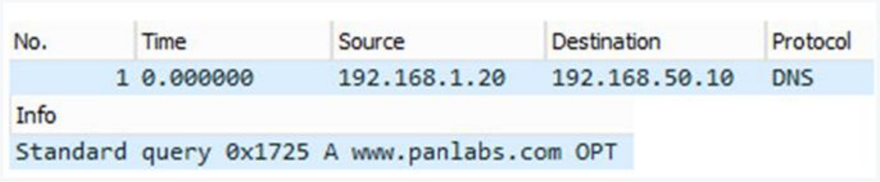
3. The first protocol you will analyze is DNS. Review packets **1** and **2**.



```
No.     Time          Source          Destination     Protocol  Length  Info
      1 0.000000      192.168.1.20    192.168.50.10   DNS           86  Standard query 0x1725 A www.panlabs.com OPT
      2 0.020115      192.168.50.10   192.168.1.20    DNS          136  Standard query response 0x1725 A www.panlabs.com A 192.168.50.10 NS ns1.panlabs.com A 127.0.0.1 OPT
```

In the previous section, you used *Google Chrome* to navigate to **http://www.panlabs.com**. The first step the Client does is to attempt to resolve **www.panlabs.com** to an IP address.

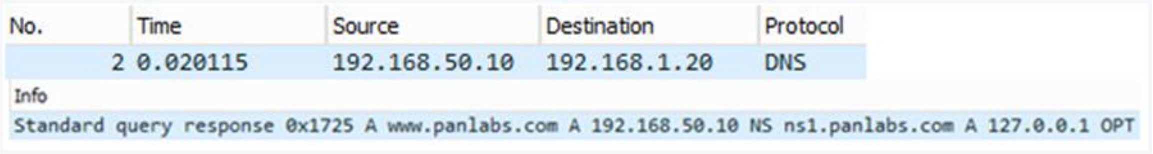
4. Observe packet **1**.



```
No.     Time          Source          Destination     Protocol
      1 0.000000      192.168.1.20    192.168.50.10   DNS
Info
Standard query 0x1725 A www.panlabs.com OPT
```

In packet 1, the Source is the Client (**192.168.1.20**), while the Destination is **192.168.50.10**. The Client is configured to use **127.0.0.1** as its DNS server. In this lab environment, the Client is running its own DNS server with the ability to forward requests to **192.168.50.10**. This is the DMZ server, which is also running a DNS server. The Info column shows it is a **Standard query** asking for the **A** record for **www.panlabs.com**.

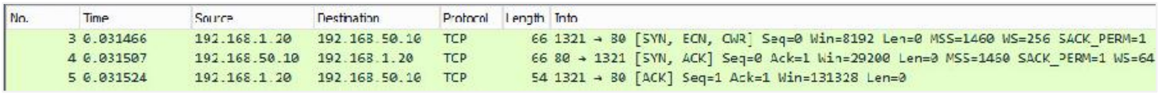
5. Observe packet **2**.



```
No.          Time          Source          Destination     Protocol
           2 0.020115      192.168.50.10   192.168.1.20    DNS
Info
Standard query response 0x1725 A www.panlabs.com A 192.168.50.10 NS ns1.panlabs.com A 127.0.0.1 OPT
```

In packet 2, the Source is the DMZ Server (**192.168.50.10**), while the Destination is **192.168.1.20**. If you look at the Info column, you will see that is a **Standard query response** indicating the **A** record for **www.panlabs.com** has an IP address of **192.168.50.10**. That is the DMZ server, which is also running a Web server hosting **www.panlabs.com**. Now that the Client knows the IP address of the original request, it can begin the request for a 3-way TCP handshake.

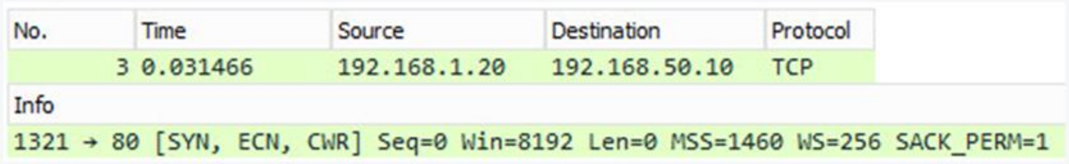
6. Review packets **3, 4,** and **5**.



```
No.      Time        Source          Destination     Protocol  Length  Info
       3 0.031466    192.168.1.20    192.168.50.10   TCP           66  1321 → 80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
       4 0.031507    192.168.50.10   192.168.1.20    TCP           66  80 → 1321 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64
       5 0.031524    192.168.1.20    192.168.50.10   TCP           54  1321 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
```

Packets 3, 4, and 5 are an example of a TCP 3-way handshake.

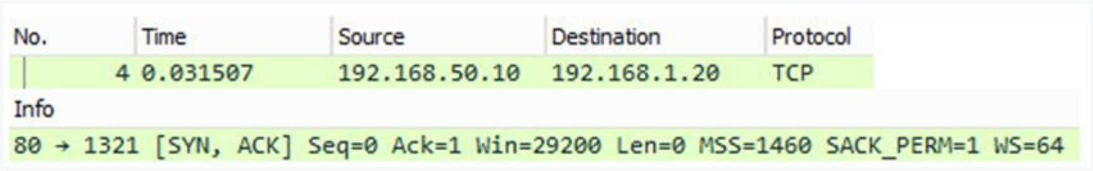
7. Observe packet **3**.



```
No.          Time          Source          Destination     Protocol
           3 0.031466      192.168.1.20    192.168.50.10   TCP
Info
1321 → 80 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

In the first part of the 3-way handshake, the Source (the Client, **192.168.1.20**) sends a TCP packet with the flags SYN, ECN, and CWR set in the header, to the Destination (the DMZ server, **192.168.50.10**). This establishes a SYN (**SYN**chronize) packet along with window size information.

8. Observe packet **4**.

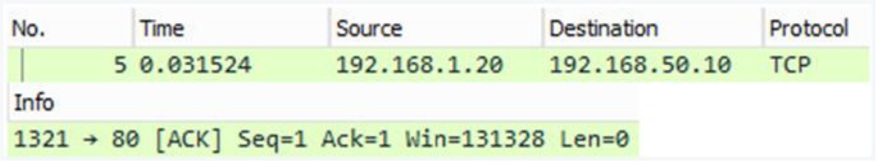


No.	Time	Source	Destination	Protocol
4	0.031507	192.168.50.10	192.168.1.20	TCP

Info
80 → 1321 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=64

In the second part of the 3-way handshake, the Source (the DMZ server, **192.168.50.10**) sends a TCP packet with the flags SYN and ACK set in the header, to the Destination (the Client, **192.168.1.20**). This establishes a SYN-ACK (**SYN**chronize-**ACK**nowledgement) packet. The DMZ server acknowledges the Client and sends back its own synchronization packet.

9. Observe packet **5**.

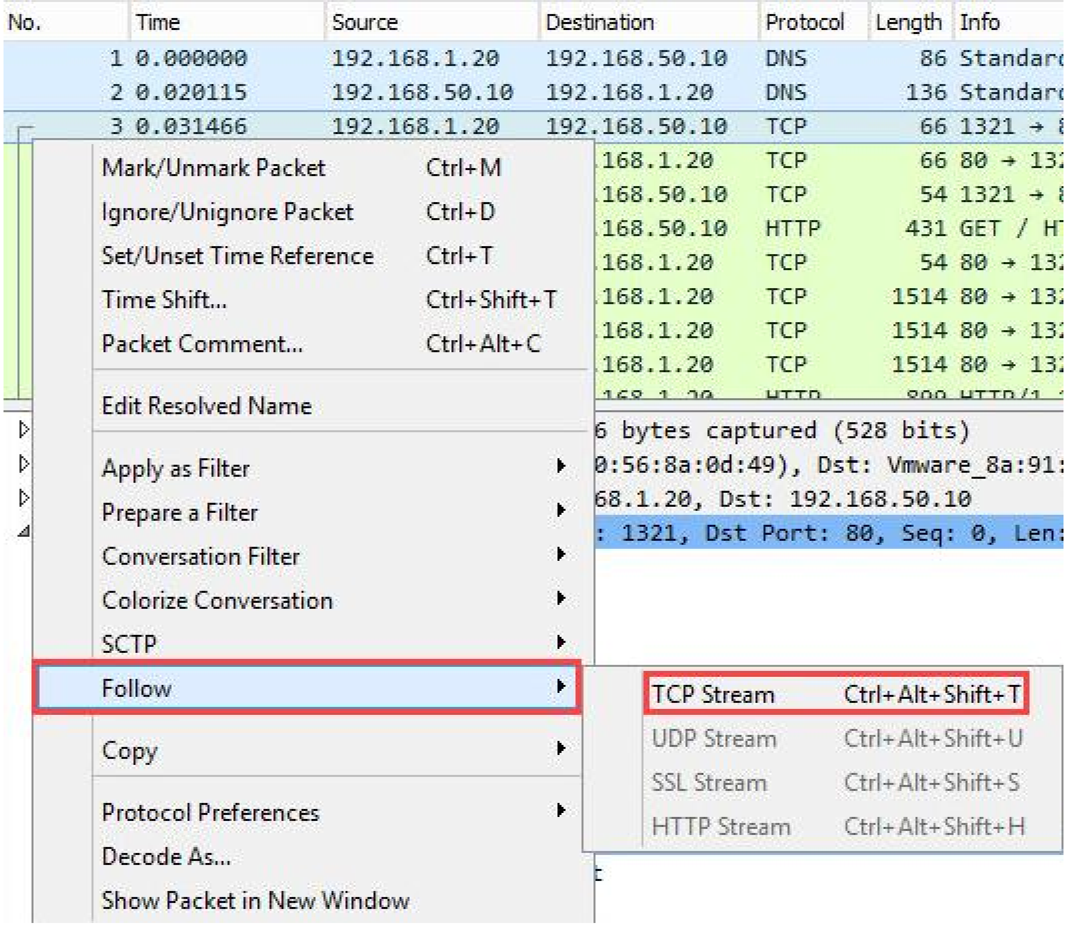


No.	Time	Source	Destination	Protocol
5	0.031524	192.168.1.20	192.168.50.10	TCP

Info
1321 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0

In the third part of the 3-way handshake, the Source (the Client, **192.168.1.20**) sends a TCP packet with the flag ACK set in the header, to the Destination (the DMZ server, **192.168.50.10**). This establishes an ACK (**ACK**nowledgement) packet. The Client acknowledges the DMZ server. The Client and the DMZ server may begin communicating over TCP.

10. Packets 3 – 45 represent a TCP Stream. When put together, this represents the website, http://www.panlabs.com, that you visited. To see this, right-click on packet **3** and select **Follow > TCP Stream**.



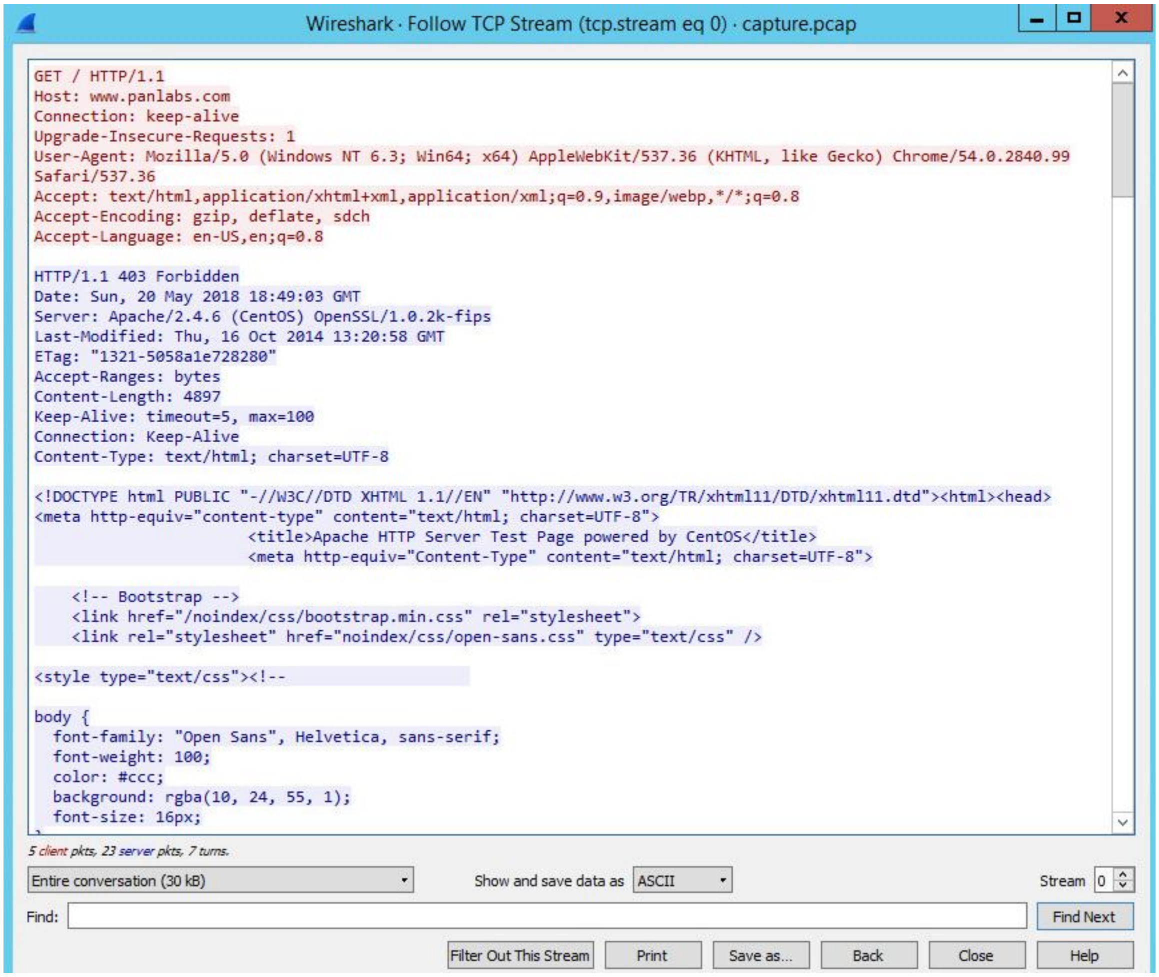
```
No.   Time       Source          Destination     Protocol  Length Info
    1 0.000000   192.168.1.20    192.168.50.10   DNS           86 Standar
    2 0.020115   192.168.50.10   192.168.1.20    DNS          136 Standar
    3 0.031466   192.168.1.20    192.168.50.10   TCP           66 1321 → 8
                                 .168.1.20       TCP           66 80 → 13
                                 .168.50.10      TCP           54 1321 → 8
                                 .168.50.10      HTTP         431 GET / HT
                                 .168.1.20       TCP           54 80 → 13
                                 .168.1.20       TCP         1514 80 → 13
                                 .168.1.20       TCP         1514 80 → 13
                                 .168.1.20       TCP         1514 80 → 13

6 bytes captured (528 bits)
0:56:8a:0d:49), Dst: Vmware_8a:91:
68.1.20, Dst: 192.168.50.10
: 1321, Dst Port: 80, Seq: 0, Len:
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
SSL Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H

Wireshark will assemble the packets associated with this TCP stream.

11. Observe the TCP Stream. Scroll through the data.


Wireshark · Follow TCP Stream (tcp.stream eq 0) · capture.pcap
Filter Out This Stream
Print
Save as...
Back
Close
Help
Find Next

```
GET / HTTP/1.1
Host: www.panlabs.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8

HTTP/1.1 403 Forbidden
Date: Sun, 20 May 2018 18:49:03 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
ETag: "1321-5058a1e728280"
Accept-Ranges: bytes
Content-Length: 4897
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"><html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
                       <title>Apache HTTP Server Test Page powered by CentOS</title>
                       <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    <!-- Bootstrap -->
    <link href="/noindex/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" />

<style type="text/css"><!--

body {
  font-family: "Open Sans", Helvetica, sans-serif;
  font-weight: 100;
  color: #ccc;
  background: rgba(10, 24, 55, 1);
  font-size: 16px;
```

5 client pkts, 23 server pkts, 7 turns.

Entire conversation (30 kB) ▾   Show and save data as ASCII ▾   Stream 0

Find:

Notice the assembled packets represent the HTML website you visited.

12. The lab is now complete; you may end the reservation.