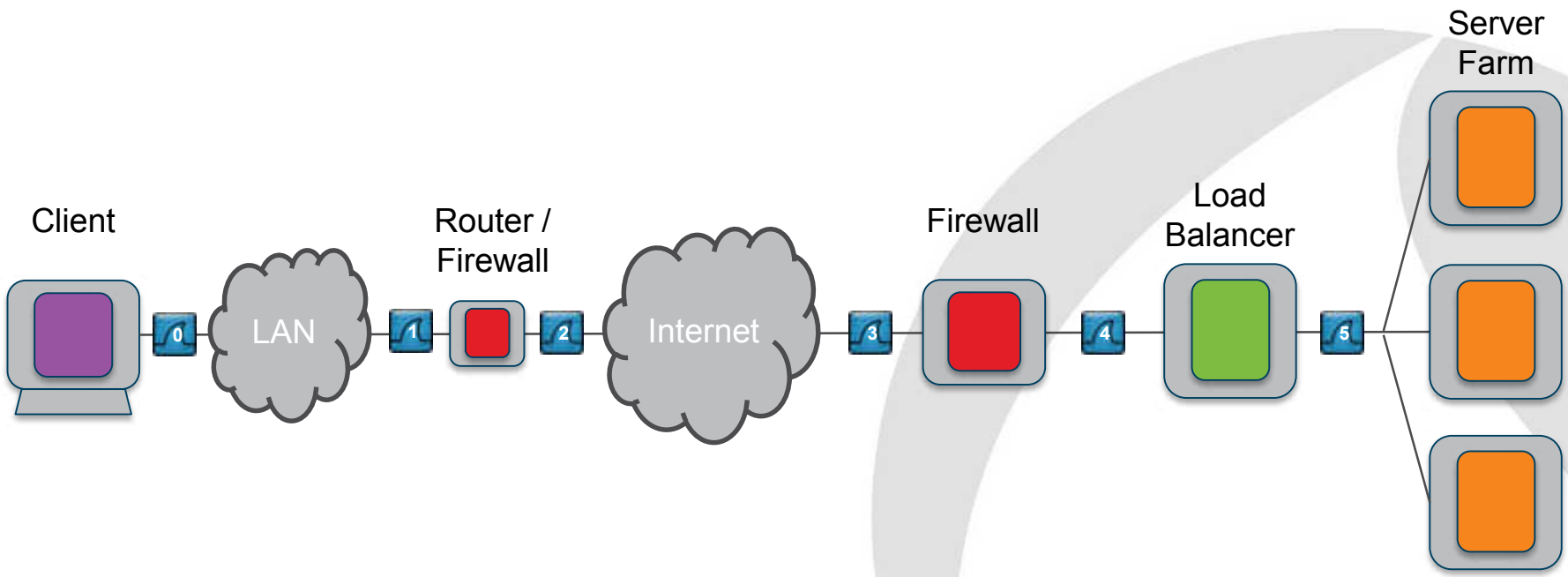
Packet Matching

Paul Offord, Advance7

Relax!

Model network



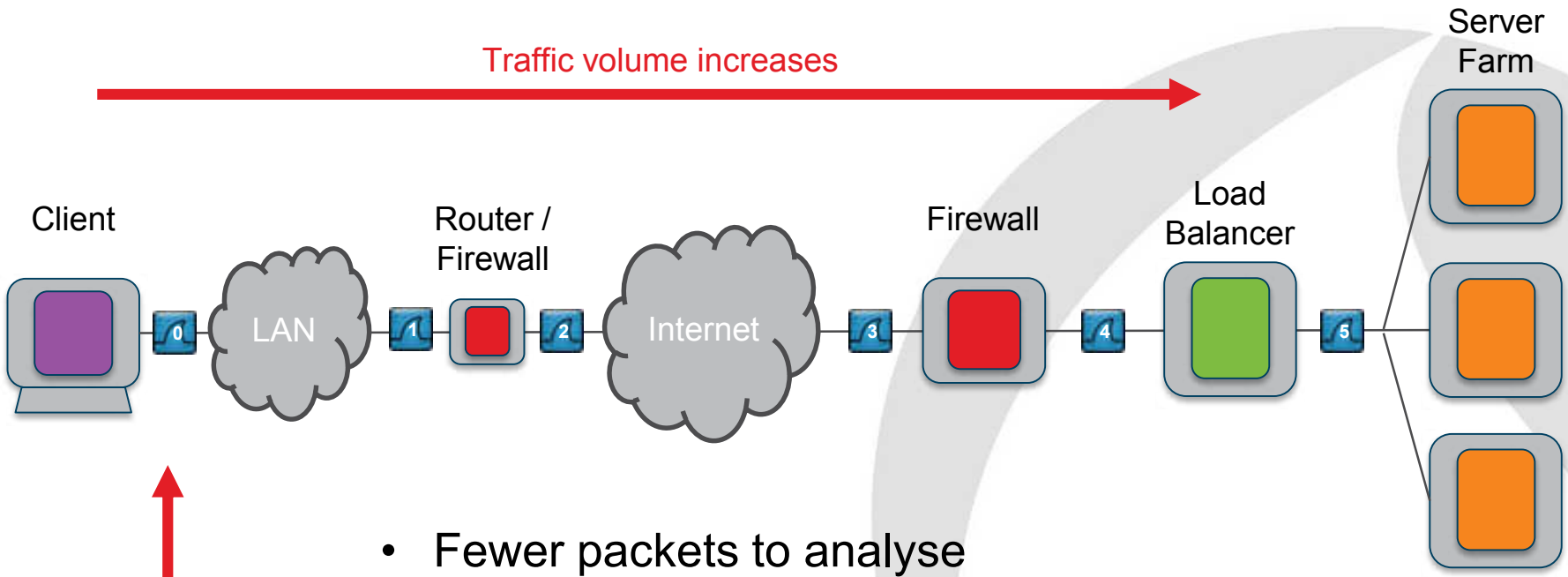
The challenge

- Matching packets from PC to 1st server tier
- NAT and PAT
- VIPs
- SSL especially with load balancers
- Volumes increase deeper into the system
- Capture time sync inaccuracies

Packet matching based on …

- Protocol field values
  - Direct match
  - Translated match
- Packet content
- Temporal match (relative times)
- Supplementary data e.g. web logs

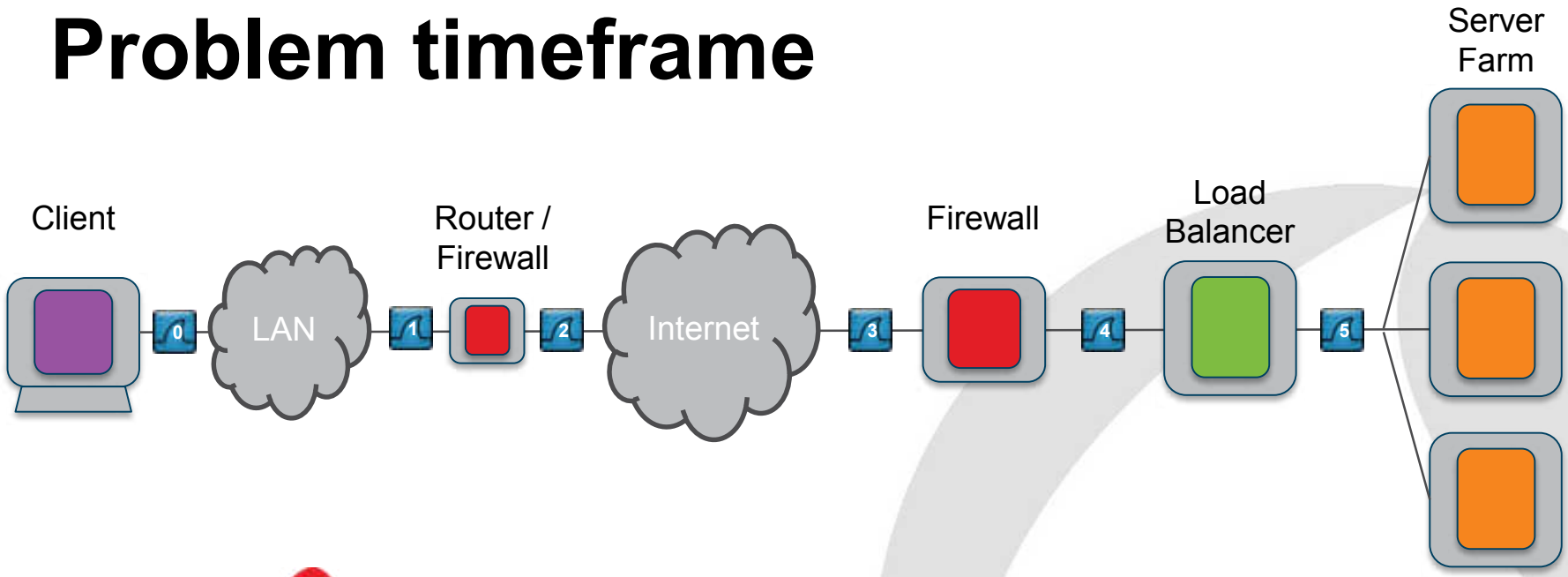
Edge inwards



Start the analysis here

- Fewer packets to analyse
- Best chance of match to users experience
- Provides signposts for the other traces
- Establish problem timeframe

Problem timeframe

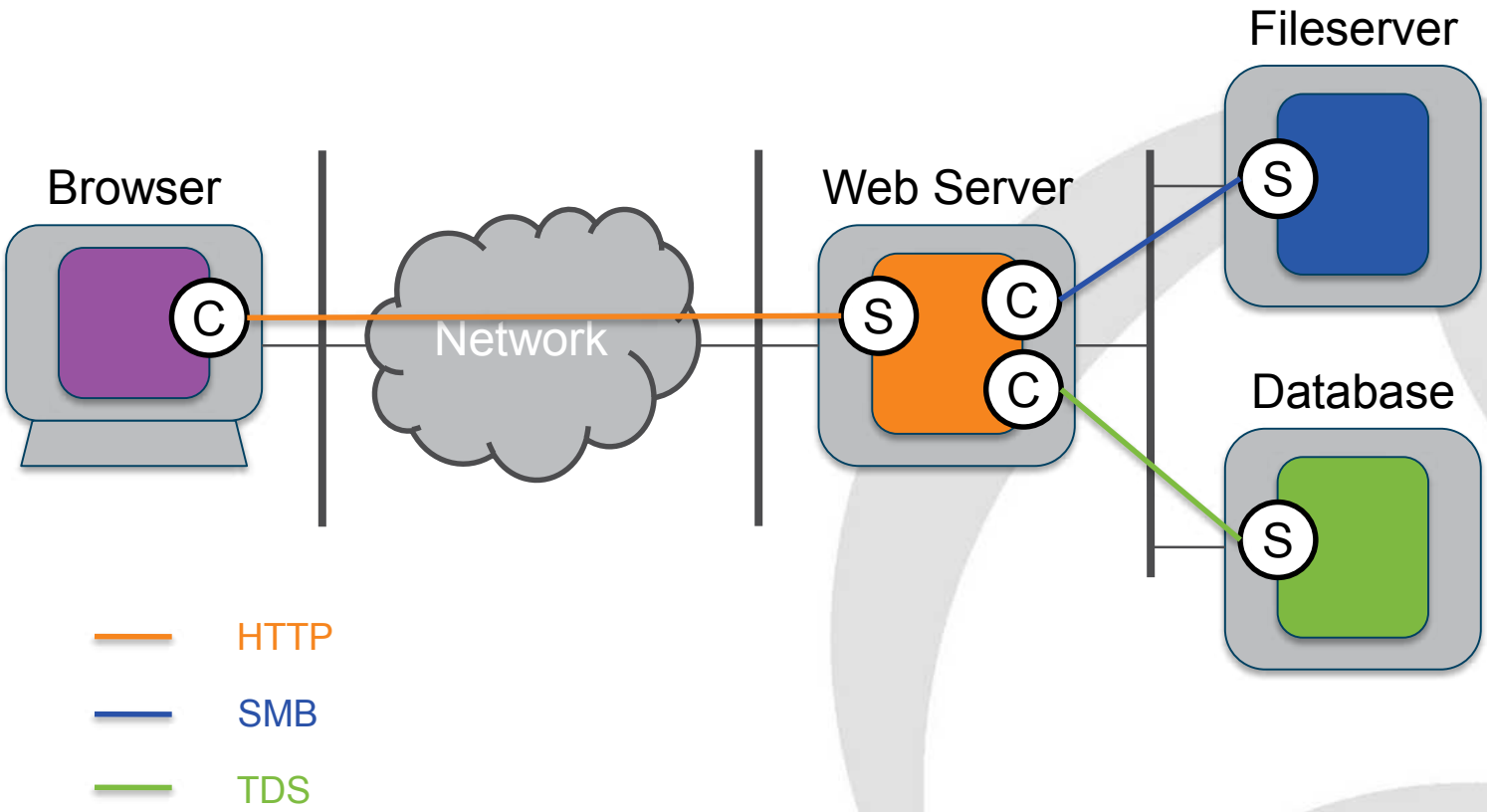


Network Trace Analysis Guide for details

www.tribelabzero.com

tribelab

Client and Service



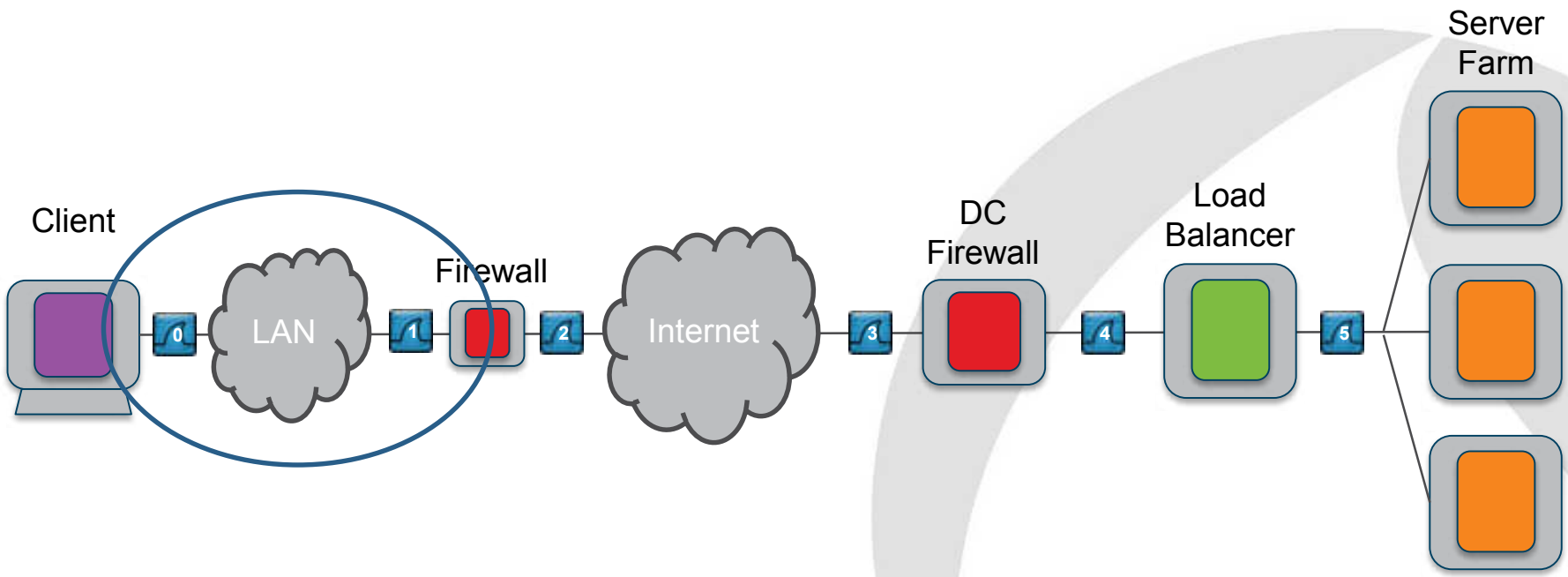
Identifying a stream - the 5-tuple

Client IP Addr : Client Port : Service IP Addr : Service Port : Protocol

192.168.1.139 : 1515 : 25.34.5.1 : 80 : TCP

192.168.1.139 : 49495 : 192.168.247.72 : 53 : UDP

Across the LAN



Across the LAN: Client to Service

No.	Time	Source	Destination	Protocol	Length	Info
782	4.28918300	10.0.0.101	82.165.203.202	HTTP	466	GET / HTTP/1.1
871	4.49797100	82.165.203.202	10.0.0.101	TCP	60	80→60170 [ACK] Seq=176892208 Ack=662554198
974	5.13406200	82.165.203.202	10.0.0.101	TCP	1514	[TCP segment of a reassembled PDU]
975	5.13436500	82.165.203.202	10.0.0.101	TCP	797	[TCP segment of a reassembled PDU]
976	5.13467400	10.0.0.101	82.165.203.202	TCP	54	60170→80 [ACK] Seq=662554198 Ack=176893668

```
⊞ Frame 782: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_d8:1e:72 (34:02:86:d8:1e:72), Dst: Fortinet_6f:a0:bc (08:5b:0e:6f:a0:bc)
⊟ Internet Protocol Version 4, Src: 10.0.0.101 (10.0.0.101), Dst: 82.165.203.202 (82.165.203.202)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT)
    Total Length: 452
    Identification: 0x4768 (18280)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x88f7 [validation disabled]
    Source: 10.0.0.101 (10.0.0.101)
    Destination: 82.165.203.202 (82.165.203.202)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: 60170 (60170), Dst Port: 80 (80), Seq: 662553786, Ack: 176892208, Len:
    Source Port: 60170 (60170)
    Destination Port: 80 (80)
    [Stream index: 9]
    [TCP Segment Len: 412]
    Sequence number: 662553786
    [Next sequence number: 662554198]
    Acknowledgment number: 176892208
    Header Length: 20 bytes
```

Identifies the stream

Across the LAN: Service to Client

No.	Time	Source	Destination	Protocol	Length	Info
782	4.28918300	10.0.0.101	82.165.203.202	HTTP	466	GET / HTTP/1.1
871	4.49797100	82.165.203.202	10.0.0.101	TCP	60	80→60170 [ACK] Seq=176892208 Ack=662554198
974	5.13406200	82.165.203.202	10.0.0.101	TCP	1514	[TCP segment of a reassembled PDU]
975	5.13436500	82.165.203.202	10.0.0.101	TCP	797	[TCP segment of a reassembled PDU]
976	5.13467400	10.0.0.101	82.165.203.202	TCP	54	60170→80 [ACK] Seq=662554198 Ack=176893668

```
⊞ Frame 974: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
⊞ Ethernet II, Src: Fortinet_6f:a0:bc (08:5b:0e:6f:a0:bc), Dst: IntelCor_d8:1e:72 (34:02:86:d8:1e:72)
⊟ Internet Protocol Version 4, Src: 82.165.203.202 (82.165.203.202), Dst: 10.0.0.101 (10.0.0.101)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x20 (DSCP 0x08: Class Selector 1; ECN: 0x00: Not-ECN-Capable Transpo
    Total Length: 1500
    Identification: 0x3d61 (15713)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 47
    Protocol: TCP (6)
  ⊞ Header checksum: 0xdfc6 [validation disabled]
    Source: 82.165.203.202 (82.165.203.202)
    Destination: 10.0.0.101 (10.0.0.101)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 60170 (60170), Seq: 176892208, Ack: 662554198, Len:
    Source Port: 80 (80)
    Destination Port: 60170 (60170)
    [Stream index: 9]
    [TCP Segment Len: 1460]
    Sequence number: 176892208
    [Next sequence number: 176893668]
    Acknowledgment number: 662554198
    Header Length: 20 bytes
```

Identifies the stream

Wireshark shortcut for TCP
Follow TCP stream

Finding actual packets - TCP

No.	Time	Source	Destination	Protocol	Length	Info
782	4.28918300	10.0.0.101	82.165.203.202	HTTP	466	GET / HTTP/1.1
871	4.49797100	82.165.203.202	10.0.0.101	TCP	60	80→60170 [ACK] Seq=176892208 Ack=662554198
974	5.13406200	82.165.203.202	10.0.0.101	TCP	1514	[TCP segment of a reassembled PDU]
975	5.13436500	82.165.203.202	10.0.0.101	TCP	797	[TCP segment of a reassembled PDU]
976	5.13467400	10.0.0.101	82.165.203.202	TCP	54	60170→80 [ACK] Seq=662554198 Ack=176893668

```
⊞ Frame 782: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_d8:1e:72 (34:02:86:d8:1e:72), Dst: Fortinet_6f:a0:bc (08:5b:0e:6f:a0:bc)
⊟ Internet Protocol Version 4, Src: 10.0.0.101 (10.0.0.101), Dst: 82.165.203.202 (82.165.203.202)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 452
    Identification: 0x4768 (18280)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0x88f7 [validation disabled]
    Source: 10.0.0.101 (10.0.0.101)
    Destination: 82.165.203.202 (82.165.203.202)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: 60170 (60170), Dst Port: 80 (80), Seq: 662553786, Ack: 176892208, Len:
    Source Port: 60170 (60170)
    Destination Port: 80 (80)
    [Stream index: 9]
    [TCP Segment Len: 412]
    Sequence number: 662553786
    [Next sequence number: 662554198]
    Acknowledgment number: 176892208
    Header Length: 20 bytes
```

Cross checks

More correlation points needed

Preferred

Finding actual packets - UDP

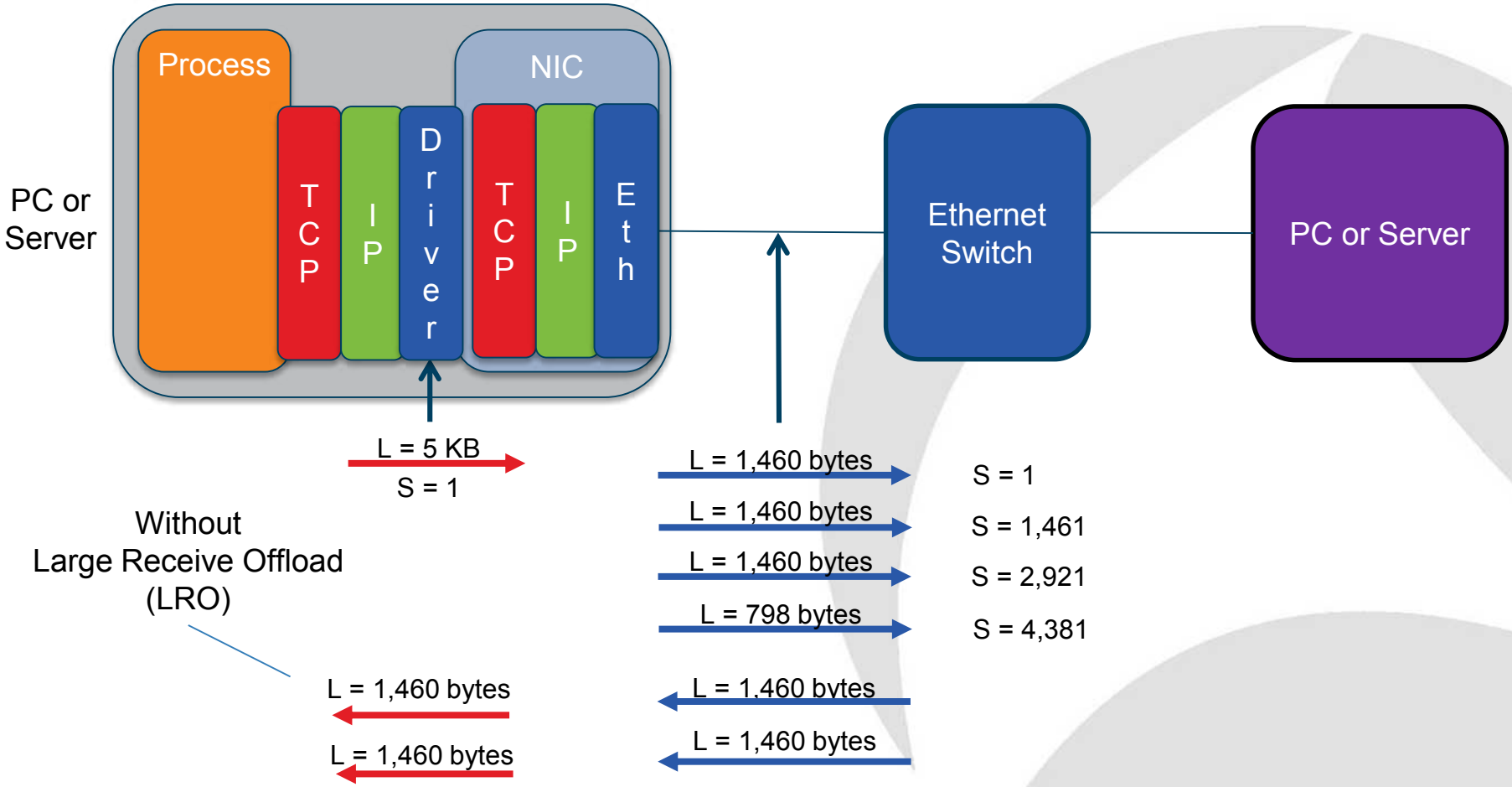
```
⊟ Frame 5742: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: 00:ff:92:17:6c:51 (00:ff:92:17:6c:51), Dst: 00:ff:93:17:6c:51 (00:ff:93:17:6c:51)
⊟ Internet Protocol Version 4, Src: 192.168.5.3 (192.168.5.3), Dst: 10.100.20.243 (10.100.20.243)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transp
    Total Length: 60
    Identification: 0x61a9 (25001)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0xf405 [validation disabled]
    Source: 192.168.5.3 (192.168.5.3)
    Destination: 10.100.20.243 (10.100.20.243)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 59408 (59408), D
    Source Port: 59408 (59408)
    Destination Port: 53 (53)
    Length: 40
  ⊞ Checksum: 0x291e [validation disabled]
    [Stream index: 3]
⊟ Domain Name System (query)
    [Response In: 5750]
    Transaction ID: 0x7b96
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
```

Use application-related IDs

DHCP Example

```
⊞ Frame 14: 356 bytes on wire (2848 bits), 356 bytes captured (2848 bits) on interface
⊞ Ethernet II, Src: IntelCor_d8:1e:72 (34:02:86:d8:1e:72), Dst: Fortinet_6f:a0:bc (08:5
⊟ Internet Protocol Version 4, Src: 10.0.0.101 (10.0.0.101), Dst: 10.0.0.1 (10.0.0.1)
    Version: 4
    Header Length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not EC
    Total Length: 342
    Identification: 0x7747 (30535)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  ⊞ Header checksum: 0xadea [validation disabled]
    Source: 10.0.0.101 (10.0.0.101)
    Destination: 10.0.0.1 (10.0.0.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
    Source Port: 68 (68)
    Destination Port: 67 (67)
    Length: 322
  ⊞ Checksum: 0x7257 [validation disabled]
    [Stream index: 5]
⊟ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x74b9b328
    Seconds elapsed: 0
```

TCP Segmentation Offload

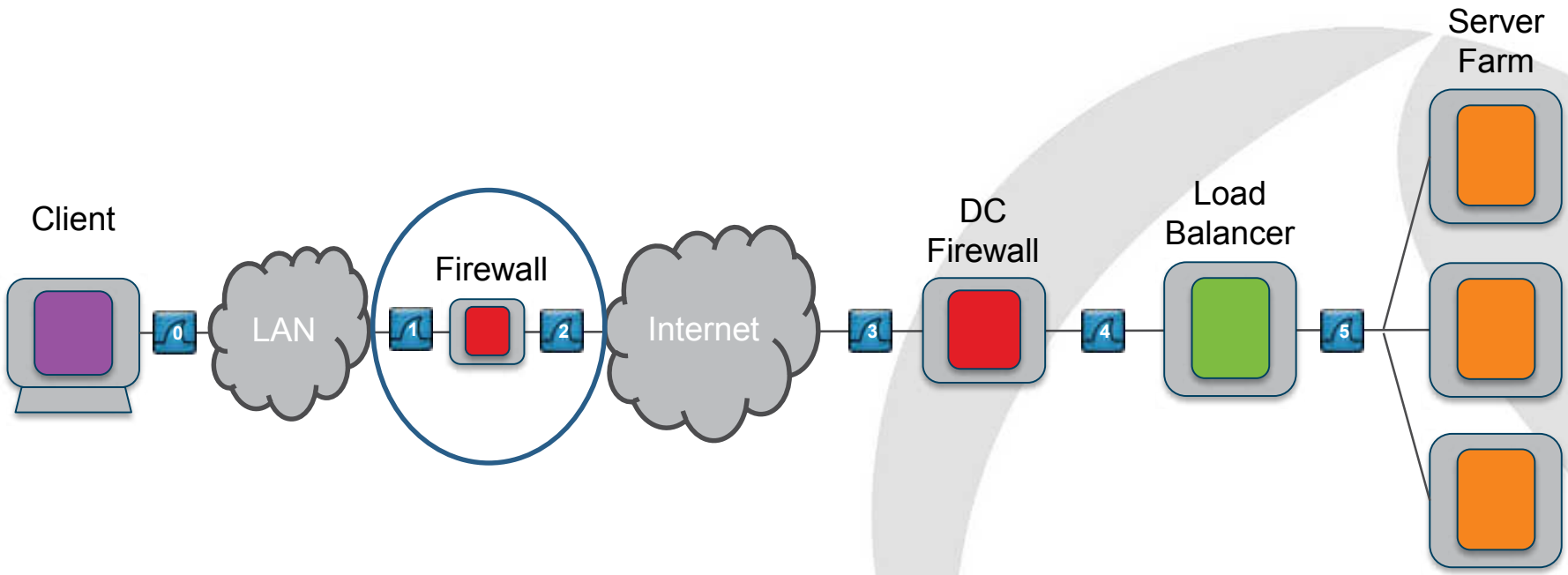


Across the LAN: Summary

- 5-tuple
- Direction (C->S or S->C)
- TCP
  - Sequence number
  - Watch out for TSO
- UDP
  - Application-related ID
- TSO => intermediate Sequence Numbers

Time for Questions

Across the firewall



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
1	14:05:41.349549	0.000000	192.168.1.139	25.34.5.1	1515	80	TCP	62	1515→80 [SYN] Seq=0
2	14:05:41.349625	0.000076	192.168.1.139	192.168.247.72	58817	53	DNS	73	Standard query 0x3e
3	14:05:41.349641	0.000016	192.168.1.139	192.168.247.72	49495	53	DNS	73	Standard query 0xec
4	14:05:41.351282	0.001641	25.34.5.1	192.168.1.139	80	1515	TCP	62	80→1515 [SYN, ACK]
5	14:05:41.351331	0.000049	192.168.1.139	25.34.5.1	1515	80	TCP	60	1515→80 [ACK] Seq=1
6	14:05:41.352643	0.001312	192.168.247.72	192.168.1.139	53	58817	DNS	125	Standard query resp
7	14:05:41.353023	0.000380	192.168.247.72	192.168.1.139	53	49495	DNS	125	Standard query resp
8	14:05:41.354312	0.001289	192.168.1.139	25.34.5.1	1515	80	HTTP	356	GET /index.html?qs=
9	14:05								
10	14:05								
11	14:05								
12	14:05								
13	14:05								
14	14:05								
15	14:05								
16	14:05								
17	14:05								

Frame 8: 3
Ethernet I
Internet P
Transmissi
Hypertext
GET /inc
Host: vm
User-Age
Accept:
Accept-L
Accept-E
Connecti
\r\n
[Full re

vmlx http client WAN.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 f

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
10	14:05:41.350135	0.492955	11.56.123.123	25.34.5.1	1515	80	TCP	62	1515→8
11	14:05:41.350366	0.000231	11.56.123.123	192.168.247.72	28652	53	DNS	73	Standa
12	14:05:41.350367	0.000001	11.56.123.123	192.168.247.72	62877	53	DNS	73	Standa
13	14:05:41.351123	0.000756	25.34.5.1	11.56.123.123	80	1515	TCP	62	80→151
14	14:05:41.351629	0.000506	11.56.123.123	25.34.5.1	1515	80	TCP	60	1515→8
15	14:05:41.352641	0.001012	192.168.247.72	11.56.123.123	53	28652	DNS	125	Standa
16	14:05:41.352876	0.000235	192.168.247.72	11.56.123.123	53	62877	DNS	125	Standa
17	14:05:41.354620	0.001744	11.56.123.123	25.34.5.1	1515	80	HTTP	356	GET /i
18	14:05:41.354863	0.000243	25.34.5.1	11.56.123.123	80	1515	TCP	60	80→151
19	14:05:41.359130	0.004267	25.34.5.1	11.56.123.123	80	1515	TCP	1434	[TCP s
20	14:05:41.359366	0.000236	25.34.5.1	11.56.123.123	80	1515	TCP	1434	[TCP s
21	14:05:41.359618	0.000252	25.34.5.1	11.56.123.123	80	1515	TCP	1434	[TCP s
22	14:05:41.359859	0.000241	11.56.123.123	25.34.5.1	1515	80	TCP	60	1515→8
23	14:05:41.360614	0.000755	25.34.5.1	11.56.123.123	80	1515	TCP	1434	[TCP s
24	14:05:41.360615	0.000001	25.34.5.1	11.56.123.123	80	1515	TCP	1434	[TCP s

vmlx http client LAN.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

elta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
0.001641	25.34.5.1	192.168.1.139	80	1515	TCP	62	0x0000 (0)	2048319624	80→1515 [SYN, ACK
0.000049	192.168.1.139	25.34.5.1	1515	80	TCP	60	0x59ee (23022)	1043578710	1515→80 [ACK] Seq=
0.001312	192.168.247.72	192.168.1.139	53	58817	DNS	125	0xb697 (46743)		Standard query res
0.000380	192.168.247.72	192.168.1.139	53	49495	DNS	125	0xb698 (46744)		Standard query res
0.001289	192.168.1.139	25.34.5.1	1515	80	HTTP	35	0x59f1 (23025)	1043578710	GET /index.html?q
0.000641	25.34.5.1	192.168.1.139	80	1515	TCP	60	0x76e7 (30439)	2048319625	80→1515 [ACK] Seq=
0.004267	25.34.5.1	192.168.1.139	80	1515	TCP	1434	0x76e8 (30440)	2048319625	[TCP segment of a
0.000149	25.34.5.1	192.168.1.139	80	1515	TCP	1434	0x76e9 (30441)	2048321005	[TCP segment of a
0.000294	25.34.5.1	192.168.1.139	80	1515	TCP	1434	0x76ea (30442)	2048322385	[TCP segment of a

vmlx http client WAN.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

elta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
0.000235	192.168.247.72	11.56.123.123	53	62877	DNS	125	0xb698 (46744)		Standard query res
0.001744	11.56.123.123	25.34.5.1	1515	80	HTTP	35	0x59f1 (23025)	1043578710	GET /index.html?q
0.000243	25.34.5.1	11.56.123.123	80	1515	TCP	60	0x76e7 (30439)	2048319625	80→1515 [ACK] Seq=
0.004267	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76e8 (30440)	2048319625	[TCP segment of a
0.000236	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76e9 (30441)	2048321005	[TCP segment of a
0.000252	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76ea (30442)	2048322385	[TCP segment of a
0.000241	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f2 (23026)	1043579012	1515→80 [ACK] Seq=
0.000755	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76eb (30443)	2048323765	[TCP segment of a
0.000001	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76ec (30444)	2048325145	[TCP segment of a
0.000249	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76ed (30445)	2048326525	[TCP segment of a
0.000002	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f3 (23027)	1043579012	1515→80 [ACK] Seq=

SNAT, DNAT, SPAT and DPAT

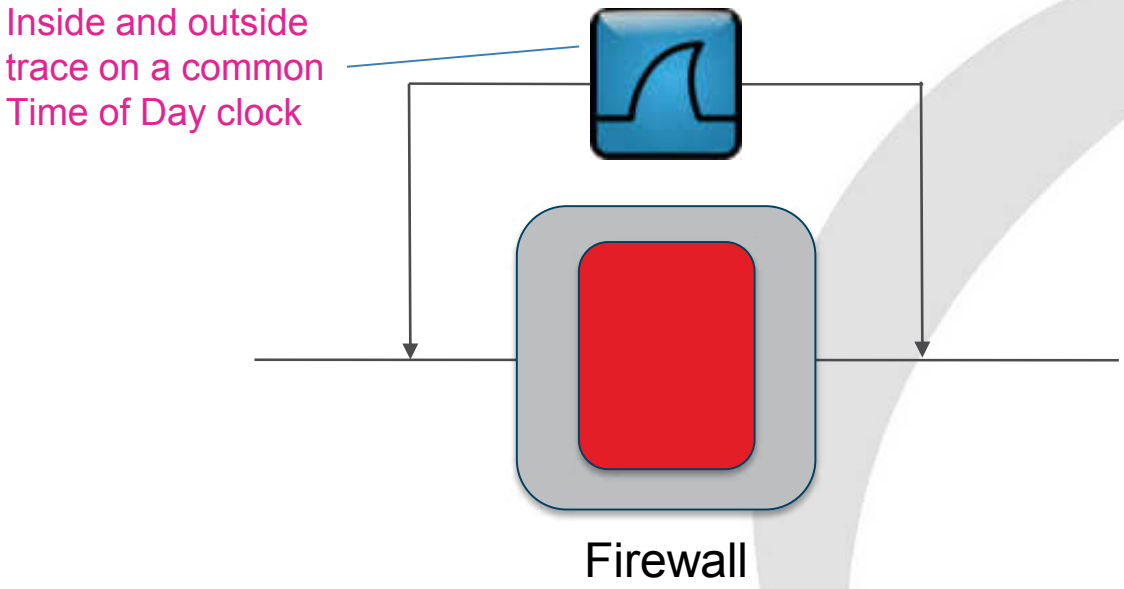
When talking NAT:

Source = Client

Destination = Service

Think – Source of SYN

Multiport capture

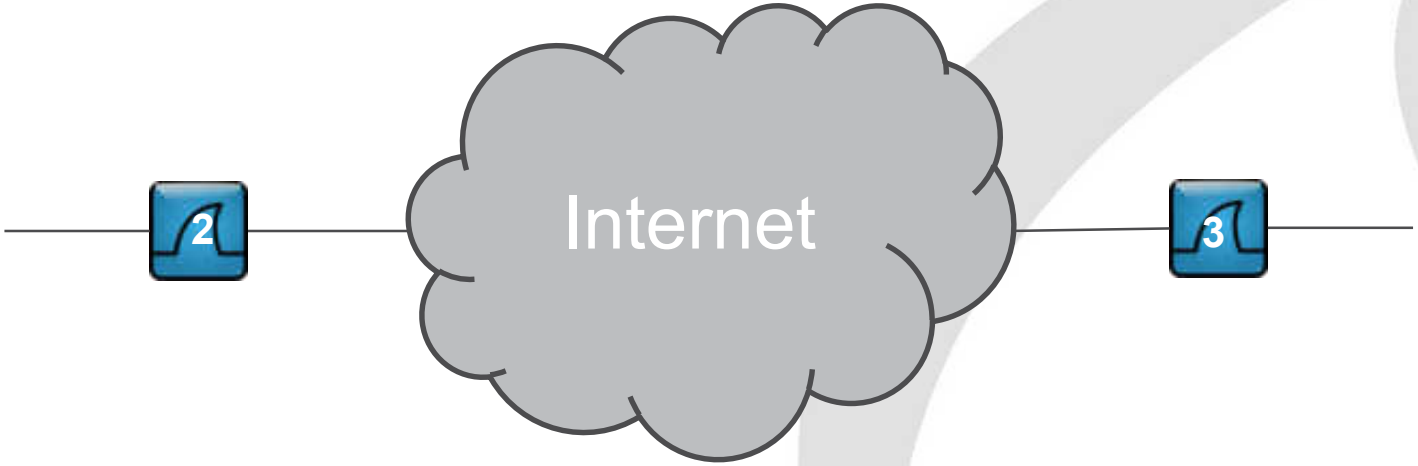


Across a firewall: Summary

- NAT/PAT
  - Client address always translated
  - Client port maybe translated
- IP ID and TCP Seq matching
  - Should work
  - May not on some firewalls
  - Try enabling TCP Relative Sequence Numbers
- Common ToD clock is a big help

Time for Questions

Across a WAN (or the Internet)



5-tuple + IP ID

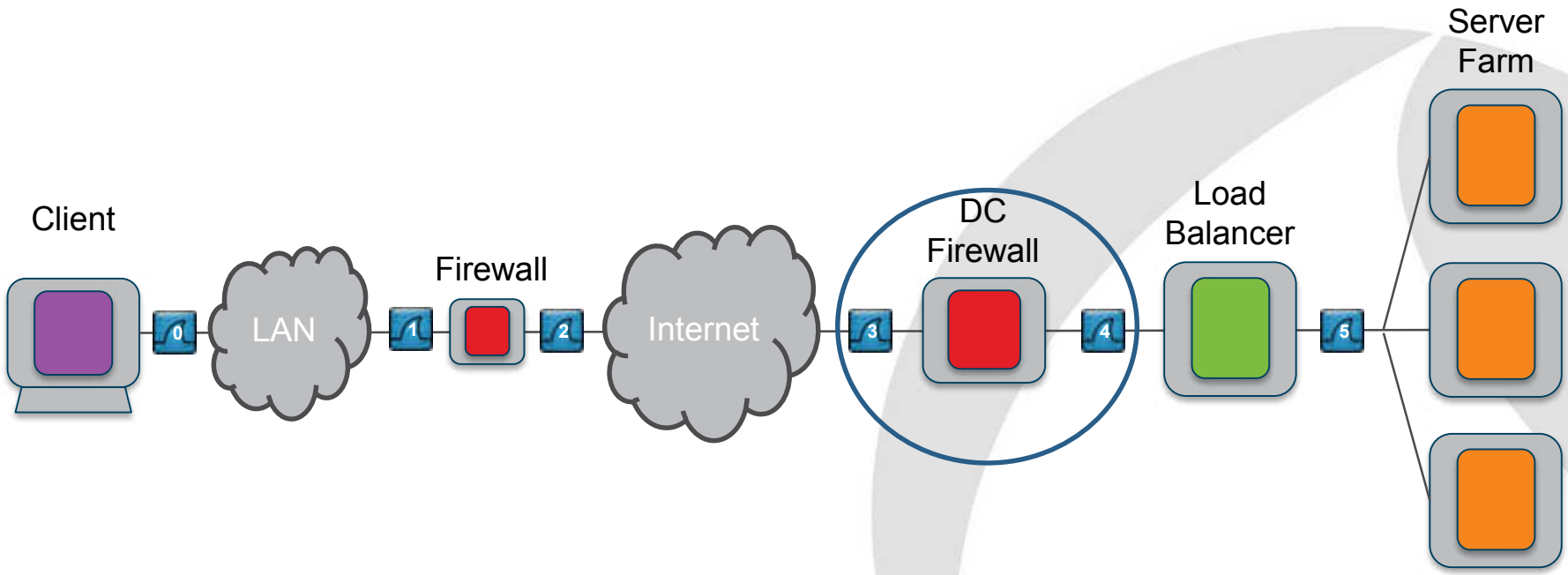
TCP: Seq Number

UDP: App-related ID

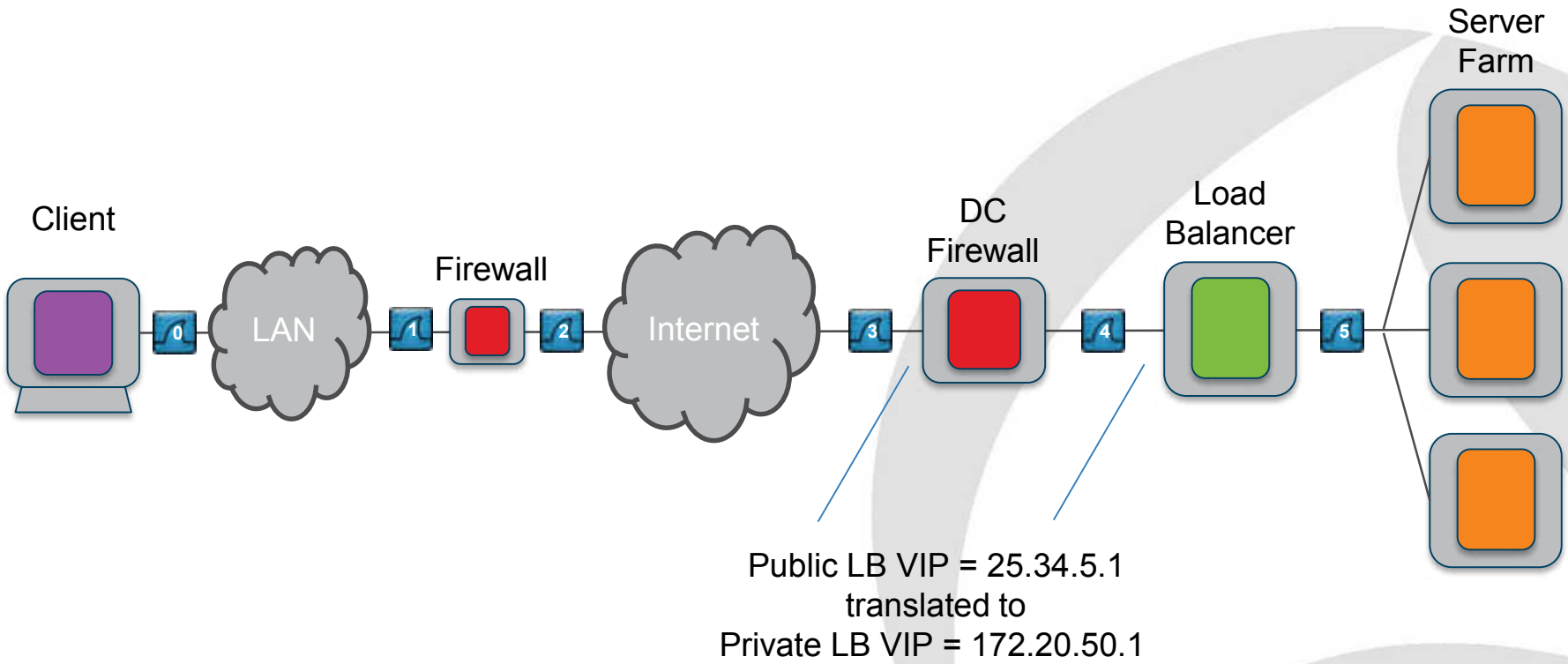
Across the WAN: Summary

- Same as LAN
- Data volumes may be high
  - Carefully filter
  - Keep original trace files!
- Sync’d clocks helps
  - AD time sync every 8 hours
  - Clock drift up to 8ms in 24 hours
  - Take care with time zones and DST

Across the DC firewall



Across the DC firewall: Dest NAT



Expression... Clear Apply Save

	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
.350135	0.000000	11.56.123.123	25.34.5.1	1515	80	TCP	62	0x59eb (23019)	1043578709	1515→80
.351123	0.000988	25.34.5.1	11.56.123.123	80	1515	TCP	62	0x0000 (0)	2048319624	80→1515
.351629	0.000506	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59ee (23022)	1043578710	1515→80
.354620	0.002991	11.56.123.123	25.34.5.1	1515	80	HTTP	356	0x59f1 (23025)	1043578710	GET /inde
.354863	0.000243	25.34.5.1	11.56.123.123	80	1515	TCP	60	0x76e7 (30439)	2048319625	80→1515
.359130	0.004267	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76e8 (30440)	2048319625	[TCP seg
.359366	0.000236	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76e9 (30441)	2048321005	[TCP seg
.359618	0.000252	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76ea (30442)	2048322385	[TCP seg

vmlx http inside fw.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

Capture Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
.636675	2.005023	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Roo
.636676	0.000001	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Roo
.641452	2.004776	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Roo
.641453	0.000001	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Roo
.350368	1.708915	11.56.123.123	172.20.50.1	1515	80	TCP	62	0x59eb (23019)	3048602986	1515→80
.350611	0.000243	172.20.50.1	11.56.123.123	80	1515	TCP	62	0x0000 (0)	259644254	80→1515
.351630	0.001019	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x59ee (23022)	3048602987	1515→80
.354621	0.002991	11.56.123.123	172.20.50.1	1515	80	HTTP	356	0x59f1 (23025)	3048602987	GET /inde
.354862	0.000241	172.20.50.1	11.56.123.123	80	1515	TCP	60	0x76e7 (30439)	259644255	80→1515
.359129	0.004267	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76e8 (30440)	259644255	[TCP segm
.359367	0.000238	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76e9 (30441)	259645635	[TCP segm
.359619	0.000252	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76ea (30442)	259647015	[TCP segm
.360108	0.000489	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x59f2 (23026)	3048603289	1515→80
.360357	0.000249	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76eb (30443)	259648395	[TCP segm
.360616	0.000259	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76ec (30444)	259649775	[TCP segm
.360865	0.000249	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76ed (30445)	259651155	[TCP segm
.361107	0.000242	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x59f3 (23027)	3048603289	1515→80
.361356	0.000249	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76ee (30446)	259652535	[TCP segm

ture Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
617	0.000744	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f8 (23032)	303	1515→80 [ACK]
618	0.000001	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f9 (23033)	303	[TCP window u
374	12.191756	11.56.123.123	25.34.5.1	1515	80	HTTP	356	0x5a00 (23040)	303	GET /index.ht
107	0.004733	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76f5 (30453)	17247	[TCP segment

vmlx http inside fw.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

ure Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
58	0.000002	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Root =
66	2.005008	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Root =
68	0.000002	Cisco_40:54:83	Spanning-tree-(for-			STP	60			Conf. Root =
86	0.436218	Cisco_40:54:83	Cisco_40:54:83			LOOP	60			Reply
10	1.448324	11.56.123.123	172.20.50.1	1515	80	HTTP	356	0x5a00 (23040)	303	GET /index.htm
59	0.004249	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76f5 (30453)	17247	[TCP segment c
56	0.000497	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76f6 (30454)	18627	[TCP segment c
09	0.000253	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76f7 (30455)	20007	[TCP segment c
05	0.000496	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76f8 (30456)	21387	[TCP segment c
61	0.000256	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76f9 (30457)	22767	[TCP segment c
62	0.000001	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x5a01 (23041)	605	1515→80 [ACK]
63	0.000001	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x5a02 (23042)	605	1515→80 [ACK]
08	0.000245	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76fa (30458)	24147	[TCP segment c
09	0.000001	11.56.123.123	172.20.50.1	1515	80	TCP	60	0x5a03 (23043)	605	[TCP ACKed uns
10	0.000001	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76fb (30459)	25527	[TCP segment c
62	0.000252	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76fc (30460)	26907	[TCP segment c
65	0.000003	172.20.50.1	11.56.123.123	80	1515	TCP	1434	0x76fd (30461)	28287	[TCP segment c

Analyze Statistics Telephony Tools Internals Help

Expression... Clear Apply Save

Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	IP ID	tcp seq	Info
0.000001	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f7 (23031)		303 1515→80 [ACK]
0.000744	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f8 (23032)		303 1515→80 [ACK]
0.000001	11.56.123.123	25.34.5.1	1515	80	TCP	60	0x59f9 (23033)		303 [TCP window u
12.191756	11.56.123.123	25.34.5.1	1515	80	HTTP	356	0x5a00 (23040)		303 GET /index.ht
0.004733	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76f5 (30453)	17247	[TCP segment
0.000001	25.34.5.1	11.56.123.123	80	1515	TCP	1434	0x76f6 (30454)	18627	[TCP segment

vmlx http inside fw.pcapng [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

Analyze Statistics Telephony Tools Internals

Expre

Delta	Source	Destinati
0.000002	Cisco_40:54:83	Spann
2.005008	Cisco_40:54:83	Spann
0.000002	Cisco_40:54:83	Spann
0.436218	Cisco_40:54:83	Cisco_
1.448324	11.56.123.123	172.20
0.004249	172.20.50.1	11.56.
0.000497	172.20.50.1	11.56.
0.000253	172.20.50.1	11.56.
0.000496	172.20.50.1	11.56.
0.000256	172.20.50.1	11.56.
0.000001	11.56.123.123	172.20
0.000001	11.56.123.123	172.20
0.000245	172.20.50.1	11.56.
0.000001	11.56.123.123	172.20
0.000001	172.20.50.1	11.56.
0.000252	172.20.50.1	11.56.
0.000003	172.20.50.1	11.56.

vmlx http inside fw.pcapng [Wiresha

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 0 Expression... Clear Apply Save

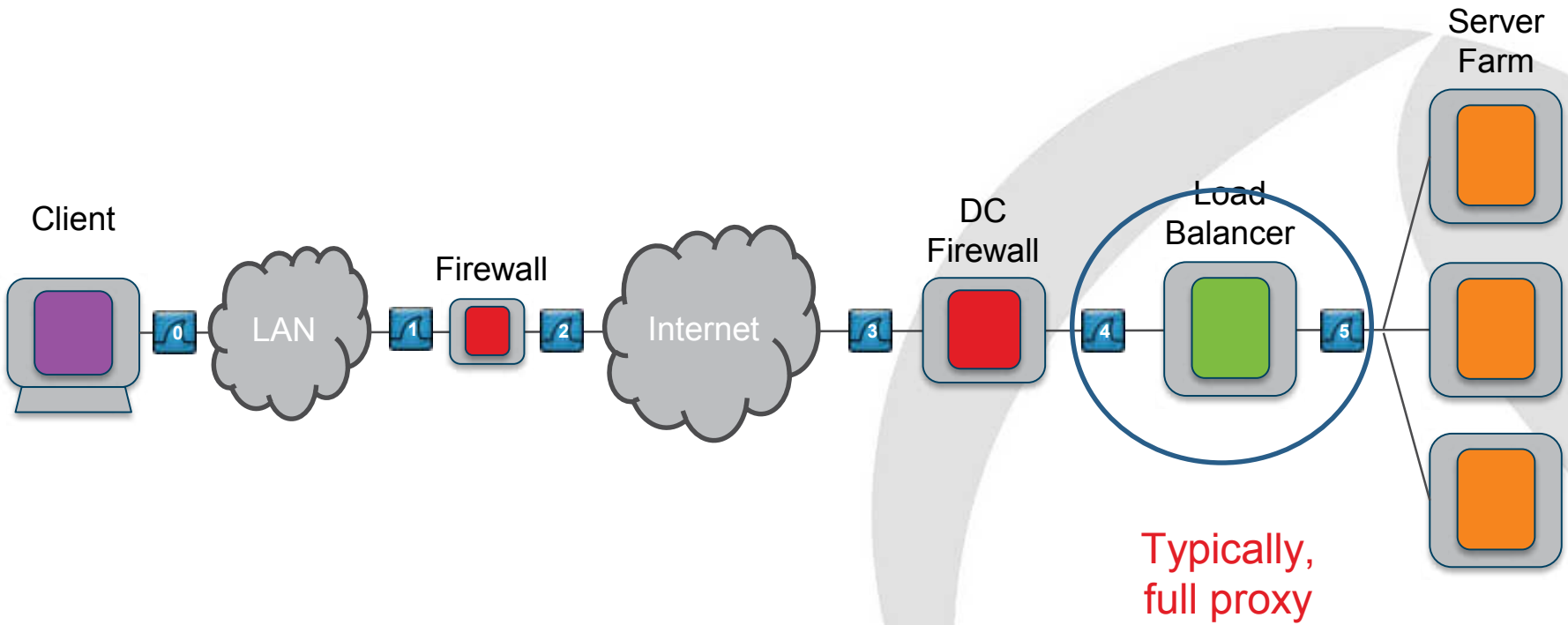
No.	Time	Delta	Source	Destination	Src Port
34	14:05:41.362614	0.000000	172.20.50.1	11.56.123.123	80
35	14:05:41.362869	0.000255	172.20.50.1	11.56.123.123	80
36	14:05:41.362871	0.000002	172.20.50.1	11.56.123.123	80
37	14:05:41.362872	0.000001	11.56.123.123	172.20.50.1	1515
38	14:05:41.363618	0.000746	11.56.123.123	172.20.50.1	1515
39	14:05:41.363860	0.000242	11.56.123.123	172.20.50.1	1515
58	14:05:53.555610	12.191750	11.56.123.123	172.20.50.1	1515
59	14:05:53.559859	0.004249	172.20.50.1	11.56.123.123	80
60	14:05:53.560356	0.000497	172.20.50.1	11.56.123.123	80
61	14:05:53.560609	0.000253	172.20.50.1	11.56.123.123	80
62	14:05:53.561105	0.000496	172.20.50.1	11.56.123.123	80
63	14:05:53.561361	0.000256	172.20.50.1	11.56.123.123	80
64	14:05:53.561362	0.000001	11.56.123.123	172.20.50.1	1515
65	14:05:53.561363	0.000001	11.56.123.123	172.20.50.1	1515
66	14:05:53.561608	0.000245	172.20.50.1	11.56.123.123	80
67	14:05:53.561609	0.000001	11.56.123.123	172.20.50.1	1515

Across the DC firewall: Summary

- **ALWAYS** trace both sides of a firewall
- WARNING – may fiddle with Seq Numbers
- Use a dual port capture if possible
- Consider possibility of HA failover
- If SNAT and DNAT also use
  - Application-related ID, or
  - Content (especially with SSL), or
  - Web log information (X-Forwarded-For)

Time for Questions

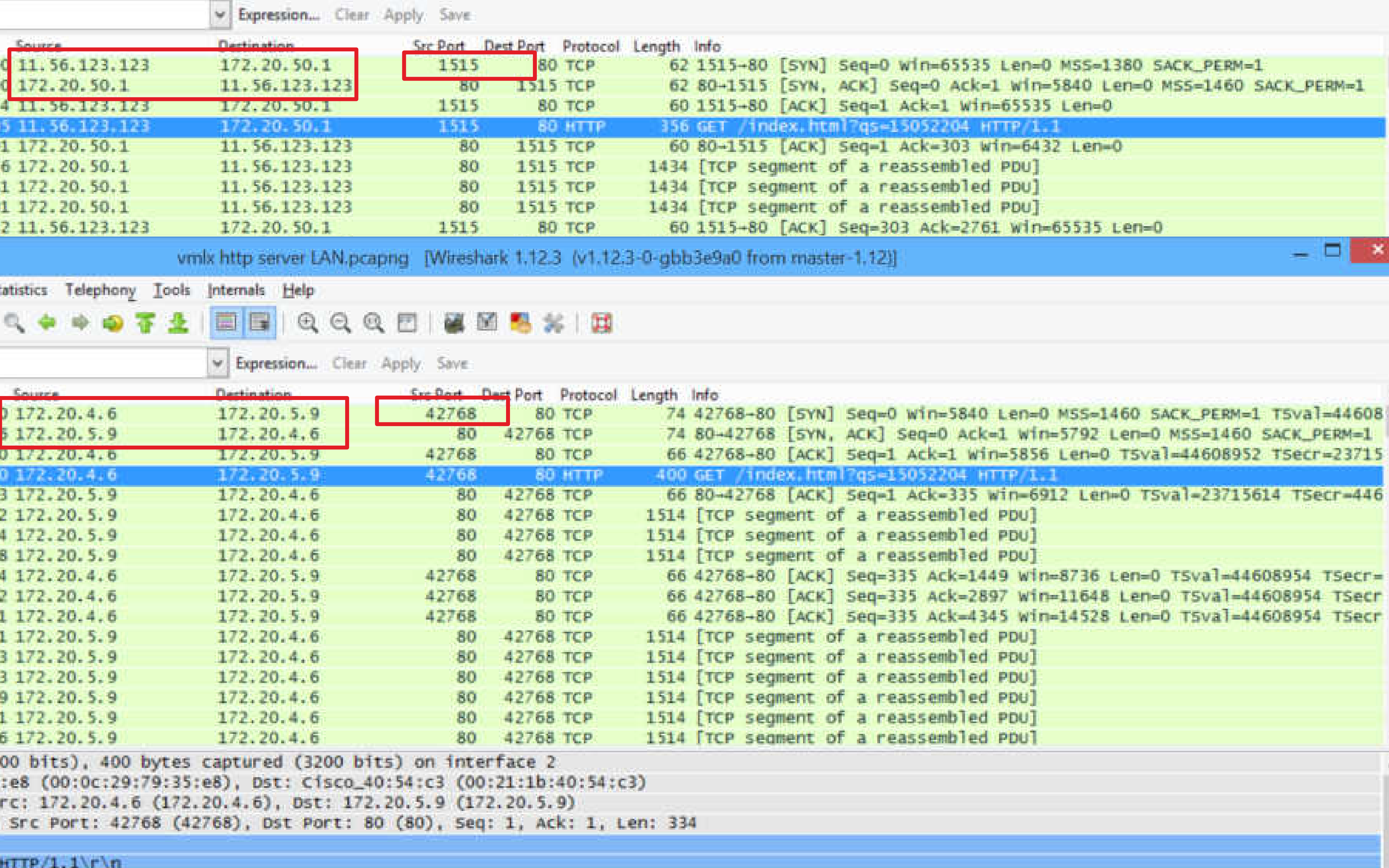
Across the Load Balancer



Typically,
full proxy

SNAT, DNAT and SPAT

Can't match on TCP Seq or IP ID



```
  Source             Destination         Src Port  Dest Port  Protocol  Length  Info
0 11.56.123.123      172.20.50.1             1515         80  TCP           62  1515→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 SACK_PERM=1
0 172.20.50.1        11.56.123.123             80       1515  TCP           62  80→1515 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
4 11.56.123.123      172.20.50.1             1515         80  TCP           60  1515→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
5 11.56.123.123      172.20.50.1             1515         80  HTTP         356  GET /index.html?qs=15052204 HTTP/1.1
1 172.20.50.1        11.56.123.123             80       1515  TCP           60  80→1515 [ACK] Seq=1 Ack=303 Win=6432 Len=0
6 172.20.50.1        11.56.123.123             80       1515  TCP         1434  [TCP segment of a reassembled PDU]
1 172.20.50.1        11.56.123.123             80       1515  TCP         1434  [TCP segment of a reassembled PDU]
1 172.20.50.1        11.56.123.123             80       1515  TCP         1434  [TCP segment of a reassembled PDU]
2 11.56.123.123      172.20.50.1             1515         80  TCP           60  1515→80 [ACK] Seq=303 Ack=2761 Win=65535 Len=0
```

vmlx http server LAN.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

```
  Source             Destination         Src Port  Dest Port  Protocol  Length  Info
0 172.20.4.6         172.20.5.9             42768         80  TCP           74  42768→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=44608
6 172.20.5.9         172.20.4.6                80      42768  TCP           74  80→42768 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
0 172.20.4.6         172.20.5.9             42768         80  TCP           66  42768→80 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=44608952 TSecr=23715
0 172.20.4.6         172.20.5.9             42768         80  HTTP         400  GET /index.html?qs=15052204 HTTP/1.1
3 172.20.5.9         172.20.4.6                80      42768  TCP           66  80→42768 [ACK] Seq=1 Ack=335 Win=6912 Len=0 TSval=23715614 TSecr=446
2 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
4 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
8 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
4 172.20.4.6         172.20.5.9             42768         80  TCP           66  42768→80 [ACK] Seq=335 Ack=1449 Win=8736 Len=0 TSval=44608954 TSecr=
2 172.20.4.6         172.20.5.9             42768         80  TCP           66  42768→80 [ACK] Seq=335 Ack=2897 Win=11648 Len=0 TSval=44608954 TSecr
1 172.20.4.6         172.20.5.9             42768         80  TCP           66  42768→80 [ACK] Seq=335 Ack=4345 Win=14528 Len=0 TSval=44608954 TSecr
1 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
3 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
3 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
9 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
1 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
6 172.20.5.9         172.20.4.6                80      42768  TCP         1514  [TCP segment of a reassembled PDU]
```

```
00 bits), 400 bytes captured (3200 bits) on interface 2
:e8 (00:0c:29:79:35:e8), Dst: Cisco_40:54:c3 (00:21:1b:40:54:c3)
rc: 172.20.4.6 (172.20.4.6), Dst: 172.20.5.9 (172.20.5.9)
 Src Port: 42768 (42768), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 334

HTTP/1.1\r\n
```

Expression... Clear Apply Save

Source	Destination	Src Port	Dest Port	Protocol	Length	Info
0 11.56.123.123	172.20.50.1	1515	80	TCP	62	1515→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 SACK_PERM=1
0 172.20.50.1	11.56.123.123	80	1515	TCP	62	80→1515 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
4 11.56.123.123	172.20.50.1	1515	80	TCP	60	1515→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
5 11.56.123.123	172.20.50.1	1515	80	HTTP	356	GET /index.html?qs=15052204 HTTP/1.1
1 172.20.50.1	11.56.123.123	80	1515	TCP	60	80→1515 [ACK] Seq=1 Ack=303 Win=6432 Len=0
6 172.20.50.1	11.56.123.123	80	1515	TCP	1434	[TCP segment of a reassembled PDU]
1 172.20.50.1	11.56.123.123	80	1515	TCP	1434	[TCP segment of a reassembled PDU]
1 172.20.50.1	11.56.123.123	80	1515	TCP	1434	[TCP segment of a reassembled PDU]
2 11.56.123.123	172.20.50.1	1515	80	TCP	60	1515→80 [ACK] Seq=303 Ack=2761 Win=65535 Len=0

vmlx http server LAN.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

tatistics Telephony Tools Internals Help

Expression... Clear Apply Save

Source	Destination	Src Port	Dest Port	Protocol	Length	Info
0 172.20.4.6	172.20.5.9	42768	80	TCP	74	42768→80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=44608
6 172.20.5.9	172.20.4.6	80	42768	TCP	74	80→42768 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1
0 172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=1 Ack=1 Win=5856 Len=0 TSval=44608952 TSecr=23715
0 172.20.4.6	172.20.5.9	42768	80	HTTP	400	GET /index.html?qs=15052204 HTTP/1.1
3 172.20.5.9	172.20.4.6	80	42768	TCP	66	80→42768 [ACK] Seq=1 Ack=335 Win=6912 Len=0 TSval=23715614 TSecr=446
2 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
4 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
8 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
4 172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335 Ack=1449 Win=8736 Len=0 TSval=44608954 TSecr=
2 172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335 Ack=2897 Win=11648 Len=0 TSval=44608954 TSecr
1 172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335 Ack=4345 Win=14528 Len=0 TSval=44608954 TSecr
1 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
3 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
3 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
9 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
1 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]
6 172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reassembled PDU]

```
00 bits), 400 bytes captured (3200 bits) on interface 2
:e8 (00:0c:29:79:35:e8), Dst: Cisco_40:54:c3 (00:21:1b:40:54:c3)
rc: 172.20.4.6 (172.20.4.6), Dst: 172.20.5.9 (172.20.5.9)
 Src Port: 42768 (42768), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 334
HTTP/1.1\r\n
```

vmlx http SLB.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
1	14:05:41.350502	0.000000	11.56.123.123	172.20.50.1	1515	80	TCP	62	1515→80 [SYN] Seq=0 Win
2	14:05:41.350502	0.000000	172.20.50.1	11.56.123.123	80	1515	TCP	62	80→1515 [SYN, ACK] Seq=
3	14:05:41.351746	0.001244	11.56.123.123	172.20.50.1	1515	80	TCP	60	1515→80 [ACK] Seq=1 Ack
4	14:05:41.354741	0.002995	11.56.123.123	172.20.50.1	1515	80	HTTP	356	GET /index.html?qs=1505

vmlx http server LAN.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
1	14:05:41.351747	0.000000	172.20.4.6	172.20.5.9	42768	80	TCP	74	42768→80 [SYN] Seq=0 W
2	14:05:41.351993	0.000246	172.20.5.9	172.20.4.6	80	42768	TCP	74	80→42768 [SYN, ACK] Se
3	14:05:41.351993	0.000000	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=1 A
4	14:05:41.354993	0.003000	172.20.4.6	172.20.5.9	42768	80	HTTP	400	GET /index.html?qs=150
5	14:05:41.354996	0.000003	172.20.5.9	172.20.4.6	80	42768	TCP	66	80→42768 [ACK] Seq=1 A
6	14:05:41.358988	0.003992	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
7	14:05:41.359232	0.000244	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
8	14:05:41.359510	0.000278	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
9	14:05:41.359514	0.000004	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335
10	14:05:41.359516	0.000002	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335
11	14:05:41.359517	0.000001	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [ACK] Seq=335
12	14:05:41.359988	0.000471	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
13	14:05:41.360231	0.000243	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
14	14:05:41.360484	0.000253	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
15	14:05:41.360733	0.000249	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
16	14:05:41.360984	0.000251	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas
17	14:05:41.361250	0.000266	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment of a reas

```
⊞ Frame 4: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on interface 2
⊞ Ethernet II, Src: Vmware_79:35:e8 (00:0c:29:79:35:e8), Dst: Cisco_40:54:c3 (00:21:1b:40:54:c3)
⊞ Internet Protocol Version 4, Src: 172.20.4.6 (172.20.4.6), Dst: 172.20.5.9 (172.20.5.9)
```

When to connect to the server?

What if I want load balancing based on a cookie value?

Delayed Binding

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
1	14:05:41.350502	0.000000	11.56.123.123	172.20.50.1	1515	80	TCP	62	1515→80 [SYN] Seq=0 Win=65535 Len=0 MSS=1380 SACK_PERM=1
2	14:05:41.350502	0.000000	172.20.50.1	11.56.123.123	80	1515	TCP	62	80→1515 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PE
3	14:05:41.351746	0.001244	11.56.123.123	172.20.50.1	1515	80	TCP	60	1515→80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
4	14:05:41.354741	0.002995	11.56.123.123	172.20.50.1	1515	80	HTTP	356	GET /index.html?qs=15052204 HTTP/1.1
5	14:05:41.354742	0.000001	172.20.50.1	11.56.123.123	80	1515	TCP	60	80→1515 [ACK] Seq=1 Ack=303 Win=6432 Len=0
6	14:05:41.359518	0.004776	172.20.50.1	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
7	14:05:41.359799	0.000281	172.20.50.1						
8	14:05:41.359800	0.000001	172.20.50.1						
9	14:05:41.362232	0.002432	11.56.123.123						
10	14:05:41.362233	0.000001	172.20.50.1						
11	14:05:41.362482	0.000249	172.20.50.1						
12	14:05:41.362483	0.000001	172.20.50.1						
13	14:05:41.362483	0.000000	11.56.123.123						
14	14:05:41.362484	0.000001	172.20.50.1						
15	14:05:41.362730	0.000246	172.20.50.1						
16	14:05:41.362731	0.000001	172.20.50.1						
17	14:05:41.362732	0.000001	11.56.123.123						

```
Frame 4: 356 bytes on wire (2848 bits), 356 byt
Ethernet II, Src: Cisco_40:54:c3 (00:21:1b:40:5
Internet Protocol Version 4, Src: 11.56.123.123
Transmission Control Protocol, Src Port: 1515 (
Hypertext Transfer Protocol
  GET /index.html?qs=15052204 HTTP/1.1\r\n
  Host: vmlx.pzqm.net\r\n
  User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:3
  Accept: text/html,application/xhtml+xml,appli
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://vmlx.pzqm.net/index
  [HTTP request 1/3]
  [Response in frame: 22]
```

```
0  00 0c 29 79 35 e8 00 21  1b 40 54 c3 08 00
0  01 56 59 f1 40 00 7e 06  3c e8 0b 38 7b 7b
0  32 01 05 eb 00 50 b5 b5  fd 6b 0f 79 db 5f
0  ff ff 1c 21 00 00 47 45  54 20 2f 69 6e 64
0  2e 68 74 6d 6c 3f 71 73  3d 31 35 30 35 32
0  34 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f
0  3a 20 76 6d 6c 78 2e 70  7a 71 6d 2e 6e 65
0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d
0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64
0  73 20 4e 54 20 35 2e 31  3b 20 72 76 3a 33
0  30 29 20 47 65 63 6b 6f  2f 32 30 31 30 30
0  31 20 46 69 72 65 66 6f  78 2f 33 38 2e 30
0  41 63 63 65 70 74 3a 20  74 65 78 74 2f 68
0  6c 2c 61 70 70 6c 69 63  61 74 69 6f 6e 2f
```

File: "U:\Projects\Slides\vmlx http SLB.pcap... Packets: 162 · Disp

vmlx http server LAN.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from ma

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Delta	Source	Destination	Src Port	Dest Port	Protocol	Length	Info
1	14:05:41.351747	0.000000	172.20.4.6	172.20.5.9	42768	80	TCP	74	42768→80 [SY
2	14:05:41.351993	0.000246	172.20.5.9	172.20.4.6	80	42768	TCP	74	80→42768 [SY
3	14:05:41.351993	0.000000	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [AC
4	14:05:41.354993	0.003000	172.20.4.6	172.20.5.9	42768	80	HTTP	400	GET /index.h
5	14:05:41.354996	0.000003	172.20.5.9	172.20.4.6	80	42768	TCP	66	80→42768 [AC
6	14:05:41.358988	0.003992	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
7	14:05:41.359232	0.000244	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
8	14:05:41.359510	0.000278	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
9	14:05:41.359514	0.000004	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [AC
10	14:05:41.359516	0.000002	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [AC
11	14:05:41.359517	0.000001	172.20.4.6	172.20.5.9	42768	80	TCP	66	42768→80 [AC
12	14:05:41.359988	0.000471	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
13	14:05:41.360231	0.000243	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
14	14:05:41.360484	0.000253	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
15	14:05:41.360733	0.000249	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
16	14:05:41.360984	0.000251	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment
17	14:05:41.361250	0.000266	172.20.5.9	172.20.4.6	80	42768	TCP	1514	[TCP segment

```
⊞ Frame 4: 400 bytes on wire (3200 bits), 400 bytes captured (3200 bits) on interface 2
⊞ Ethernet II, Src: Vmware_79:35:e8 (00:0c:29:79:35:e8), Dst: Cisco_40:54:c3 (00:21:1b:40:54:c3)
⊞ Internet Protocol Version 4, Src: 172.20.4.6 (172.20.4.6), Dst: 172.20.5.9 (172.20.5.9)
⊞ Transmission Control Protocol, Src Port: 42768 (42768), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 334
⊟ Hypertext Transfer Protocol
  ⊞ GET /index.html?qs=15052204 HTTP/1.1\r\n
    Host: vmlx.pzqm.net\r\n
    User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:38.0) Gecko/20100101 Firefox/38.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    X-Forwarded-For: 11.56.123.123\r\n
    \r\n
    [Full request URI: http://vmlx.pzqm.net/index.html?qs=15052204]
    [HTTP request 1/3]
```

```
0000  00 21 1b 40 54 c3 00 0c  29 79 35 e8 08 00 45 00   .!.@T... )y5...E.
```

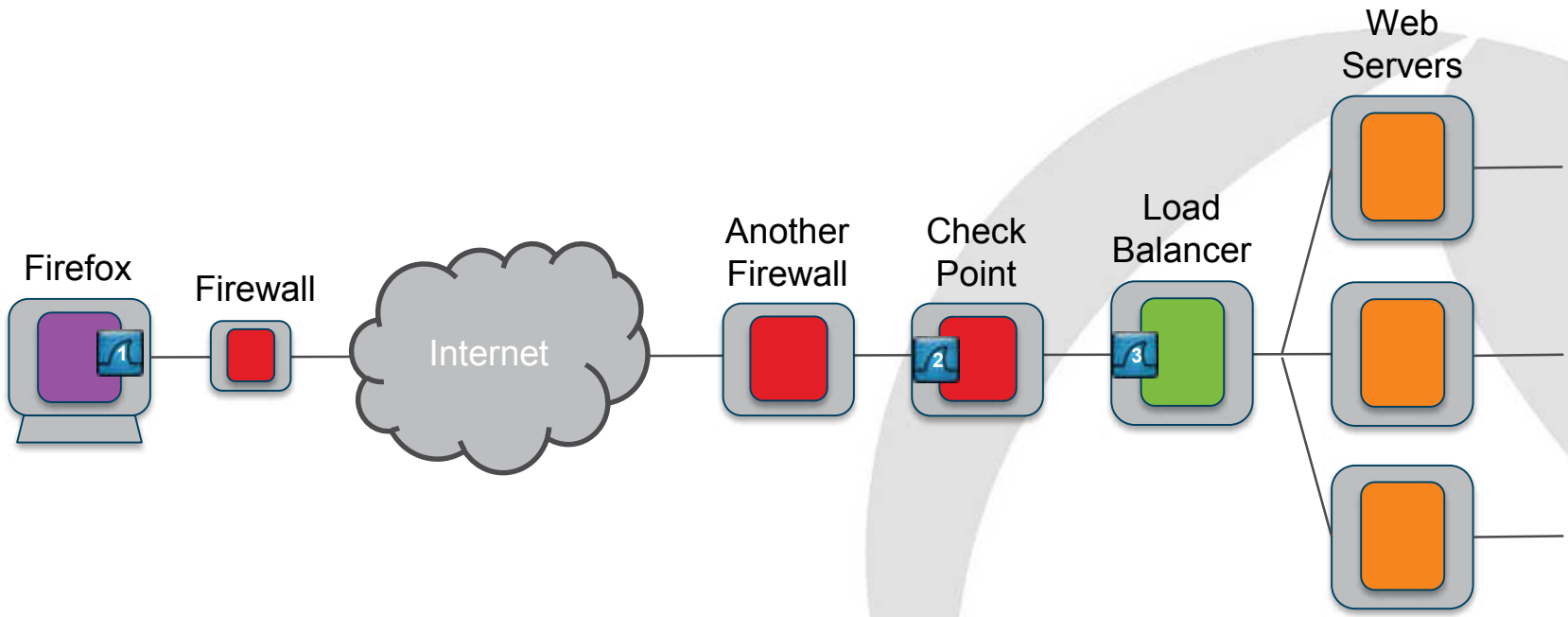
The Load Balancer - Summary

- Similar to Firewall, but worse
- Will obscure details as a TCP full proxy
- May re-segment TCP with different packet sizes
- TCP session starts are separate on client and server sides
- Always capture both sides of a load balancer
- Preferably with a common clock

Time for Questions

Airline booking system example

System topology



Packet flow summary

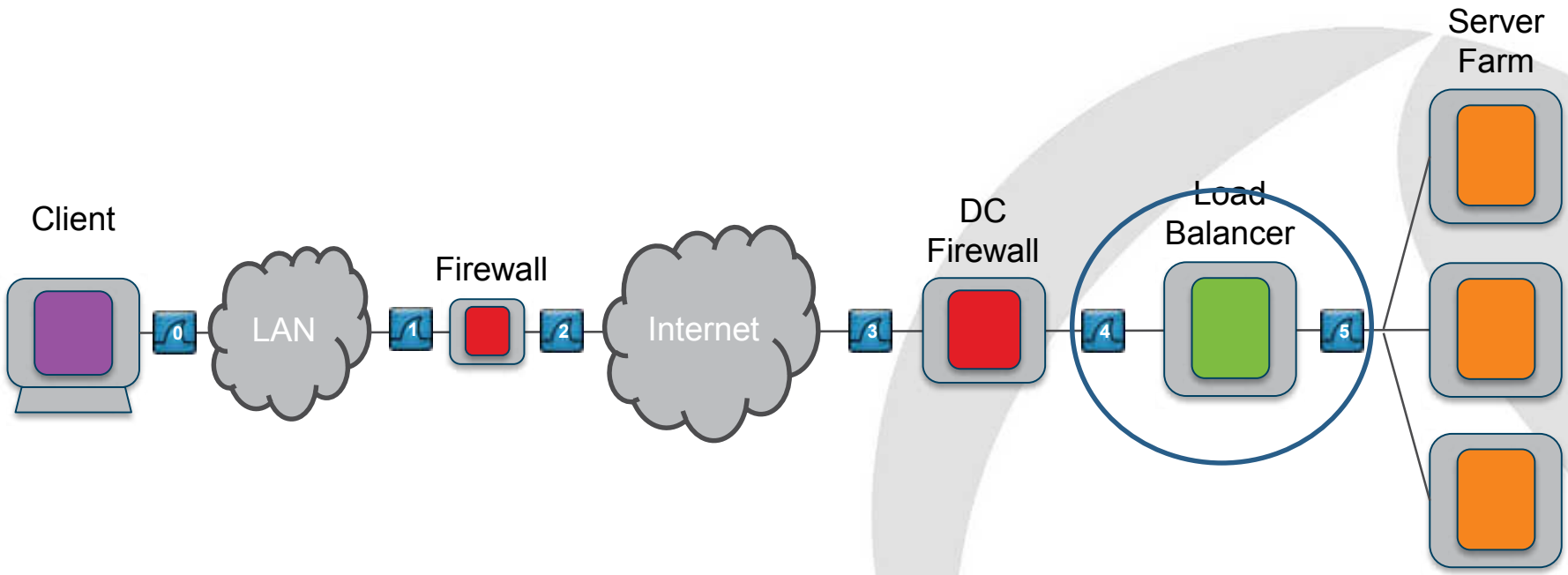
		PC			Check Point eth2			BIG-IP Ext			Delta PC to CP	Delta CP to BIG-IP
Dir	Detail	Frame	Time	Client Port	Frame	Time	Client Port	Frame	Time	Client Port		
-->	GET /book/index.asp	4256	16:00:53.424	53287	1733	16:00:11.596	13349	5509	16:02:43.713	13349	00:00:41.828	00:02:32.117
<--	200 OK - First of 20 pkt seq	4258	16:00:53.424	53287	1735	16:00:11.744	13349	5571	16:02:43.861	13349	00:00:41.680	00:02:32.117
	.											
	.											
<--	200 OK - Last of 20 pkt seq	4285	16:00:53.608	53287	1762	16:00:11.775	13349	5618	16:02:43.891	13349	00:00:41.833	00:02:32.116
-->	[ACK]	4286	16:00:53.608	53287	1763	16:00:11.779	13349	5619	16:02:43.896	13349	00:00:41.829	00:02:32.117
<--	[RST] - origin = web server				1909	16:02:23.176	13349	6980	16:04:55.284	13349		00:02:32.108
-->	POST /book/step1.asp - pt 1	5170	16:03:01.764	53287								
-->	POST /book/step1.asp - pt 2	5171	16:03:01.764	53287								
-->	POST /book/step1.asp - pt 1	5181	16:03:02.006	53287								
-->	POST /book/step1.asp - pt 1	5189	16:03:02.655	53287								
-->	POST /book/step1.asp - pt 1	5198	16:03:03.856	53287								
-->	POST /book/step1.asp - pt 1	5213	16:03:06.256	53287								
-->	POST /book/step1.asp - pt 1	5226	16:03:08.656	53287								
-->	POST /book/step1.asp - pt 1	5235	16:03:11.057	53287								
-->	POST /book/step1.asp - pt 1	5253	16:03:15.857	53287								
-->	[RST]	5350	16:03:25.449	53287								
-->	[SYN]	5351	16:03:25.452	53300	1910	16:02:43.624	14185	6981	16:05:15.732	14185	00:00:41.828	00:02:32.108
<--	[SYN, ACK]	5353	16:03:25.457	53300	1911	16:02:43.624	14185	6982	16:05:15.732	14185	00:00:41.833	00:02:32.108
-->	[ACK]	5354	16:03:25.457	53300	1912	16:02:43.628	14185	6983	16:05:15.736	14185	00:00:41.829	00:02:32.108
-->	POST /book/step1.asp - pt 1	5355	16:03:25.457	53300	1913	16:02:43.629	14185	6984	16:05:15.737	14185	00:00:41.828	00:02:32.108
-->	POST /book/step1.asp - pt 2	5356	16:03:25.457	53300	1914	16:02:43.629	14185	6985	16:05:15.737	14185	00:00:41.828	00:02:32.108
<--	[ACK]	5357	16:03:25.462	53300	1915	16:02:43.630	14185	6987	16:05:15.738	14185	00:00:41.832	00:02:32.108
<--	302 Object Moved	5358	16:03:25.476	53300	1916	16:02:43.644	14185	6994	16:05:15.752	14185	00:00:41.832	00:02:32.108

From the RPR Manual

Time for Questions

SSL
Matching on content

Across the Load Balancer



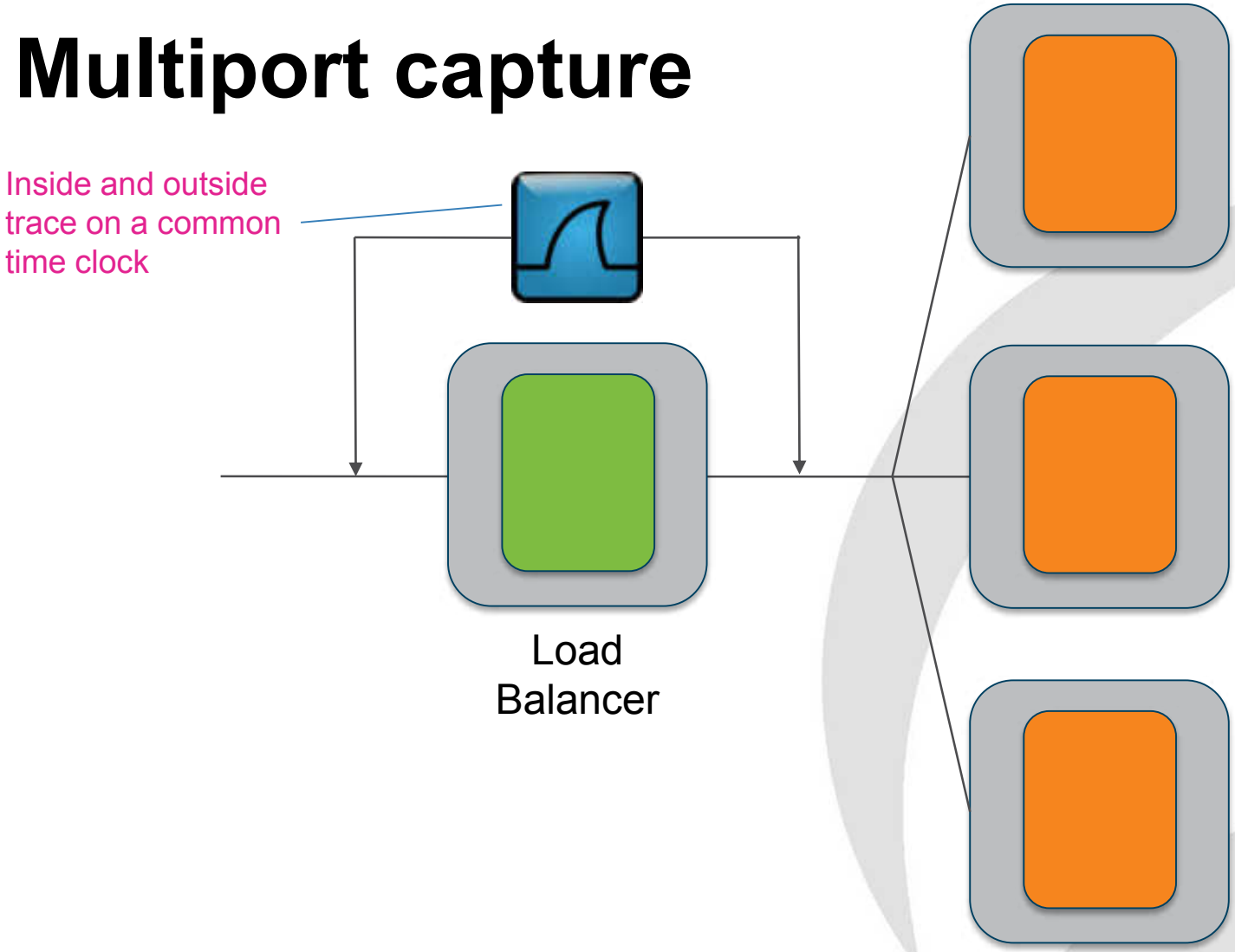
Delayed binding

No.	Time	Src Port	Dst Port	Info
1	14:04:35.370905	1514	443	1514→443 [SYN] Seq=27959
2	14:04:35.371140	443	1514	443→1514 [SYN, ACK] Seq=
4	14:04:35.372140	1514	443	Client Hello
6	14:04:35.421646	443	1514	Server Hello
7	14:04:35.421861	443	1514	[TCP segment of a reasser
8	14:04:35.421862	443	1514	Certificate
10	14:04:35.425362	1514	443	Client Key Exchange, Char
12	14:04:35.429354	443	1514	New Session Ticket, Chang
13	14:04:35.430104	1514	443	Application Data, Applic
15	14:04:35.499344	443	1514	Application Data
16	14:04:35.499829	443	1514	[TCP segment of a reasser
17	14:04:35.500072	443	1514	[TCP segment of a reasser
18	14:04:35.500073	443	1514	Application Data
20	14:04:35.500317	443	1514	[TCP segment of a reasser
21	14:04:35.500320	443	1514	[TCP segment of a reasser
22	14:04:35.500572	443	1514	Application Data
23	14:04:35.500572	443	1514	[TCP segment of a reasser
25	14:04:35.500820	443	1514	[TCP segment of a reasser
26	14:04:35.500821	443	1514	Application Data
28	14:04:35.501065	443	1514	[TCP segment of a reasser
29	14:04:35.501066	443	1514	[TCP segment of a reasser
30	14:04:35.501339	443	1514	Application Data
31	14:04:35.501341	443	1514	Application Data
36	14:04:49.055986	1514	443	Application Data, Applic
38	14:04:49.126700	443	1514	Application Data

Use RR turns to help
with alignment
Last req APDU
First rsp APDU

No.	Time	Sr[illegible]t	Dst Port	Info
1	14:04:35.430353	[illegible]916	443	34916→443 [SYN] Seq=35268281
2	14:04:35.430611	443	34916	443→34916 [SYN, ACK] Seq=395
4	14:04:35.430613	34916	443	Client Hello
6	14:04:35.480348	443	34916	Server Hello
7	14:04:35.480578	443	34916	[TCP segment of a reassemble
8	14:04:35.480843	443	34916	Certificate
12	14:04:35.488572	34916	443	Client Key Exchange, Change
14	14:04:35.492568	443	34916	Change Cipher Spec, Encrypte
15	14:04:35.492814	34916	443	Application Data
16	14:04:35.496844	443	34916	Application Data, Applicatio
17	14:04:35.497065	443	34916	[TCP segment of a reassemble
18	14:04:35.497323	443	34916	[TCP segment of a reassemble
19	14:04:35.497571	443	34916	[TCP segment of a reassemble
20	14:04:35.497829	443	34916	[TCP segment of a reassemble
23	14:04:35.498068	443	34916	Application Data
24	14:04:35.498366	443	34916	[TCP segment of a reassemble
25	14:04:35.498570	443	34916	[TCP segment of a reassemble
26	14:04:35.498815	443	34916	[TCP segment of a reassemble
27	14:04:35.499069	443	34916	[TCP segment of a reassemble
31	14:04:35.499573	443	34916	[TCP segment of a reassemble
32	14:04:35.499824	443	34916	Application Data
33	14:04:35.499827	443	34916	Application Data
36	14:04:49.056232	34916	443	Encrypted Alert

Multiport capture



Mobile phone app example

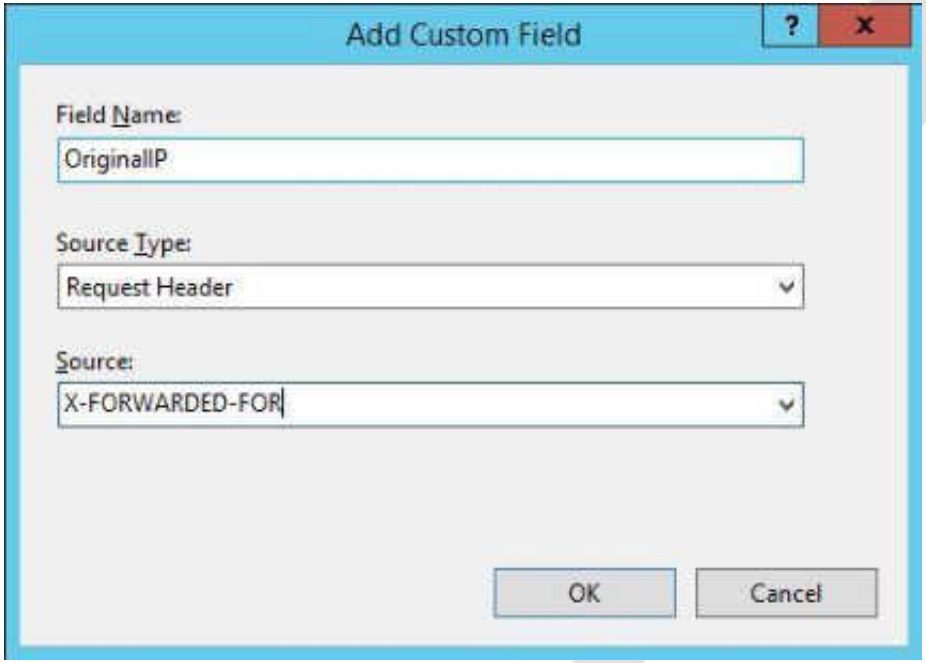
Web server response times

```
192.168.1.87 - - [09/Jul/2012:08:25:29 +0100] 379 "GET / HTTP/1.1" 401 479 "-
" "Mozilla/5.0 (Windows NT 6.1; rv:13.0) Gecko/20100101 Firefox/13.0.1"
```

```
192.168.1.87 – user01 [09/Jul/2012:08:25:35 +0100] 24313 "GET / HTTP/1.1" 302
242 "-" "Mozilla/5.0 (Windows NT 6.1; rv:13.0) Gecko/20100101 Firefox/13.0.1"
```

```
192.168.1.87 – user01 [09/Jul/2012:08:25:35 +0100] 542911 "GET /Setup.php
HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; rv:13.0) Gecko/20100101
Firefox/13.0.1"
```

IIS Advanced Logging



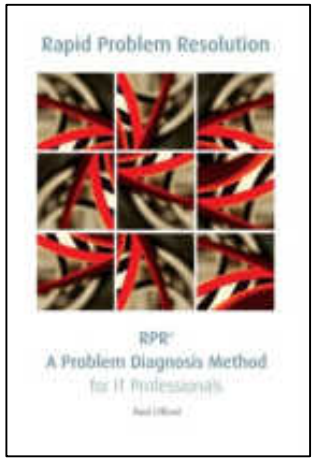
Load Balancer (SSL) - Summary

- Not much to go on in the capture file:
  - Packet sizes (approx.)
  - Temporal relationships
- Use turns to align
  - Last packet of APDU Request
  - First packet of APDU Response
- Use web logs to help
- Very difficult without time sync

Overall Summary

- 5-tuple and TCP Seq will get you a long way
- Use application-related ID for UDP
- Overcome SSL with:
  - Match on content
  - Temporal relationships
  - Packet lengths (even if approx.)
- Time sync'd traces help a lot
- Visualise in spreadsheet

Further information



Amazon
or free
eBook

tribelab

Tech community at
TribeLabZero.com

Paul Offord
Mobile: +44 (0) 1279 211 668
Email: paul.offord@advance7.com
Web: www.advance7.com