

DMZ Network Visibility with Wireshark

June 15, 2010


Ashok Desai

Senior Network Specialist | Intel Information Technology

SHARKFEST '10

Stanford University

June 14-17, 2010



SHARKFEST '10

Outline

Presentation Objective

DMZ Overview / Challenges

Case Study

Summary



Presentation Objective

- Share challenges faced when DMZ network visibility is needed
- Share methods to help overcome these challenges
- Share Wireshark capabilities that are useful for analyzing DMZ traffic

DMZ Overview

- DMZ (Demilitarized Zone) Network
 - “a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network”*
 - “a network, not part of Internet or Intranet”*
- Typical DMZ Services
 - Firewall
 - Load Balancer
 - Reverse Proxy

Firewall

- Firewall
 - Designed to block unauthorized access while permitting authorized communications
- Types:
 1. Network layer firewall
 2. Application layer firewall



Firewall Types

- Network layer firewall
 - Will not allow packets to pass through the firewall unless they match the established rule set
 - Includes source and destination IP address, UDP or TCP ports
- Application layer firewall
 - Application firewalls can prevent all unwanted outside traffic from reaching protected machines
 - Work at the application layer of the TCP/IP stack (i.e., all browser traffic, or all telnet or ftp traffic)
- Can be single appliance or separate appliances

Firewall Functionality

- Network and Port Address Translation
 - Hides the true address of protected hosts
- Load Balancer
 - Provides redundancy & load balancing requests
- Challenges for Protocol Analysis
 - Tracking the user task's level traffic
 - Source IP and TCP port number can change when they pass through

Load Balancer

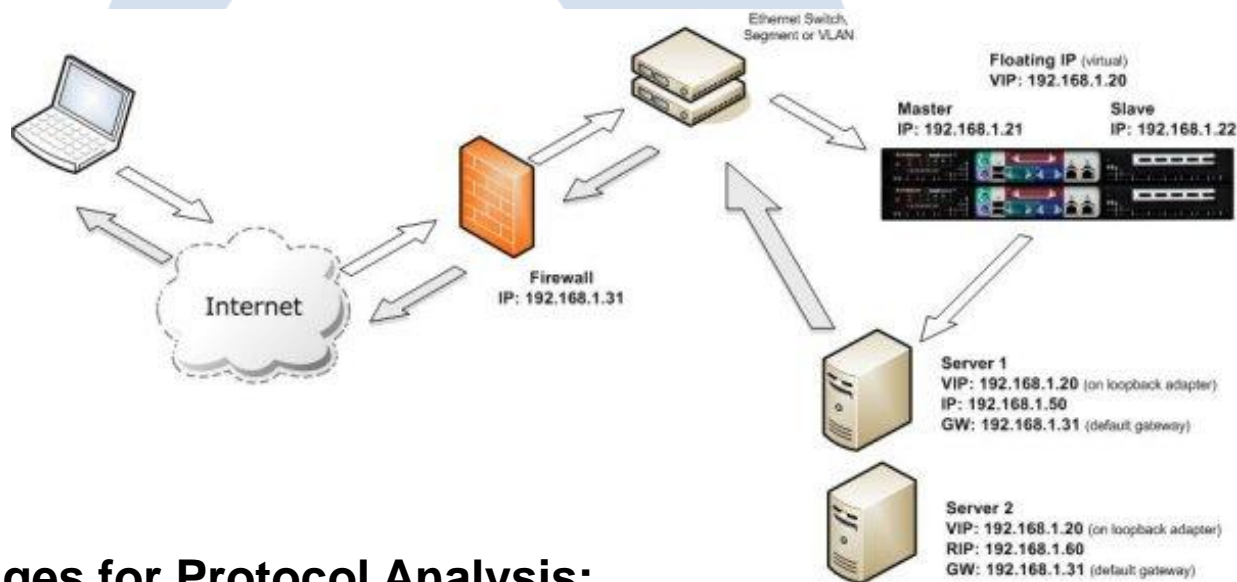
- Load Balancer
 - A technique to distribute workload evenly across two or more computers, network links, CPUs, hard drives, or other resources
 - Can be software or appliance based
- Types of Load Balancers*
 1. Direct Routing (DR)
 2. Network Address Translation (NAT)
 3. Source Network Address Translation (SNAT)
 4. Transparent Source Network Address Translation (SNAT-TPROXY)
 5. SSL Termination or Acceleration (SSL) with or without TPROXY

*- Source <http://loadbalancer.org>

Load Balancer: Type 1

- **Direct Routing (DR) load balancing method**

- The virtual IP address is shared by real servers and the load balancer
- Load balancer selects on real server, directly forwards to real server
- Real server process the request locally and sends response packet directly to client



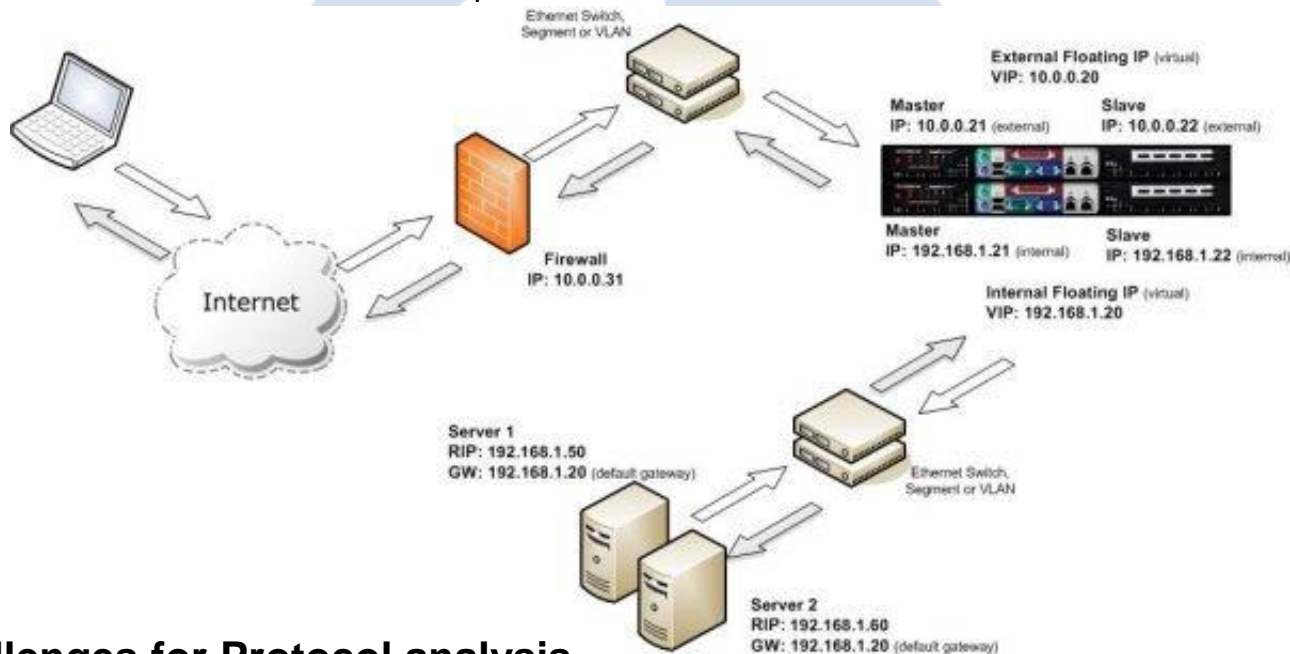
- **Challenges for Protocol Analysis:**

- There could be duplicate packets seen in real server LAN network

Load Balancer: Type 2

- **Network Address Translation (NAT) load balancing method**

- A two arm infrastructure with an internal and external subnet to carry out the translation
- Appliance becomes the default gateway for the real servers
- Load balancer translates all requests from the external virtual server to the internal real servers.

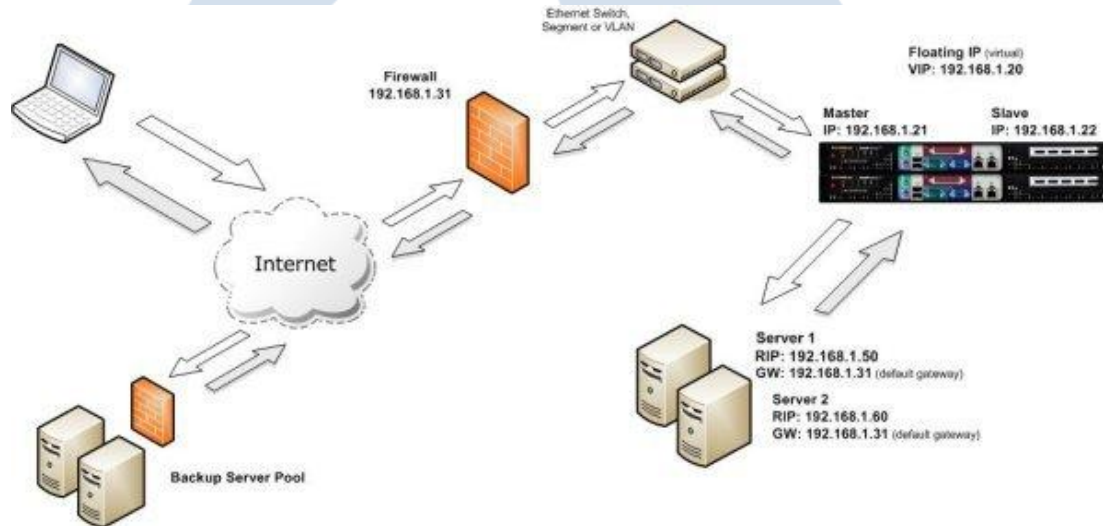


- **Challenges for Protocol analysis**

- Tracking the user task's level traffic
- Source IP and TCP port number will change when they pass through

Load Balancer: Type 3

- **Source Network Address Translation (SNAT) load balancing method**
 - The load balancer proxies the application traffic to the servers so that the source of all traffic becomes the load balancer
 - Load balancer handles cookie insertion

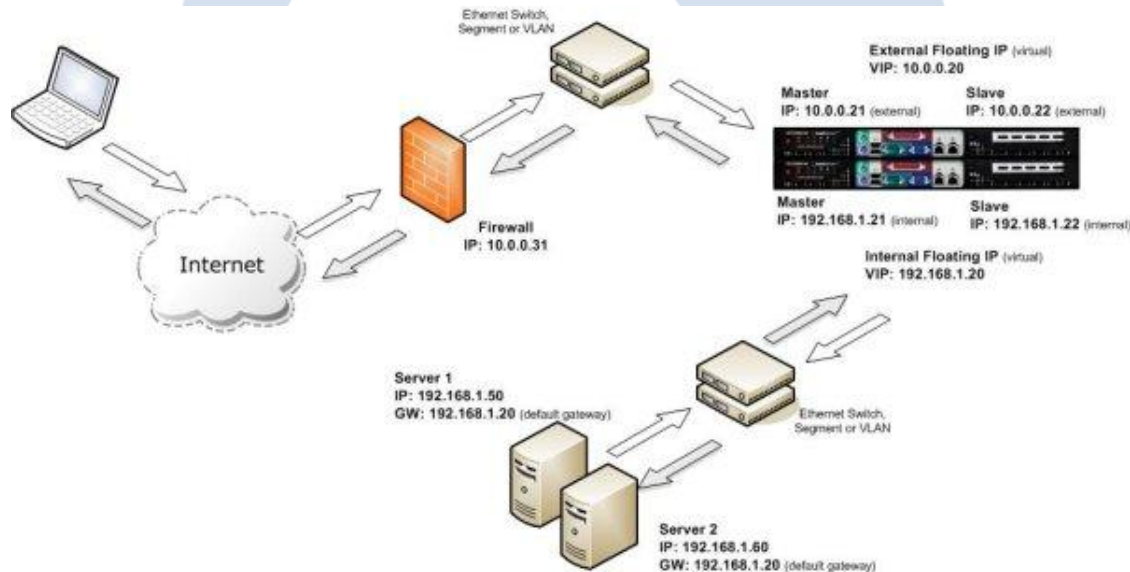


- **Challenges for Protocol Analysis:**

- Tracking the user task's level traffic as Source IP and TCP port number will change when they pass through the load balancer

Load Balancer: Type 4

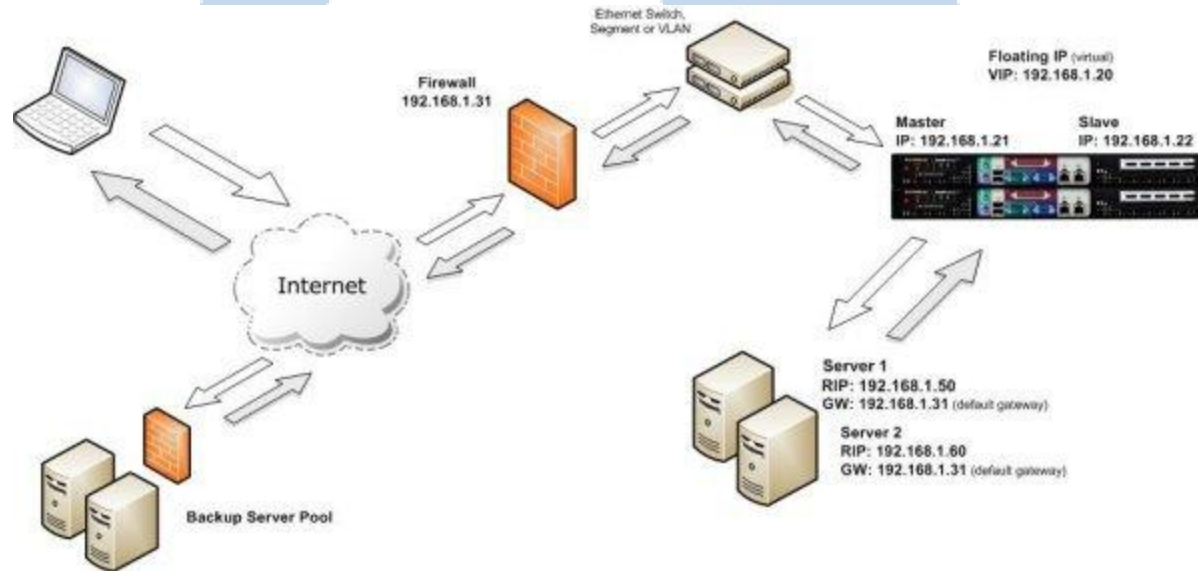
- **Transparent Source Network Address Translation (SNAT-TPROXY) load balancing method**
 - Source address of the client is a requirement
 - SNAT acts as a full proxy but in TPROXY mode all server traffic must pass through the load balancer
 - The real servers must have their default gateway configured to point at the load balancer



- **Challenges for Protocol Analysis:**
 - Not as many challenges as other types

Load Balancer: Type 5

- **SSL Termination or Acceleration (SSL) with or without TPROXY**
 - To process cookie persistence in HTTPS streams on the load balancer
 - Can be configured to see Source IP or Source IP as load balancer IP

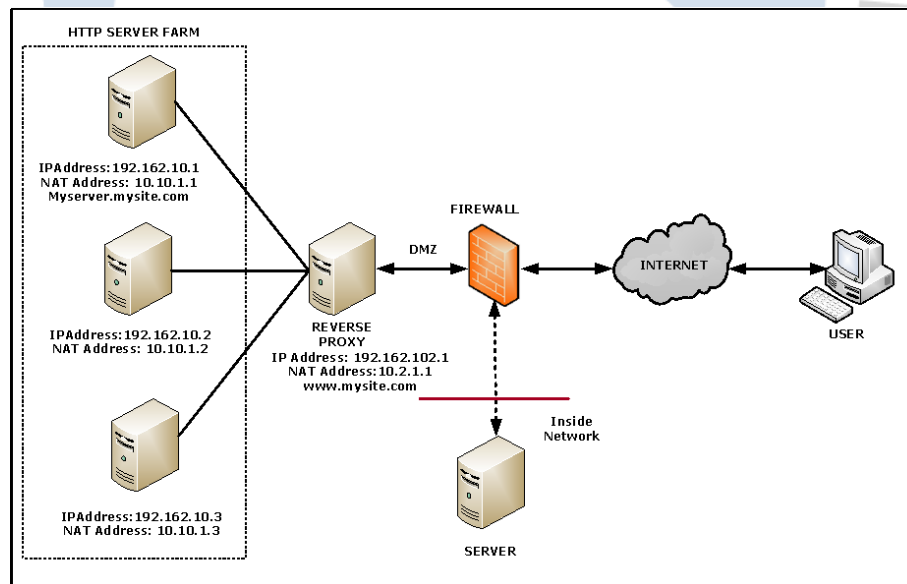


- **Challenges for Protocol Analysis:**

- Tracking the user task's level traffic as Source IP and TCP port number will change when they pass through the load balancer

Reverse Proxy

- Reverse Proxy
 - Acts as a gateway to an HTTP server or HTTP server farm by acting as the final IP address for requests from the outside
 - Dispatches in-bound network traffic to a set of servers, presenting a single interface to the caller
 - Uses NAT or PAT to accomplish this



Reverse Proxy

- Challenges for Protocol Analysis
 - Tracking the user task's traffic across DMZ appliances
 - IP Address and port number will change once it passes through the reverse proxy
 - URL may be different at each DMZ appliance

DMZ Network Challenges – Summary

- DMZ network analysis can be challenging:
 - Encrypted traffic
 - Changing IP addresses and port numbers across:
 - Load Balancer
 - Reverse Proxy
 - Firewall
 - Traffic can be difficult to correlate across tiers

HTTP Protocol Overview

- Compliments protocol analysis efforts
 - HTTP is a request-response standard typical of client-server computing
 - Provides response when there is successful or unsuccessful event
 - Helps to guide where could be cause of issue

Outline

Presentation Objective

DMZ Overview / Challenges

Case Study

Problem Statement

Methodology

Testing Details

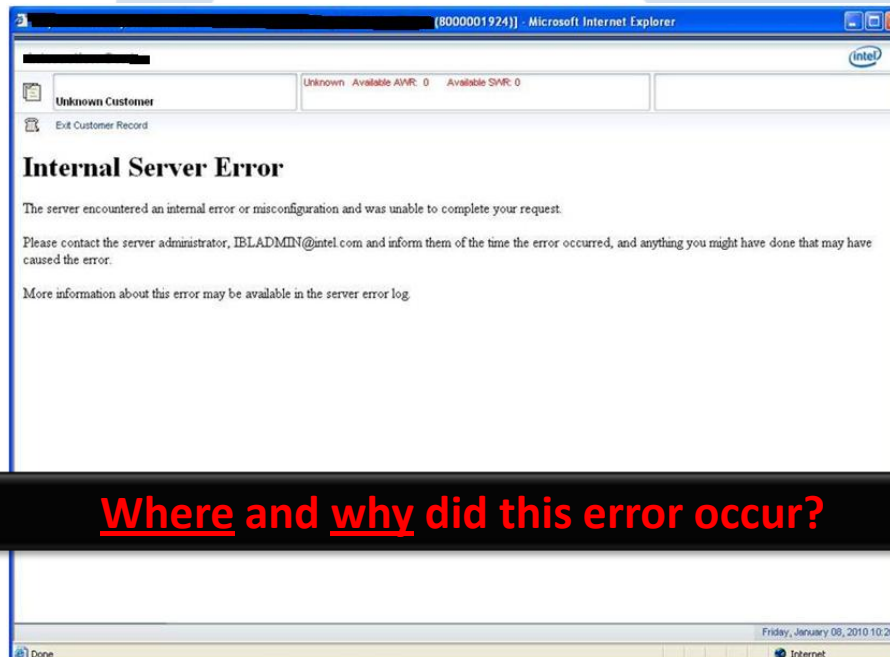
Analysis & Inferences

Summary

SHARKFEST '10

Problem Statement

- Users were intermittently receiving an **“Internal Server Error”** when accessing an external facing website

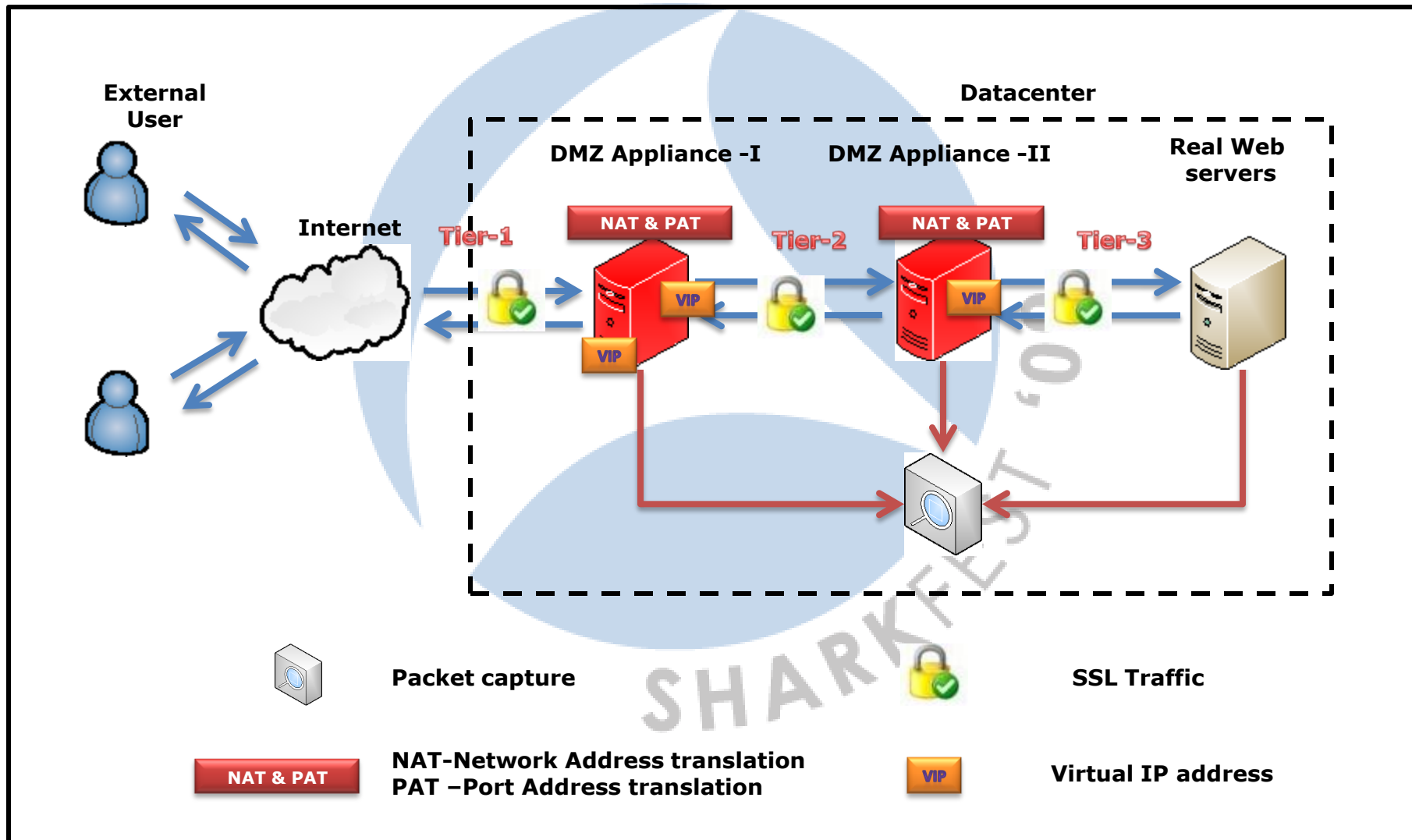


Where and why did this error occur?

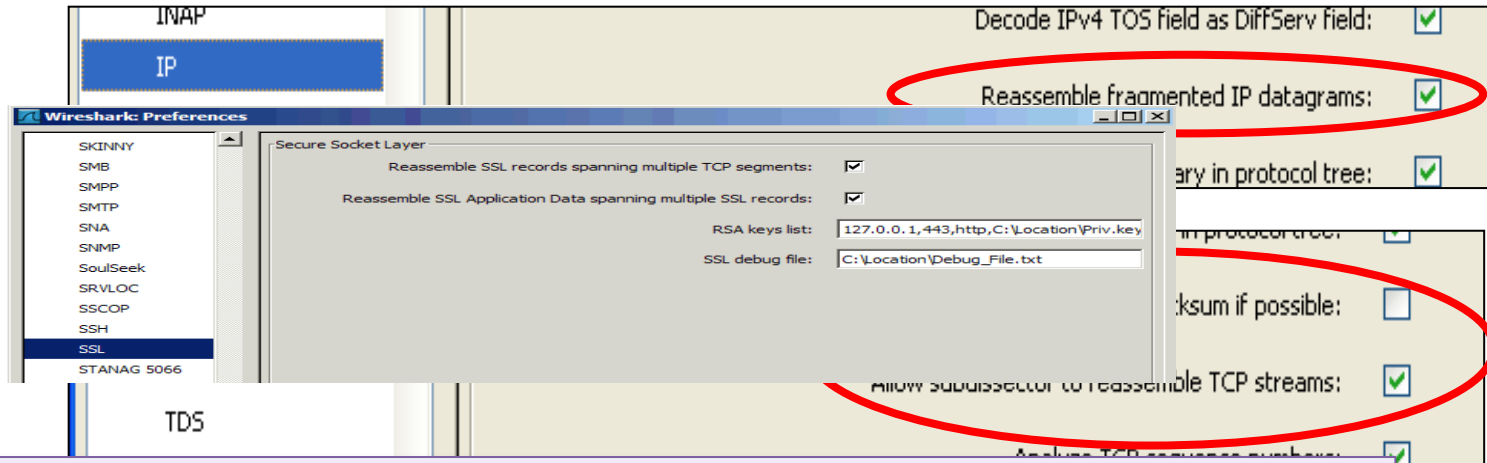
Methodology

- Understand the application flow through the DMZ infrastructure
- Capture interesting traffic
- Filter based on the time of the error event
- Decrypt the traffic to provide visibility
- Analyze the traffic
- Correlate the findings to identify the root cause

Understand the Flow - Capture the Interesting Traffic



Decrypt the Traffic



Where:

IP: is the IP Address of the server / appliance with the private key

Port: is usually 443 for SSL/TLS or destination port seen in the trace file

Protocol :is usually HTTP

Key File_Name: is the location and file name of the private key

- For more info please refer "[SSL Troubleshooting with Wireshark and Tshark](#)" By Sake Blok in SHARKFEST '09

DMZ Tier-1 Observations

(8000001924) - Microsoft Internet Explorer

Unknown Customer Unknown Available AWR: 0 Available SMR: 0

Exit Customer Record

Internal Server Error

→ ERROR OBSERVED @ USER

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, IBLADMIN@intel.com and inform them of the time the error occurred, and anything you might have done that may have caused the error.

More information about this error may be available in the server error log.

Friday, January 08, 2010 10:26

Done Internet

REFERENCE IN WEB PAGE

TIME @ EVENT OCCURRED

DMZ Tier-1 Observations Cont..

Filter with response code "500"

No.	Time	delta	window Size	length	IP TTL	Source	Destination	Protocol	Info
134593	2010-01-08 10:26:18.782757394	0.000	32768	60	255 19			TCP	https > dts [ACK] Seq=28106 Ack=30010 win=32768 Len=0
134594	2010-01-08 10:26:18.796005215	0.013	32768	60	255 19			TCP	https > 64213 [ACK] Seq=14625 Ack=95568 win=32768 Len=0
134595	2010-01-08 10:26:18.812681415	0.016	64775	608	115 10			HTTP	GET /sap(====)/bc/bsp/sap/crmcmp_ic_frame/crmcmp_.../sap(====)/bc/bsp/sap/crmcmp_ic_frame/crmcmp_...
134596	2010-01-08 10:26:18.815047694	0.002	10625	1298	255 19			HTTP	HTTP/1.1 200 OK (application/javascript)
134597	2010-01-08 10:26:18.826490474	0.011	32768	841	255 19			HTTP	HTTP/1.1 500 Internal Server Error (text/html)
134598	2010-01-08 10:26:18.837920415	0.011	65535	1078	115 10			TCP	[TCP segment of a reassembled PDU]
134599	2010-01-08 10:26:18.844113014	0.006	65535	1456	115 10			TCP	[TCP segment of a reassembled PDU]

Time of Event occurred matches with error observed @ user Browser

Error Content matches with error observed @ user Browser

```
Request Version: HTTP/1.1
Response Code: 500
Date: Fri, 08 Jan 2010 04:56:19 GMT\r\n
Content-Length: 538\r\n
Content-Type: text/html; charset=iso-8859-1\r\n
Set-Cookie: TS97404c=6ff183e7d15e8925d5bd413d8a16ec605e109bef877dcff74b46baf3; Path=/\r\n\r\n
Line-based text data: text/html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n
<html><head>\n
<title>500 Internal Server Error</title>\n
</head><body>\n
<h1>Internal Server Error</h1>\n
<p>The server encountered an internal error or\n
misconfiguration and was unable to complete\n
your request.</p>\n
<p>Please contact the server administrator,\n
IBLADMIN@intel.com and inform them of the time the error occurred,\n
and anything you might have done that may have\n
caused the error.</p>\n
<p>More information about this error may be available\n
in the server error log.</p>\n
```

0000 48 54 54 50 2f 31 2e 31 20 85 30 30 20 49 6e 74 HTTP/1.1 500 Int
0010 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 ernal Se rver Err
0020 6f 72 0d 0a 44 61 74 65 3a 20 46 72 69 2c 20 30 or..Date : Fri, 0
0030 38 30 43 61 6e 30 33 30 31 30 30 30 34 33 35 36 8 30 30 30 04:56

Frame (841 bytes) Decrypted SSL data (766 bytes)

HTTP Response Code (http.response.code), 3 b... Packets: 153339 Displayed: 153339 Marked: 0 Profile: Default

DMZ Tier-1 Observations Cont..

The image shows a Wireshark capture of network traffic. The top pane displays a list of packets with columns for No., Time, delta, window Size, length, IPTTL, Source, Destination, Protocol, and Info. A specific packet (No. 134778) is highlighted with a yellow background and an arrow pointing to it. A text box with the text "Time of Event occurred matches with error observed @ user Browser" has an arrow pointing to the Time column of this packet.

The bottom pane shows the raw data of the selected packet, which is a reassembled TCP segment. A red circle highlights a portion of the data: `7Bt1cke tno%3A%5 B8000001 924%5D%7 d%3C%2Ft d%3E%3C% 2Ftr%3E% 3C%2Ftd% 3E%3C%2F tr%3E%3C %2Ftbody %3E%3C%2`. An arrow points from this highlighted text to a text box on the right that reads "Content matches with web page content observed @ user Browser".

No.	Time	delta	window Size	length	IPTTL	Source	Destination	Protocol	Info
134586	2010-01-08 10:26:18.702516835	0.000	64433	107	115	10...	115 10...	HTTP	POST /sap/bd11b1z1PTUXMCzkPw1pb1z2ZPTCImmUwMCzPTEr
134587	2010-01-08 10:26:18.702531675	0.000	32768	60	255	192...	192.168.1.255	HTTP	https > qadmifevent [ACK] Seq=39696 Ack=254108 win=...
134597	2010-01-08 10:26:18.826490474	0.011	32768	841	255	192...	192.168.1.255	HTTP	HTTP/1.1 500 Internal Server Error (text/html)
134636	2010-01-08 10:26:19.167611514	0.024	65535	60	115	10...	115 10...	HTTP	qadmifevent > https [ACK] Seq=254108 Ack=40483 win=...
134776	2010-01-08 10:26:20.263198014	0.004	65535	1078	115	10...	115 10...	TCP	[TCP segment of a reassembled PDU]
134777	2010-01-08 10:26:20.269427154	0.006	65535	1456	115	10...	115 10...	TCP	[TCP segment of a reassembled PDU]
134778	2010-01-08 10:26:20.269428255	0.000	65535	112	115	10...	115 10...	TCP	[TCP segment of a reassembled PDU]

Time of Event occurred matches with error observed @ user Browser

Content matches with web page content observed @ user Browser

DMZ Tier-1 Observations Cont..

Filter with "session ID" & "Post" request

At Tier-1 there are Six (6) Post request Observed

No. -	Time	delta	window Size	length	IP TTL	Source	Destination	Protocol	Info
130394	2010-01-08 10:25:47.146411355	0.003	65535	718				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH
132310	2010-01-08 10:26:02.306467975	0.002	65140	510				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH
133377	2010-01-08 10:26:10.818874075	0.003	65535	114				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH
134586	2010-01-08 10:26:18.702516835	0.000	64433	107				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH
137557	2010-01-08 10:26:49.485228614	0.001	64350	488				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH
137745	2010-01-08 10:26:52.095378075	0.001	65140	488				HTTP	POST /sap(bd11bfzjPTUxMCZkPwLpb1z2PTc1MmUwMCZpPTeH

```
0000 00 01 d7 98 72 c2 00 03 31 79 87 fc 08 00 45 00  ....r... 1y...E.
0010 00 5d 4e 46 40 00 73 06 c9 25 0a f2 80 41 c0 c6  .]NF@s. %.A..
0020 a4 35 09 9e 01 bb 5d 9b 9f ff 95 f6 5c 47 50 18  .5....]. ...GP.
0030 fb b1 40 ac 00 00 12 ce 7c 0b 26 73 68 73 68 1e  .@..... |.&shsh.
0040 6a b6 e8 94 a9 a8 8c c7 43 f6 f1 64 11 d3 18 6e  j..... C..d...n
0050 ff 69 fc bd 6c 0b 59 5d 06 4d 78 03 44 64 71 73  .i..l.Y] .Mx.Ddqs
0060 06 b6 ca d9 1d 24 24 43 f4 f1 1b                .....$$C ...
```

Frame (107 bytes) | Reassembled TCP (2574 bytes) | Decrypted SSL data (2553 bytes) | Reassembled SSL (79900 bytes)

File: "C:\Documents and Settings\adesai\Desko... | Packets: 153339 Displayed: 6 Marked: 0 | Profile: Default

Signature Identified

- Signature identified from Tier-1 to track to next level of DMZ Appliances
 - Time of event occurred : **10:26:18:8264 AM**
 - Cookie info – session ID:
ID0767292151DB00270059887862992407End
 - Number of Post request in interesting SSL stream: **6**
 - Content info in web page : “**800001924**”

DMZ Tier-2 Observations

The image shows a Wireshark capture of an HTTP 500 Internal Server Error response. The main pane displays a list of packets, with packet 585 highlighted in green. A red text box with an arrow pointing to packet 585 contains the text "Filter with response code '500'". The packet list shows the following details for packet 585:

No.	Time	Source	Destination	Protocol	Info
583	2010-01-08 10:26:18.722493	10.26.18.722493	10.26.18.722493	TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2450
584	2010-01-08 10:26:18.722721	10.26.18.722721	10.26.18.722721	TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2480
585	2010-01-08 10:26:18.821915	10.26.18.821915	10.26.18.821915	HTTP	POST /sap(bd11bz1jPTUXMCZkPw1pb1z2PTc1MmuwMCZpPTEmcz) [200 OK]
586	2010-01-08 10:26:18.822078	10.26.18.822078	10.26.18.822078	TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2506
587	2010-01-08 10:26:18.822399	10.26.18.822399	10.26.18.822399	HTTP	HTTP/1.1 500 Internal Server Error (text/html)
588	2010-01-08 10:26:18.822457	10.26.18.822457	10.26.18.822457	TCP	qadmifevent > etlservicemgr [ACK] Seq=250681 Ack=2836

A yellow text box with an arrow pointing to the time field of packet 585 contains the text "10:26:18.8219" Time of Event occurred matches with error observed @ user Browser".

The packet details pane for packet 587 shows the following information:

- Request Version: HTTP/1.1
- Response Code: 500
- Date: Fri, 08 Jan 2010 04:56:19 GMT\r\n
- Content-Length: 538\r\n
- Content-Type: text/html; charset=iso-8859-1\r\n
- Line-based text data: text/html

The text data pane shows the following HTML content:

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n<title>500 Internal Server Error</title>\n</head><body>\n<h1>Internal Server Error</h1>\n<p>The server encountered an internal error or\nmisconfiguration and was unable to complete\nyour request.</p>\n<p>Please contact the server administrator,\nIBLADMIN@intel.com and inform them of the time the error occurred,\nand anything you might have done that may have\ncaused the error.</p>\n<p>More information about this error may be available\nin the server error log.</p>\n</body></html>\n
```

A yellow text box with an arrow pointing to the HTML content contains the text "Error Content matches with error observed @ user Browser as well as tier -1 appliance also".

The packet bytes pane shows the following hex dump:

```
0000 48 54 54 50 2f 31 2e 31 20 85 30 30 20 49 6e 74  HTTP/1.1 500 Int
0010 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72  ernal server Err
0020 6f 72 0d 0a 44 61 74 65 3a 20 46 72 69 2c 20 30  0..Date : Fri, 0
0030 28 28 43 61 6e 28 22 20 21 28 28 28 24 23 28 26
```

DMZ Tier-2 Observations, Cont..

WAF_RP_1026_internal server error.cap - Wireshark

Filter: Expression... Clear Apply

No.	Time	delta	window Size	length	IP TTL	Source	Destination	Protocol	Info
583	2010-01-08 10:26:18.722493	0.000	65535	60				TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2450
584	2010-01-08 10:26:18.722721	0.000	65535	60				TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2480
585	2010-01-08 10:26:18.821915	0.099	32768	1271				HTTP	POST /sap/bb1/bjZjPTUXMCZkPwLpbjZ2PTC/ImmUwMCZpPTEmcz
586	2010-01-08 10:26:18.822078	0.000	65535	60				TCP	etlservicemgr > qadmifevent [ACK] Seq=282921 Ack=2500
587	2010-01-08 10:26:18.822399	0.000	65535	775				HTTP	HTTP/1.1 500 Internal Server Error (text/html)
588	2010-01-08 10:26:18.822457	0.000	32768	60				TCP	qadmifevent > etlservicemgr [ACK] Seq=250681 Ack=2830

04b90 65 25 32 30 65 6e 63 6f 75 72 61 67 65 25 32 30 e
04ba0 79 6f 75 25 32 30 74 6f 25 32 30 75 73 65 25 32 y
04bb0 30 25 33 43 61 25 32 30 6f 6e 63 6c 69 63 6b 25 c
04bc0 33 44 25 32 32 72 65 74 75 72 6e 25 32 30 74 6f 3
04bd0 70 2e 6a 73 2e 4f 70 65 6e 45 78 74 4c 69 6e 6b p
04be0 28 77 69 6e 64 6f 77 25 32 43 65 76 65 6e 74 25 (
04bf0 32 43 74 68 69 73 29 25 32 32 25 32 30 68 72 65 2
04c00 66 25 33 44 25 32 32 6d 61 69 6c 74 6f 25 33 41 f
04c10 73 61 73 75 70 70 6f 72 74 25 34 30 6d 61 69 6c s
04c20 62 6f 78 2e 69 6e 74 65 6c 2e 63 6f 6d 25 32 32 b
04c30 25 32 30 74 61 72 67 65 74 25 33 44 25 32 32 5f %
04c40 62 6c 61 6e 6b 25 32 32 25 33 45 73 61 73 75 70 b
04c50 70 6f 72 74 25 34 30 6d 61 69 6c 62 6f 78 2e 69 p
04c60 6e 74 65 6c 2e 63 6f 6d 25 33 43 25 32 46 61 25 r
04c70 33 45 2e 25 32 30 25 30 44 25 30 41 33 2e 25 32 3
04c80 30 57 68 65 6e 25 32 30 72 65 70 6c 79 69 6e 67 0
04c90 25 32 30 74 6f 25 32 30 6f 75 72 25 32 30 45 6d %
04ca0 61 69 6c 73 25 32 30 70 6c 65 61 73 65 25 32 30 a
04cb0 63 6c 69 63 6b 25 32 30 52 45 50 4c 59 25 32 30 c
04cc0 6f 6e 6c 79 25 32 30 61 6e 64 25 32 30 44 4f 25 c
04cd0 32 30 4e 4f 54 25 32 30 63 72 65 61 74 65 25 32 2
04ce0 30 61 25 32 30 6e 65 77 25 32 30 65 6d 61 69 6c 0
04cf0 2e 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a .
04d00 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a *
04d10 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a *
04d20 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a *
04d30 72 76 69 63 65 25 32 30 74 69 63 6b 65 74 25 33 s
04d40 41 25 32 30 38 30 30 30 30 30 31 39 32 34 25 43 A
04d50 32 25 41 30 50 72 6f 64 75 63 74 25 33 41 25 32 2%
04d60 30 44 47 34 35 49 44 25 32 30 25 33 43 25 32 46 0%
04d70 73 70 61 6e 25 33 45 4d 61 72 6b 69 6e 67 73 25 s
04d80 33 41 25 32 30 25 33 43 73 70 61 6e 25 32 30 73 3
04d90 74 79 6c 65 25 33 44 25 32 32 46 4f 4e 54 2d 53 t
04da0 49 5a 45 25 33 41 25 32 30 31 32 70 74 25 33 42 I
04db0 25 32 30 46 4f 4e 54 2d 46 41 4d 49 4c 59 25 33 %
04dc0 41 25 32 30 25 32 36 25 32 33 33 39 25 33 42 54 A
04dd0 69 6d 65 73 25 32 30 4e 65 77 25 32 30 52 6f 6d i

Content matches with web page content observed @ user Browser as well as @ tier-1 appliance

DMZ Tier-2 Observations, Cont..

The image shows a Wireshark capture of a WAF error page. The filter bar is set to "http contains ID0767292151D800270059887862992407End && http.requ". A red arrow points to the filter bar with the text "Filter with 'session ID' & 'Post' request". Below the filter bar, a table of captured packets is shown. A blue arrow points from the table to a text box that says "At Tier-2 there are Six (6) Post request Observed".

No.	Time	delta	window Size	length	IP TTL	Source	Destination	Protocol	Info
16	2010-01-08 10:25:47.159465	0.000	5977	969				HTTP	POST /sap(bd1 biz PTUXMCzkPW1pbiz2PTc MmUwMCzpPTEmcz]
300	2010-01-08 10:26:02.424837	0.098	32768	1338				HTTP	POST /sap(bd1 biz PTUXMCzkPW1pbiz2PTc MmUwMCzpPTEmcz]
443	2010-01-08 10:26:10.937971	0.099	32768	1336				HTTP	POST /sap(bd1 biz PTUXMCzkPW1pbiz2PTc MmUwMCzpPTEmcz]
585	2010-01-08 10:26:18.821915	0.099	32768	1271				HTTP	POST /sap(bd1 biz PTUXMCzkPW1pbiz2PTc MmUwMCzpPTEmcz]
634	2010-01-08 10:26:49.489705	0.001	32768	1422				SSL	[SSL segment of a reassembled PDU]
646	2010-01-08 10:26:52.099405	0.001	32768	1422				SSL	[SSL segment of a reassembled PDU]

At Tier-2 there are Six (6) Post request Observed

Frame 1271 (1271 bytes) on interface (eth0): Reassembled TCP (13350 bytes) → Decrypted SSL data (13329 bytes) → Reassembled SSL (79868 bytes)

DMZ Tier-3 Observations

The image shows a screenshot of the Wireshark network protocol analyzer. The title bar reads "10_26_error_between_RP_WD_correctone.cap - Wireshark". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, navigation, and analysis. The filter bar at the top contains the text "Filter: http.response.code == 500" with a red arrow pointing to it. To the right of the filter bar, the text "Filter with response code of '500'" is displayed in red. Below the filter bar is a table with columns: No., Time, delta, window Size, length, IPTTL, Source, Destination, Protocol, and Info. The table is currently empty. A black arrow points from the left side of the table area to a grey box containing the text "At Tier-3 server '500' Error is missing". The status bar at the bottom shows "File: 'C:\Documents and Settings\adesal\Desкто...", "Packets: 653 Displayed: 0 Marked: 0", and "Profile: Default".

Filter: `http.response.code == 500`

Filter with response code of "500"

At Tier-3 server "500" Error is missing

File: "C:\Documents and Settings\adesal\Desкто... | Packets: 653 Displayed: 0 Marked: 0 | Profile: Default

DMZ Tier-3 Observations, Cont..

The image shows a Wireshark capture of network traffic. The filter is set to `292151DB00270059887862992407End &&.http.request.method == "POST"`. The packet list shows five POST requests from source IP 10.18.15.10 to destination IP 10.1.185.120. A text box with an arrow pointing to the first packet states: "At Tier-3 there are only Five(5) Post request Observed". A larger blue text box at the bottom states: "Didn't observe one post request for which earlier tiers had the 'Internal server Error'". The packet details pane shows the structure of the first packet: Internet Protocol, Reassembled TCP, and Decrypted SSL data.

Filter with "session ID" & "Post" request

No.	Time	delta	window Size	length	IP TTL	Source	Destination	Protocol	Info
20	2010-01-08 10:25:47.182885	0.000	64655	719	128	10.18.15.10	10.1.185.120	HTTP	POST /sap(bd1 b1z PTUXMCZkPw1pb1z2PTc MmUwMCZpPTEmcZ
336	2010-01-08 10:26:02.433358	0.000	65106	679	128	10.18.15.10	10.1.185.120	HTTP	POST /sap(bd1 b1z PTUXMCZkPw1pb1z2PTc MmUwMCZpPTEmcZ
499	2010-01-08 10:26:10.946531	0.000	65535	671	128	10.18.15.10	10.1.185.120	HTTP	POST /sap(bd1 b1z PTUXMCZkPw1pb1z2PTc MmUwMCZpPTEmcZ
627	2010-01-08 10:26:49.492859	0.000	64248	1093	128	10.18.15.10	10.1.185.120	HTTP	POST /sap(bd1 b1z PTUXMCZkPw1pb1z2PTc MmUwMCZpPTEmcZ
645	2010-01-08 10:26:52.102616	0.000	65106	1093	128	10.18.15.10	10.1.185.120	HTTP	POST /sap(bd1 b1z PTUXMCZkPw1pb1z2PTc MmUwMCZpPTEmcZ

At Tier-3 there are only Five(5) Post request Observed

Didn't observe one post request for which earlier tiers had the "Internal server Error"

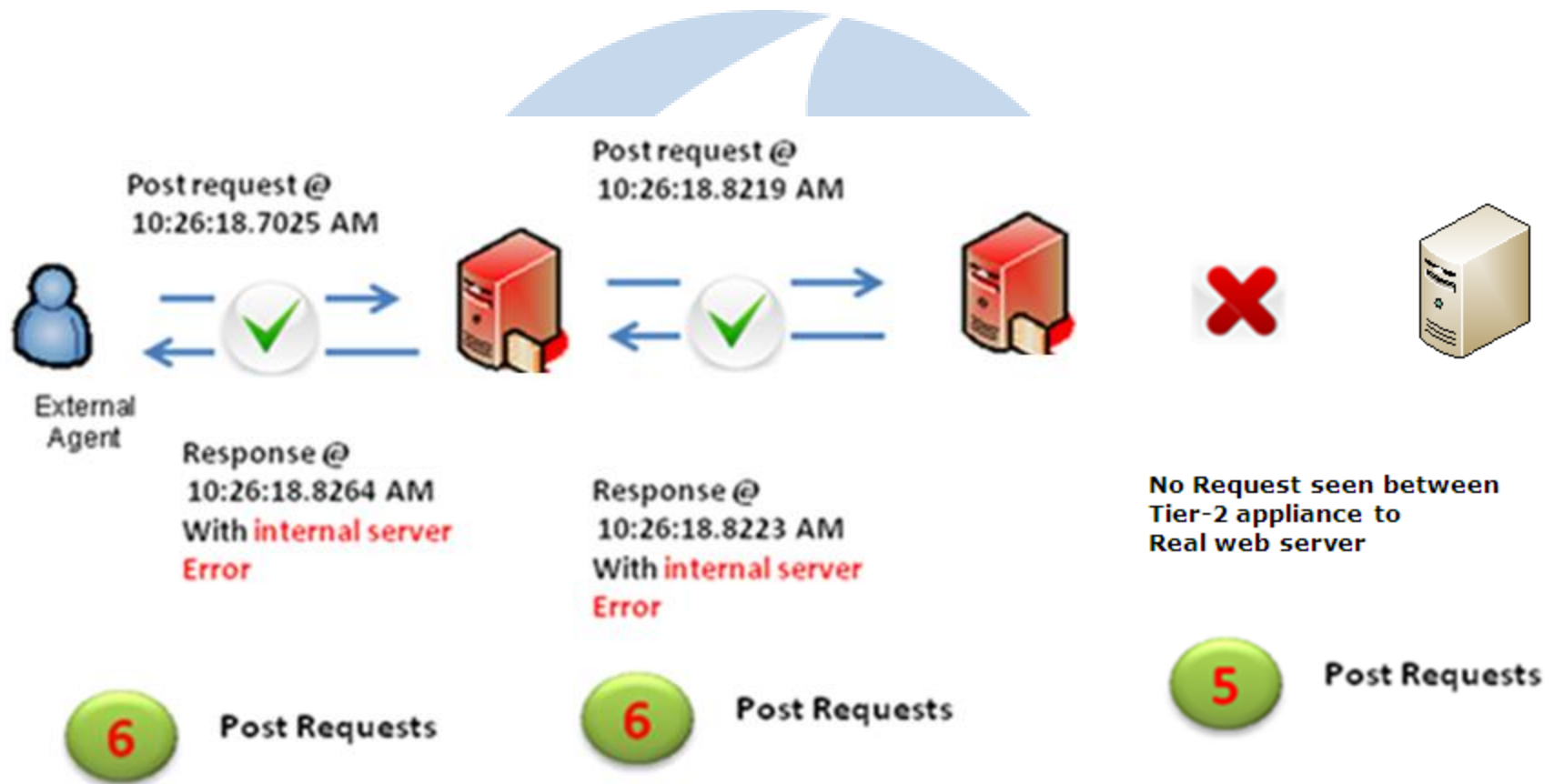
Internet Protocol, Src: 10.18.15.10 (10.18.15.10), dst: 10.1.185.120 (10.1.185.120)

```
0000 00 00 0c 07 ac 01 00 14 c2 3f ed f2 08 00 45 00 ..... ?....E.
0010 02 c1 43 a4 40 00 80 06 d7 fd 0a 12 0f 0a 0a 01 ...C.@.....
0020 b9 78 04 b6 20 1c 8f 77 15 85 3e fa 8e 43 50 18 ...x...w...>..CP.
0030 fc 8f 30 44 00 00 76 12 76 39 21 bb ba a3 52 e8 ...0d..v.v9!...R.
0040 7c b7 32 2b 44 9c 6f c9 45 91 a7 bc fe 10 03 7b |.2+d.o. E.....{
0050 06 f2 e8 c4 e8 67 62 4f 69 0e f1 fb 02 00 48 bf ....gbo i.....H.
0060 83 0b ab 54 a0 a4 c5 94 01 32 a2 23 be 94 34 8d ...T.....2.#..4.
0070 5c 4e be 96 c6 36 35 9e 1d e1 38 cb f0 8a a4 78 \N...65...8...x
0080 2d 85 2e 22 92 da f7 f1 cc ad 04 ca 9c ee 76 76 ..."......vv
0090 5d ff 68 7a 30 ca ce 85 13 64 d6 67 e9 3d f4 24 ].hz0....d.g.=.$
00a0 a9 3d 3a 30 d1 45 c1 26 e6 11 d9 91 0f 45 93 df .=:0.E.&....E.
00b0 11 4e d0 16 ea c9 95 a6 cd 0f 9a 90 55 96 64 ee .N.....U.d.
00c0 8d 44 47 a4 44 23 04 11 06 88 66 c3 53 b4 bf f9 .DG.D#.f.S...
00d0 c3 30 ef 01 ba 02 34 53 be 64 d0 4e 82 3f 45 71 .0...45.d.N.?Eq
00e0 3f db 3e 81 30 b3 12 91 ba 93 b5 84 37 8c f5 30 ?.>.0....7..0
00f0 61 fc c9 cf 60 3f 0f 8a 50 44 db 4d a9 cb 03 57 a...?. PD.M...W
0100 1e 58 36 5f c3 05 bb bf a6 54 19 c3 3c e9 f7 45 .X6.....T.<..E
0110 f5 31 c8 ff 90 30 a1 9b e7 e1 10 2f 6f 2a cc 43 .1...0..../o*.C
0120 57 29 40 87 85 5f cb b8 ec 3e 51 1a 08 24 4f 96 w)@...>.Q. $O.
0130 8c 68 1e b5 9f bd 74 55 54 8b 9a 9b 91 83 ae 98 .h...tU T.....
0140 84 ed 97 78 12 9a d4 4b 4b d5 a2 26 0d ed aa 6e ...x...K K.&...n
0150 d9 77 9e 81 73 17 f5 79 d8 d7 6f ea f4 8e 0d c7 .w..S.y.....
0160 d0 f1 8e 97 f4 c7 53 59 69 94 37 ad fa aa 4a 0f .....SY i.7..J.
0170 70 14 50 7c 5f 4b 06 f8 c5 ed a0 53 e6 h6 e7 2h n.pl K...S...+
```

Frame (719 bytes) | Reassembled TCP (3157 bytes) | Decrypted SSL data (3127 bytes) | Reassembled SSL (8338 bytes)

File: "C:\Documents and Settings\adesa\Desko... | Packets: 653 Displayed: 5 Marked: 0 | Profile: Default

Analysis Summary



Root Cause Identified

- Tier-2 appliance was not forwarding to next tier (real server) and was dropping the request.
- In response, it sent an “Internal Server Error” to the requestor

Solution

- Escalated to vendor regarding observations:
 - Vendor acknowledged this is a software “bug”
 - Suggested upgrading to prevent this issue
- After upgrading, issue no longer seen! 😊

Presentation Summary

- Understand the application flow to help you capture interesting traffic
- Pay attention to any data that could be used as a “signature” to correlate traces with user events
- Wireshark’s capabilities of decryption, filtering, follow SSL stream, and others will help your analysis
- X-forwarding can provide info on IP address/host, but to get visibility of user task look above IP layer

Questions?

