Remote Analysis Report
Enabling Continual Service Improvement in Critical Systems

Overall Health

Web Application
Middleware
Storage
Application Communication
Database
Citrix
Supporting Application Infrastructure
Security

PREPARATION
Month: June 2016
Report: Sample
Prepared for: Customer
Analyst: Analyst
ExtraHop Networks

Configuration:
EDA9100
Firmware: 5.2
ID: XXXXX
WEB APPLICATION

A review of the web application protocols including HTTP and HTTPS. More information regarding presentation of the HTTP protocol in the ExtraHop UI is available here.

FINDINGS:

<table>
<thead>
<tr>
<th>File Not Found errors (HTTP status code 404) on device1 have significantly decreased. (Trend: Resolved)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate Internal Server errors (HTTP status code 500) that occurred on the server and were associated with a single URI. Internal Server errors were not previously noted on this server. (New finding)</td>
</tr>
<tr>
<td>Investigate improvements that can be made to the server that experienced lengthy processing time on average. Processing time on this server has become less severe since the previous analysis period. (Trend: Improvement)</td>
</tr>
</tbody>
</table>

Each piece of analysis comes with an indicator of how it compares with the previous report. An up-and-to-the-right arrow indicates improvement, a down arrow indicates degradation, and a star symbolizes a new finding.
CRITICAL CONCERNS:

86.9% of HTTP responses on the AAAA server were Internal Server errors (HTTP status codes 500). Internal Server errors indicate that HTTP server encountered an unexpected condition that prevented it from fulfilling the request.

Internal Server errors on AAAA (indicated by the vertical red bars) appeared to correlate with the HTTP transaction rate (indicated by the green line). At peak, 3,859 Internal Server errors occurred on this device in a single hour.

100% of Internal Server errors on AAAA occurred while attempting to access a single URI resource, xxxxxxxx/PrePayService.

Trend graphs make it easy to determine if errors occur during acute events or if they are part of a chronic problem.
**IMPROVEMENT OPPORTUNITIES:**

Several HTTP servers are experiencing lengthy processing time on average. Notice that the **server accounted for 55,742 responses and experienced an average processing time of over 2 seconds.**

<table>
<thead>
<tr>
<th>Device Server</th>
<th>IP Address</th>
<th>Responses</th>
<th>Errors</th>
<th>Processing Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>12</td>
<td>0</td>
<td>11,208.5</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>55,742</td>
<td>10,785</td>
<td>2,080</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>6,554</td>
<td>0</td>
<td>1,521</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>6</td>
<td>0</td>
<td>1,505.5</td>
</tr>
</tbody>
</table>

Utilizing the ExtraHop Heatmaps feature, we see that a high concentration of transactions on **experienced approximately 5 seconds of processing time. A darker area on the graph below indicates a high concentration of transactions.**

Note the large standard deviation tied to processing time for the **xxx.xxx.xxx.xxx/EAI/OA URI. This indicates that the processing times experienced for this URI were very "dispersed" and had a large amount of variation, meaning that much larger processing times were also observed. Using these standard deviation and mean measurements, we can conclude that approximately 1,277 transactions experienced processing times of approximately 12.7 seconds.**

Each report includes different types of visualizations, optimized for the type of data being shown.
DATABASE

A review of all parsed database protocol traffic, regardless of the type of database. Protocols include (if licensed): TNS (Oracle), TDS (MS SQL), DB2, Informix, Sybase, PostgreSQL, and MySQL. More information regarding presentation of database protocols in the ExtraHop UI is available here.

FINDINGS:

Investigate database errors on the BBBB server that occurred constantly; these errors were related to failed logins for the ZZZ_ZZZZZ database. (New finding)

CRITICAL CONCERNS:

None noted.

IMPROVEMENT OPPORTUNITIES:

1.0% of all database responses were errors.

93.3% of database errors were concentrated on the BBBB server. Also note that there were approximately twice as many errors on this server than there were responses, indicating that each response sent from this server corresponded to two error messages.
Database error rate (indicated by the vertical red bars) on BBBB directly correlated with overall database transaction rate (indicated by the green line). Both of these metrics remained approximately constant for the duration of the observation period. For the majority of the analysis period more than 700 database errors were sent from this server each hour.

100% of database errors from BBBB were returned to the YYYY client.

Database errors from BBBB had two error messages. These error messages suggest that 100% of errors on BBBB result from the YYYY client attempting to log on to BBBB and open a ZZZ_ZZZZZ database. 100% of these login and open attempts are failing. Investigate scheduled tasks that may be causing these errors.

Also worth noting are the processing times observed on this database server. While a majority of transactions were non-concerning (75% of all database transactions took, at most, 3 milliseconds of processing time), note that database transactions on BBBB experienced as much as a minute of processing time.
The ExtraHop Heatmaps feature reveals that a “concentration” of transactions experienced around 3 seconds (3,000 milliseconds) of processing time. A darker area on the graph below indicates a higher concentration of transactions so while a large volume of transactions experienced less than 400 milliseconds of processing time, it may be worth researching what is causing some of the previously discussed failed logins to experience such lengthy processing times.
**Middleware**

A review of all parsed middleware protocol traffic (if licensed): FTP, MQSeries, and Memcache. More information regarding presentation of the FTP protocol in the ExtraHop UI is available here.

**Findings:**

Investigate FTP errors that occurred on the server that appeared to correlate with SITE method calls. Overall FTP error rate has decreased since the previous analysis period. (Trend: Improvement)

**Critical Concerns:**

16.8% of FTP responses resulted in an error. This is a decrease from the 25.4% FTP error rate noted in the previous report.

<table>
<thead>
<tr>
<th>FTP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests: 203,043</td>
</tr>
</tbody>
</table>

38.4% of FTP errors occurred on the server.

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>Responses</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>44,267</td>
<td>10,696</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>28,222</td>
<td>4,713</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>25,897</td>
<td>4,350</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>20,532</td>
<td>4,297</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td>1,749</td>
<td>922</td>
</tr>
</tbody>
</table>
Spikes, in both FTP error rate (indicated by the vertical red bars) and transaction rate (indicated by the green line) on ccccc, occurred at the same time each day. The nightly spike is highly suggestive of an automated FTP process that is broken or otherwise misconfigured.

93.8% of FTP errors from ccccc were returned to the device2 client.

100% of FTP errors from ccccc affected FTP transactions for the xxx_xxx user.

68.2% of FTP errors from ccccc had a single error message, "500 ' redacted : command not understood". FTP 500 errors are indicative of failures related to invalid syntax.

Additionally, another 31.8% of FTP errors from ccccc had the “550 Access is denied.” error message. FTP 550 errors imply that a file is not available because it was not found or there was some other error related to invalid use of the file system.
Further analysis of FTP errors suggests that there is a relationship between FTP 500 errors and the use of the FTP SITE method. FTP 500 errors are indicative of erroneous syntax resulting in an unrecognized action that, as a result, could not take place.

Looking at the busiest FTP server (CCCC), we see an almost 1:1 relationship between the use of the SITE method and FTP error code 500.

The report's visualizations also show trends over time so that correlations are easier to identify.

**IMPROVEMENT OPPORTUNITIES:**

Not evaluated.
CITRIX
A review of Citrix performance.

**FINDINGS:**

Investigate lengthy session load times on the DDDD device that primarily affected two clients and were related to a single application. Citrix load times have slightly decreased since the previous observation period. (Trend: Improvement)

**CRITICAL CONCERNS:**

None noted.

**IMPROVEMENT OPPORTUNITIES:**

Several ICA servers are experiencing lengthy load times in excess of 40 seconds per session launch. When launching an ICA session, lengthy load times will delay the start of the ICA session and cause latency in overall application processing. ICA session launches transiting the DDDD device experienced a high number of launches with long load times.
Drilling into **DDDDD**, we can see that session launches transiting two Cisco devices are primarily affecting two clients: **FFFFF** and **GGGGGG**.

<table>
<thead>
<tr>
<th>Device</th>
<th>IP Address</th>
<th>Host</th>
<th>Launches</th>
<th>Load Time (ms)</th>
<th>Login Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>redacted</td>
<td>redacted</td>
<td></td>
<td>321</td>
<td>37049.4</td>
<td>11254.1</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td></td>
<td>257</td>
<td>38294.8</td>
<td>9867.9</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td></td>
<td>37</td>
<td>34242.1</td>
<td>8063.9</td>
</tr>
<tr>
<td>redacted</td>
<td>redacted</td>
<td></td>
<td>16</td>
<td>29034.0</td>
<td>53013.8</td>
</tr>
</tbody>
</table>

Three **MMMMMM** application was most impacted by lengthy load times. Investigate transactions that may be impacted by lengthy load times for this application.
STORAGE

A review of all parsed storage protocol traffic. Protocols include (if licensed): CIFS, NFS, and iSCSI. More information regarding presentation of storage protocols in the ExtraHop UI is available here.

**FINDINGS:**

Investigate `STATUS_ACCESS_DENIED` CIFS errors that transited the device and appeared to have originated at yyyy.yyyyyyyyy. The volume of CIFS errors significantly increased since the previous observation period. (Trend: Worse)

**CRITICAL CONCERNS:**

49.6% of CIFS responses were errors. This is an increase from the 3.4% CIFS error rate noted in the previous report. High volumes of errors should be investigated to determine if action is required to fix or if changes can be made to reduce unnecessary processing time.

70.7% of CIFS errors transited the device. Additionally, note that 49.0% of CIFS responses that transited this device were errors.
CIFS error rate (indicated by the vertical red bars) on directly correlates with overall CIFS transaction rate (indicated by the green line). Both of these metrics increased each afternoon. At peak, this device experienced 1,049,331 errors over the course of a single hour, or more than 291 errors every second. Note that this server was only active for the first four days of the observation period.

CIFS errors from have variations of STATUS_ACCESS_DENIED error messages. This error indicates that a method, in this case NT_CREATE_ANDX, was unable to complete due to invalid credentials.

CIFS errors from were returned to a wide variety of clients.
Looking at client-side CIFS metrics for some of these clients, we see that a large portion of CIFS errors that transited NNNNN originated on the SSSSS server at yy.yy.yy.yy.

**IMPROVEMENT OPPORTUNITIES:**

Not evaluated.
SUPPORTING APPLICATION INFRASTRUCTURE

A review of protocol traffic related to supporting application infrastructure, including DNS, SMTP, LDAP and Kerberos. More information regarding presentation of the DNS and LDAP protocols in the ExtraHop UI is available via the previous links.

**FINDINGS:**

Investigate the high volume of DNS response errors concentrated on the HHHHH device that were related to reverse IP lookups. (New finding)

**CRITICAL CONCERNS:**

91.4% of all DNS responses were errors. A DNS response error occurs when a client makes a DNS lookup and the DNS server responds with some sort of error. These errors may not break an application, but they add latency to application transactions and cause unnecessary processing on the DNS server.

48.6% of DNS response errors occurred on the HHHHH server. Note that 99.5% of DNS requests made to this server resulted in response errors.

DNS problems often go unnoticed by IT staff, but contribute to overall latency and can be fixed with minimal effort.
DNS response error rate (indicated by the vertical red bars) on HHHHH directly correlated with transaction rate (indicated by the green line). Both of these metrics fluctuated over the course of the analysis period but generally increased during daytime hours.

DNS response errors from HHHHH occurred in association with what appear to be a variety of reverse DNS lookups, when the client feeds the server an IP address looking for a hostname. Note that these queries are erring nearly 100% of the time they are called.

Nearly 100% of DNS response errors from HHHHH were returned the LLLLL client via a Cisco device.

**IMPROVEMENT OPPORTUNITIES:**

Not evaluated.
APPLICATION COMMUNICATION


FINDINGS:

<table>
<thead>
<tr>
<th>Investigation</th>
<th>Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate Zero Windows sent from the RRRR device that impacted HTTP transactions. The overall volume of Zero Windows increased 223% (more than tripled) since the previous analysis period. (Trend: Worse)</td>
<td>↓</td>
</tr>
<tr>
<td>Investigate IP fragmentation on the UUUU device. (New finding)</td>
<td>☀</td>
</tr>
</tbody>
</table>

CRITICAL CONCERNS:

More than 111,000,000 Zero Windows were observed on the Customer network over the course of the seven-day observation period. This is an increase from the 34,600,000 Zero Windows noted in the previous report. A Zero Window indicates that the connection between two devices has stalled and that the device sending the Zero Window is unable to keep up with the rate of data that a peer is sending. In effect, the device sending the Zero Window is saying, "send no data until further notice." 80.3% of Zero Windows were sent from the RRRR device at aa.ee.ii.oo.

TCP analysis offers insight into a commonly overlooked area. The Atlas report's TCP analysis reveals how well applications and the network interact.
The rate of Zero Windows sent from \texttt{RRRR} increased during daytime hours. At peak, 1,140,000 Zero Windows were sent from this device over the course of a single hour, or \textbf{more than 316 Zero Windows every second}.

99.8\% of Zero Windows sent from \texttt{RRRR} impacted HTTP transactions.

67.9\% of Zero Windows sent from \texttt{RRRR} impacted communication with four similarly named \texttt{EHEH0#} devices.

Tying TCP metrics with Layer 7 protocols helps staff to diagnose underlying communication problems.
More than 29,300,000 IP fragments were sent onto the Customer network over the course of the seven-day observation period. IP fragmentation may be caused by an MTU mismatch between devices on the network. This results in high volumes of segments being sent across the network, which can overwhelm both the network as well as devices.

<table>
<thead>
<tr>
<th>User Group:</th>
<th>L3</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Fragments In:</td>
<td>8,244,681</td>
</tr>
</tbody>
</table>

44.4% of IP fragments were outbound from the UUUUUU device. Note that there were no IP fragments inbound to UUUUUU. This indicates that all IP fragmentation originated on UUUUUU (rather than UUUUUU simply transferring IP fragments from other transactions).

100% IP fragments from UUUUUU were sent to uu.xx.yy.zz via broadcast traffic on UDP port 8156.

**IMPROVEMENT OPPORTUNITIES:**

Not evaluated.
**SECURITY**

Review of SSL sessions that may be insecure, transactions involving suspicious foreign IPs, and other L7 protocol activity that may be easily compromised. More information regarding presentation of the SSL protocol in the ExtraHop UI is available [here](http://www.us-cert.gov/ncas/alerts/TA13-088A).

**FINDINGS:**

<table>
<thead>
<tr>
<th>Findings</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigate excessive use of the <strong>ANY</strong> method by the PPPPP server; a significant volume of <strong>ANY</strong> method calls originated in Australia. The volume of <strong>ANY</strong> method calls has slightly decreased since the previous analysis period. (Trend: Improvement)</td>
<td>![↑]</td>
</tr>
<tr>
<td>Reduce use of the <strong>TLS_DH_anon_WITH_AES_256_GCM_SHA384</strong> cipher suite associated with connections involving the LLLLLL client. Overall usage of the <strong>TLS_DH_anon_WITH_AES_256_GCM_SHA384</strong> cipher suite has not significantly changed since the previous analysis period. (Trend: No change)</td>
<td>![→]</td>
</tr>
<tr>
<td>Reduce FTP 530 errors that occurred on the PPPPPP server and were primarily returned to clients in China. (New finding)</td>
<td>![☀]</td>
</tr>
</tbody>
</table>

**CRITICAL CONCERNS:**

Over 15,500,000 instances of the DNS “**ANY**” method occurred during the observation period. This is a decrease from the volume of **ANY** method requests noted in the previous report, however, this is still a concerning volume. Use of the **ANY** method returns all known information about a DNS zone in a single request, and high volumes of these method calls is usually indicative of a DNS Amplification Attack. More information available here: [http://www.us-cert.gov/ncas/alerts/TA13-088A](http://www.us-cert.gov/ncas/alerts/TA13-088A).

The Atlas report’s security section frequently uncovers user and system behavior that represents risk to your organization.
86.3% of ANY method calls occurred on the PPPP DNS server at xx.yy.zz.aa.

The following Geomap identifies the physical location of IPs that sent ANY requests to the server at xx.yy.zz.aa. A denser dot indicates a higher volume of transactions. Note that the AAA.BB.XXX.ZZ IP located in Canberra, Australia accounts for a large portion of these ANY method requests. Investigate if transactions with this IP are expected behavior on the Customer network, or indicative of a larger issue.

Where appropriate, geomaps from the ExtraHop UI enable you to quickly determine the geographic origin of application communications.
11.7% of encrypted traffic on the Customer network used the 
TLS_DH_anon_WITH_AES_256_GCM_SHA384 cipher suite. This is not a significant change from the 
10.5% of encrypted traffic using this cipher suite noted in the previous report. Note that this was the 
fourth most commonly used cipher suite. A server that supports a cipher suite containing "anon" does 
not require key authentication, which allows clients to establish encrypted connections with the server 
anonymously. As such, ciphers of this type are vulnerable to man-in-the-middle attacks.

A variety of servers established encrypted connections using the 
TLS_DH_anon_WITH_AES_256_GCM_SHA384 cipher suite.

Nearly 100% of connections using the TLS_DH_anon_WITH_AES_256_GCM_SHA384 cipher 
suite were associated with SSL sessions involving the ______ client. This behavior was also 
noted in the previous report.

Additionally, note that 75.9% of SSL sessions involving the ______ client used the 
TLS_DH_anon_WITH_AES_256_GCM_SHA384 cipher suite. Additionally, note that the 
second most commonly used cipher suite by this client, 
TLS_DH_anon_WITH_AES_256_CDC_SHA, is also vulnerable to the same pitfalls.
1.7% of FTP responses were errors.

32.6% of FTP errors occurred on the PPPPP server. Additionally, note that 33.6% of FTP responses sent from this server were errors.

FTP error rate (indicated by the orange line) on PPPPP directly correlated with overall FTP response rate (indicated by the blue line). Both of these metrics fluctuated over the course of the observation period and did not appear to follow a particular pattern. At peak, 261 FTP errors were sent over the course of a single hour.
99.5% of FTP errors sent from PPPPP had a single error message, "530 User cannot log in.". FTP 530 errors occur due to invalid usernames and/or passwords provided during login, or other authentication and accounting errors. This was also the most common error message during the previous analysis period.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>530 User cannot log in.</td>
<td>5,732</td>
</tr>
<tr>
<td>534 Local policy on server does not allow TLS secure connections.</td>
<td>16</td>
</tr>
<tr>
<td>504 Security mechanism not implemented.</td>
<td>7</td>
</tr>
<tr>
<td>530 Please login with USER and PASS.</td>
<td>7</td>
</tr>
<tr>
<td>503 Login with USER first.</td>
<td>1</td>
</tr>
</tbody>
</table>

FTP errors sent from PPPPP were returned to a variety of what appear to be external client IPs via a Cisco device.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Device</th>
<th>Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>redacted</td>
<td>via</td>
<td>258</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>196</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>186</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>131</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>129</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>126</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>114</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>114</td>
</tr>
<tr>
<td>redacted</td>
<td>via</td>
<td>97</td>
</tr>
<tr>
<td>via</td>
<td></td>
<td>96</td>
</tr>
</tbody>
</table>
Utilizing the ExtraHop Geomap feature, we can physically locate the clients that received FTP errors from PPPPP. Note that FTP errors from PPPPP were primarily returned to clients across China. FTP errors with these IPs are likely not by design, and should be further investigated and eliminated so as to reduce potential malicious behavior on the Customer network.

**IMPROVEMENT OPPORTUNITIES:**

Deferred due to critical concerns.
**METRICS CHECKLIST**

Atlas Remote Analysis reports include analysis of more than 20 protocols and look into problems regarding 70+ metrics that commonly impact network performance. For a complete overview of the protocols included and a detailed list of items analyzed in this report, please visit the following:

https://www.extrahop.com/platform/services/atlas-remote-analysis/checklist/

The findings in Atlas reports are based off of common issues seen across IT infrastructures in many different verticals, and with network configurations utilizing a wide swath of tools. If, however, some of the findings included in this report are expected behavior in your network, please send a note to atlas@extrahop.com outlining these items. ExtraHop Atlas analysts will keep note of the expected and/or excluded behavior seen in your infrastructure, and eliminate these findings from future report composition.