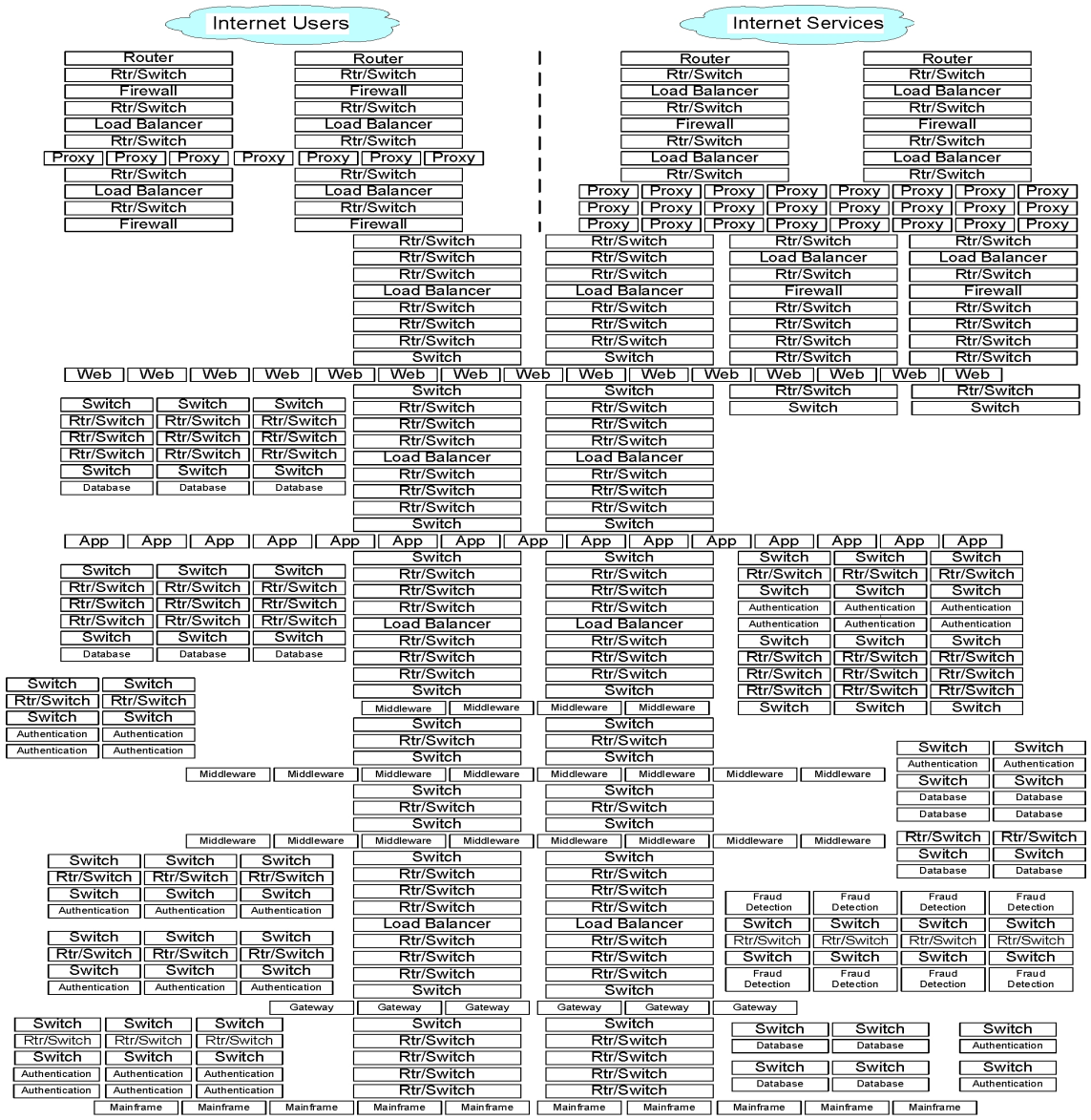
TLS 1.3 Operational Challenges

Steve Fenter

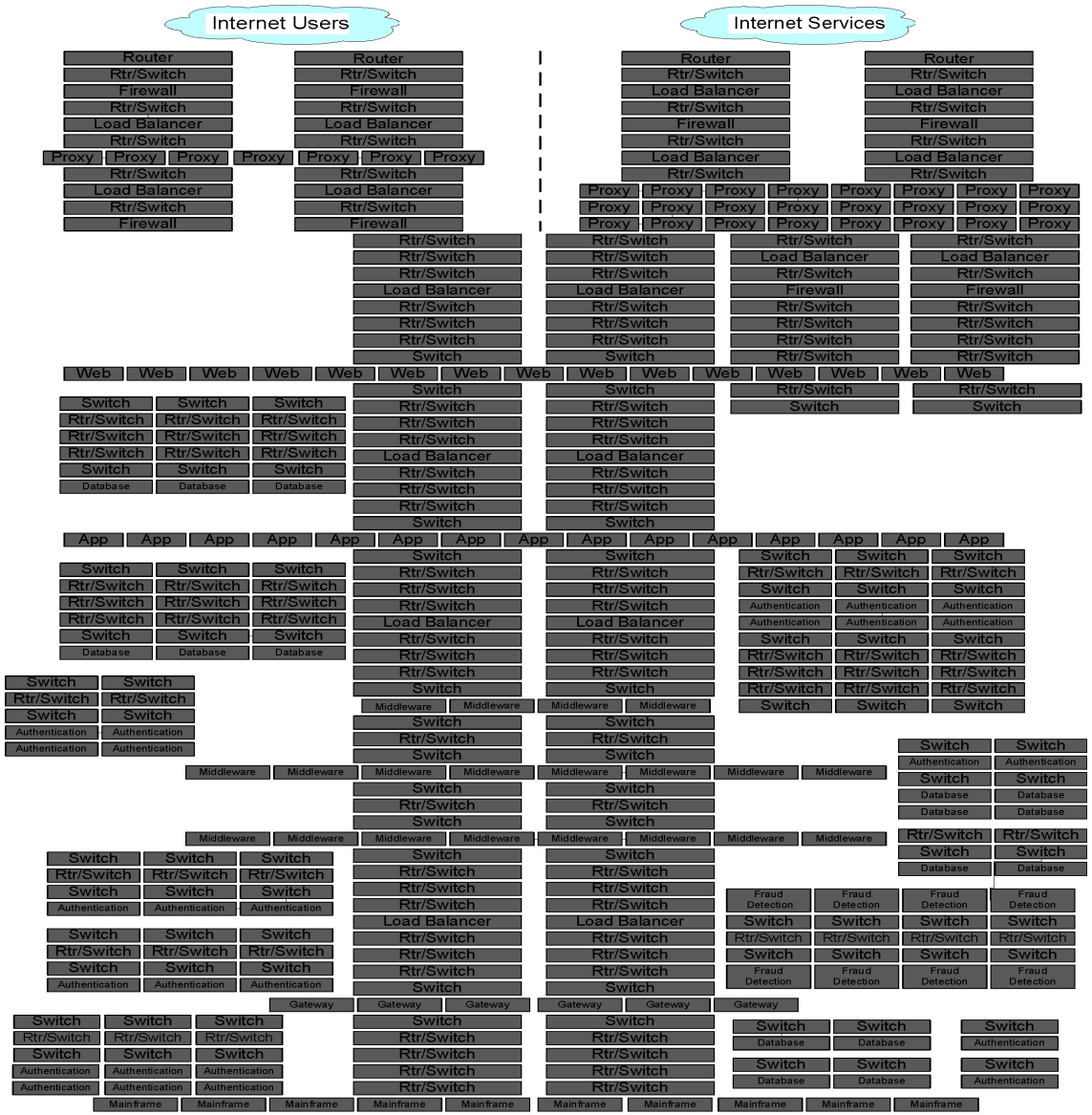
The TLS 1.3 Decryption Problem

- The RSA key exchange option has been removed
- This eliminates out-of-band TLS decryption capability
- Impact if you're TLS encrypted internally
  - Fraud Monitoring
  - IDS/IPS
  - Malware Detection
  - Threat Detection and Incident Response
  - Wireshark PCAP decryption

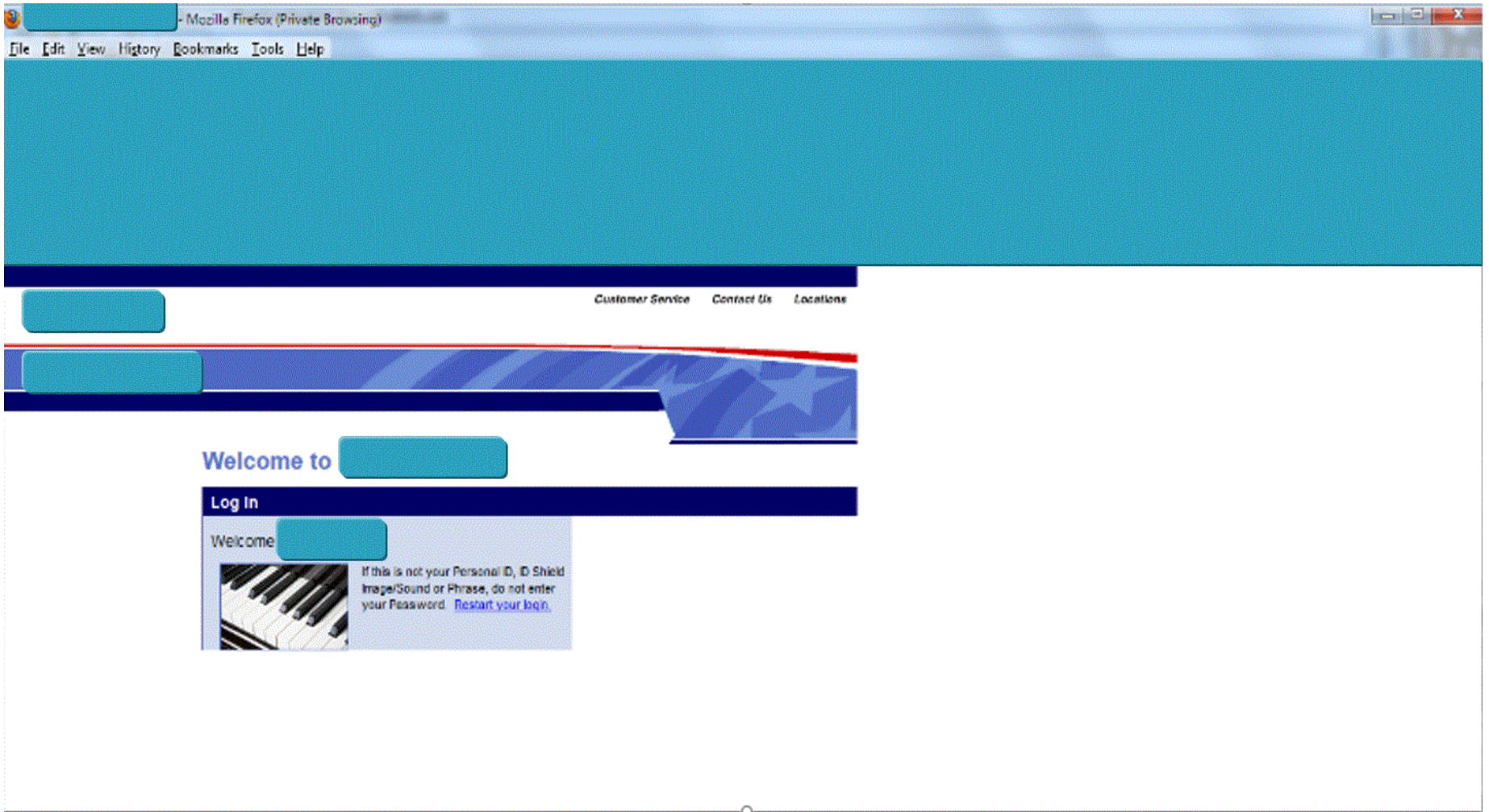
Enterprise Operational Support Environment



Enterprise Operational Support Environment – TLS 1.3



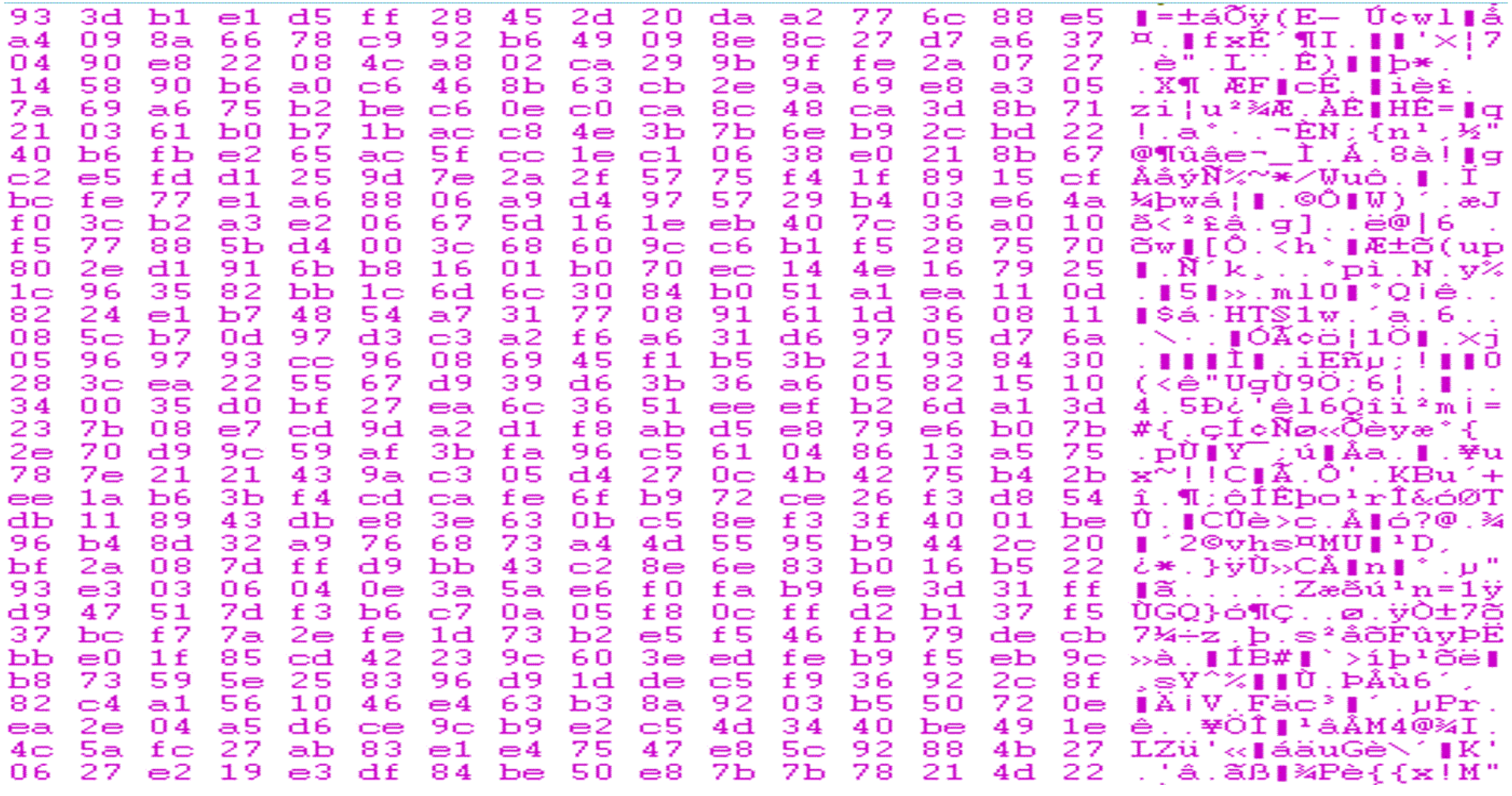
Login Failure



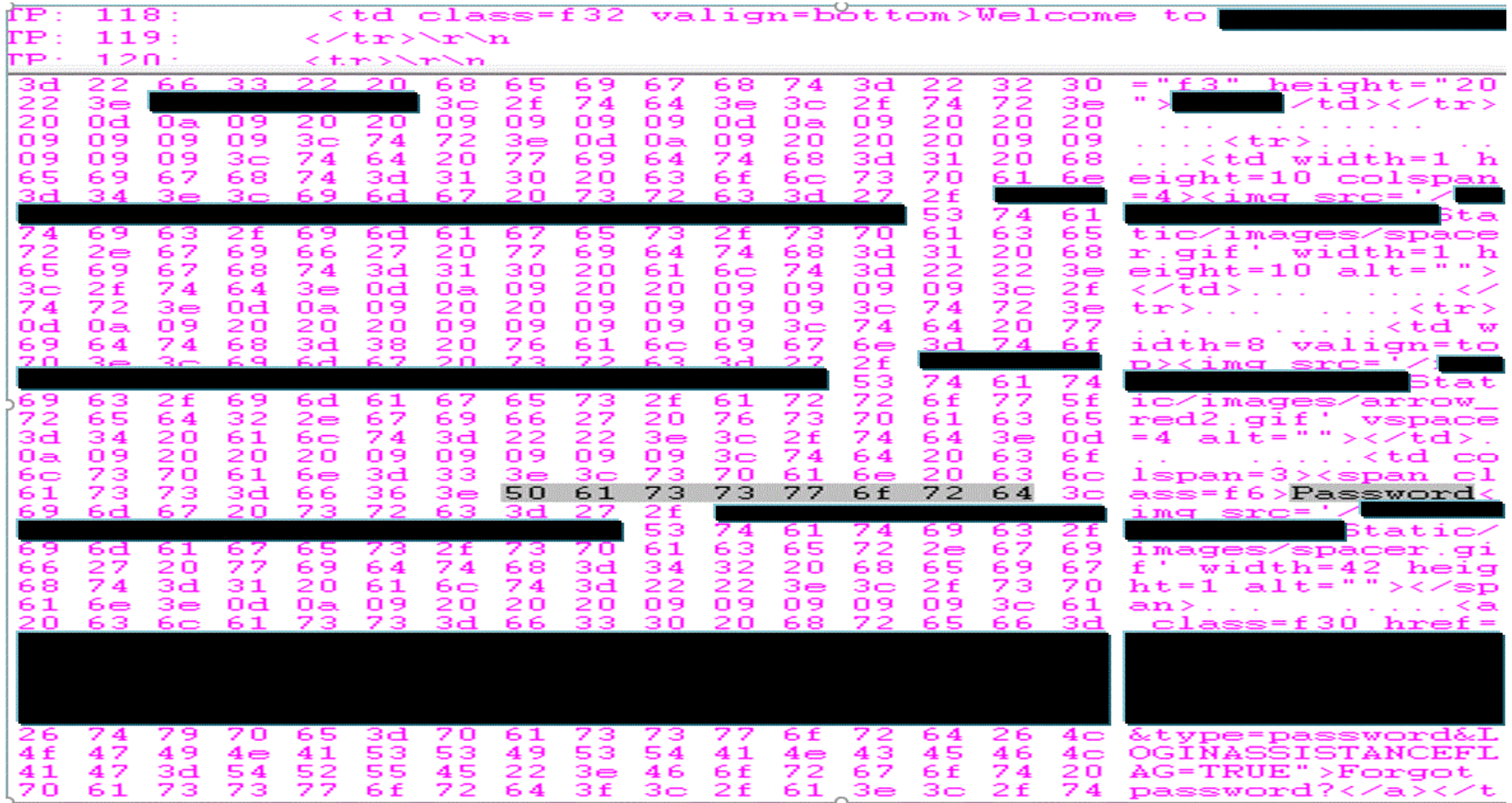
Application Log

15:30:43	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:30:59	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:36:29	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:36:34	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:41:35	Column 11	10.10.10.10	Enter Userid	Challenge Question
15:41:44	Column 11	10.10.10.10	Challenge Answer	Answer OK
15:49:01	Column 6	10.10.10.10	Enter Userid	Challenge Question
15:49:06	Column 6	10.10.10.10	Challenge Answer	Answer OK
15:54:16	Column 9	10.10.10.10	Enter Userid	Challenge Question
15:54:22	Column 9	10.10.10.10	Challenge Answer	Answer OK

Encrypted Login Screen



Decrypted Login Screen



Login Screen – Hex Data

```
20 63 6c 61 73 73 3d 22 66 32 22 3e 49 66 20 74   class="f2">If t
68 69 73 20 69 73 20 6e 6f 74 20 79 6f 75 72 20   his is not your 
50 65 72 73 6f 6e 61 6c 20 49 44 2c 20 49 44 20   Personal ID, ID 
53 68 69 65 6c 64 20 49 6d 61 67 65 2f 53 6f 75   Shield Image/Sou
6e 64 20 6f 72 20 50 68 72 61 73 65 2c 20 64 6f   nd or Phrase, do
20 6e 6f 74 20 65 6e 74 65 72 20 79 6f 75 72 20    not enter your 
50 61 73 73 77 6f 72 64 2e 26 23 31 36 30 3b 3c   Password. <
2f 73 70 61 6e 3e 26 23 31 36 30 3b 3c 73 70 61   /span> <spa
[redacted]
6c 66 22 3e 52 65 73 74 61 72 74 20 79 6f 75 72   lf">Restart your
20 6c 6f 67 69 6e 2e 3c 2f 61 3e 3c 2f 73 70 61    login.</a></spa
6e 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00   n>..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

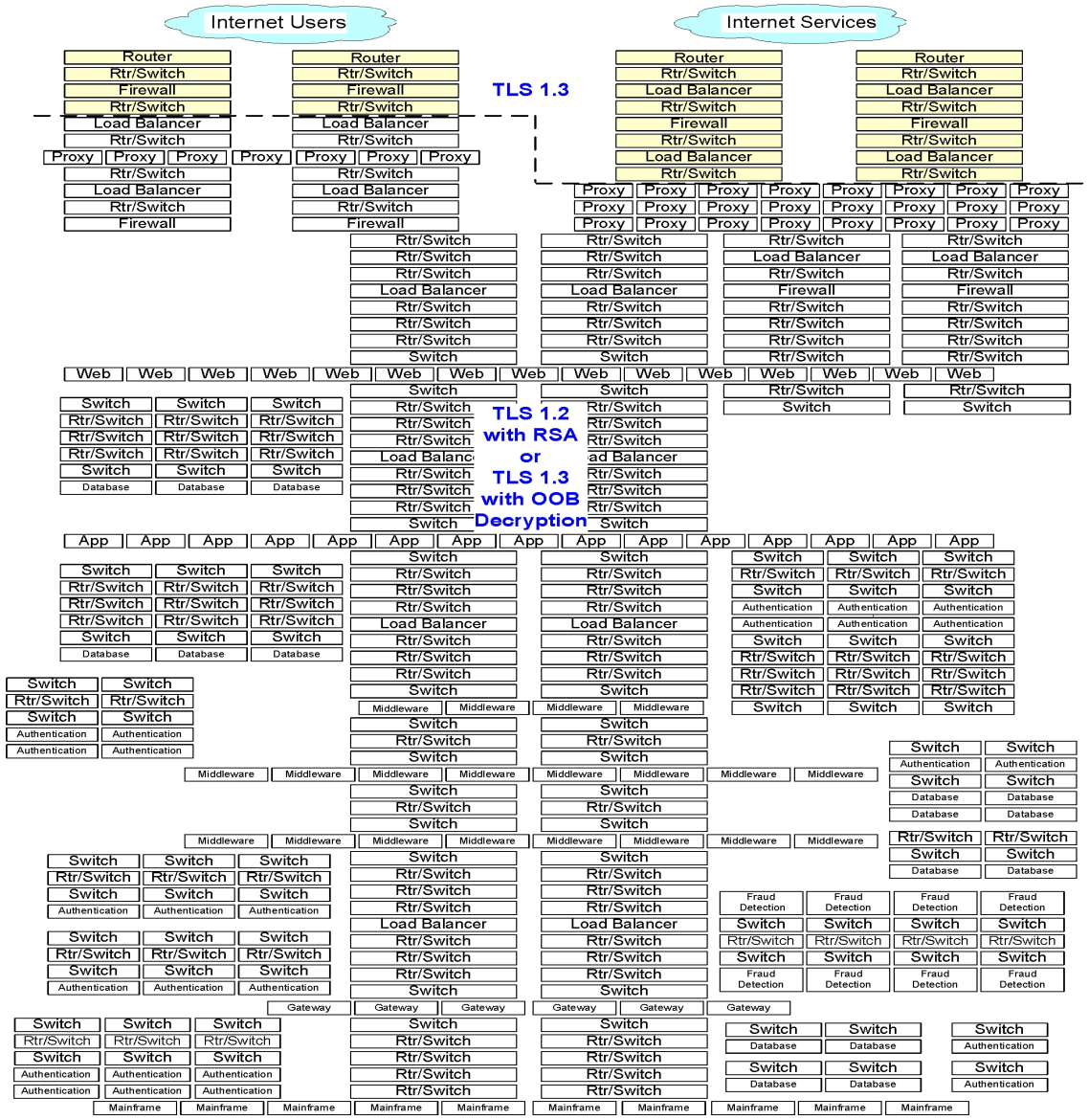
Enterprise Operations Requirements Summary

- Be able to trace a network packet anywhere in the enterprise and decrypt it.
- Be able to follow a transaction through the entire application and network infrastructure (and see what the transaction is doing).

Proposed Solution

- ETSI Middlebox Security Protocol Part 3 (Enterprise Transport Security)
  - Static Diffie-Hellman
  - Scalability
  - Consistent with TLS 1.3 Standard
  - Changes to TLS servers only

Proposed Data Center Visibility Solution



Limitations of Alternative Solutions

- Alternative TLS 1.3 Decryption Solutions
  - Inline/MITM TLS decryption
  - Ephemeral/session key export
- Alternative Tools
  - Bytecode instrumentation
  - Logs

Urgency – TLS 1.2

- We have a Diffie-Hellman problem, not just a TLS 1.3 problem.
- Vendors are moving Diffie-Hellman ciphers to the top of their TLS 1.2 cipher list
  - http/2 requires Diffie-Hellman only ciphers
- A few vendors are completely removing RSA from their TLS 1.2 cipher list.