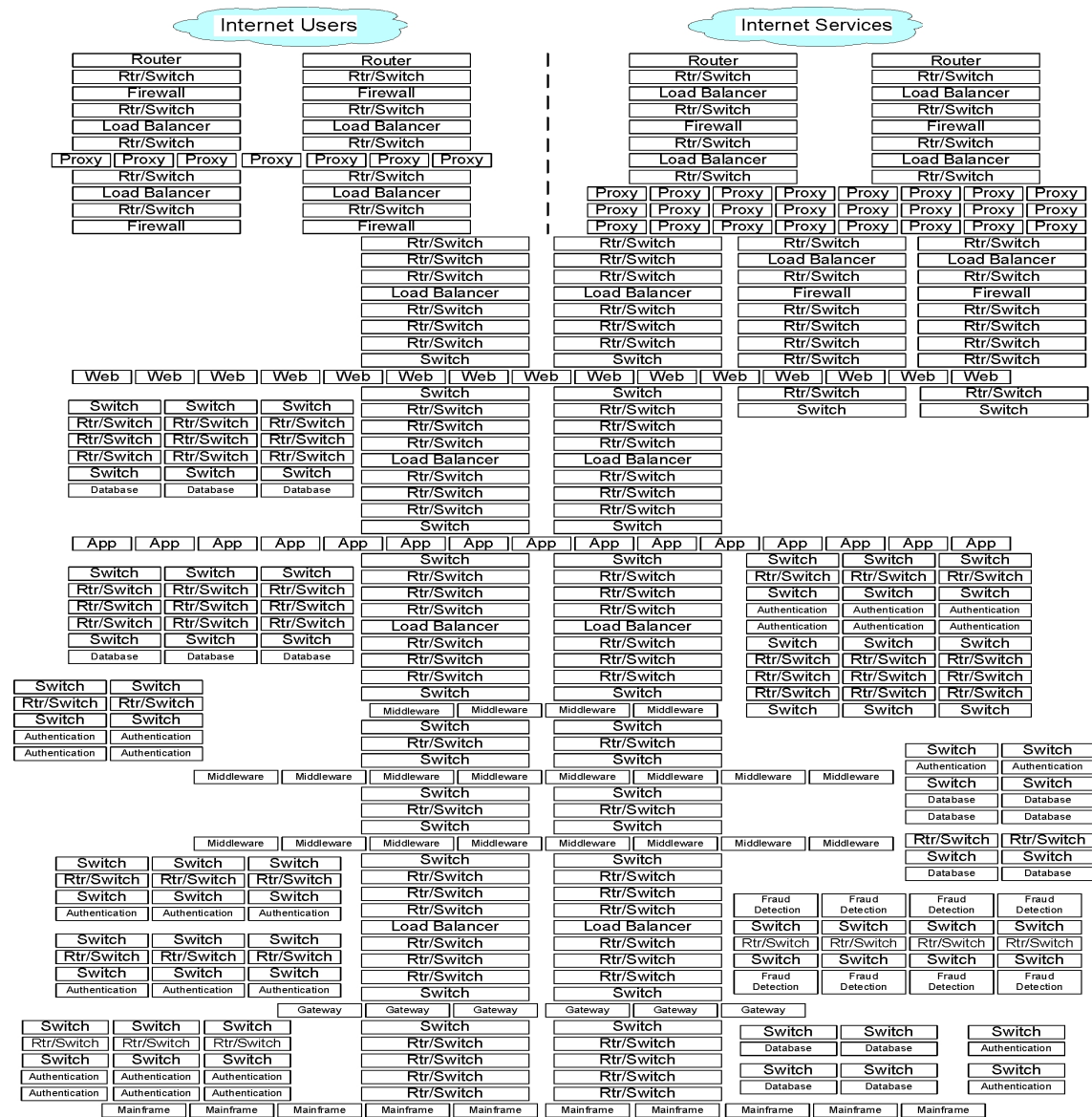
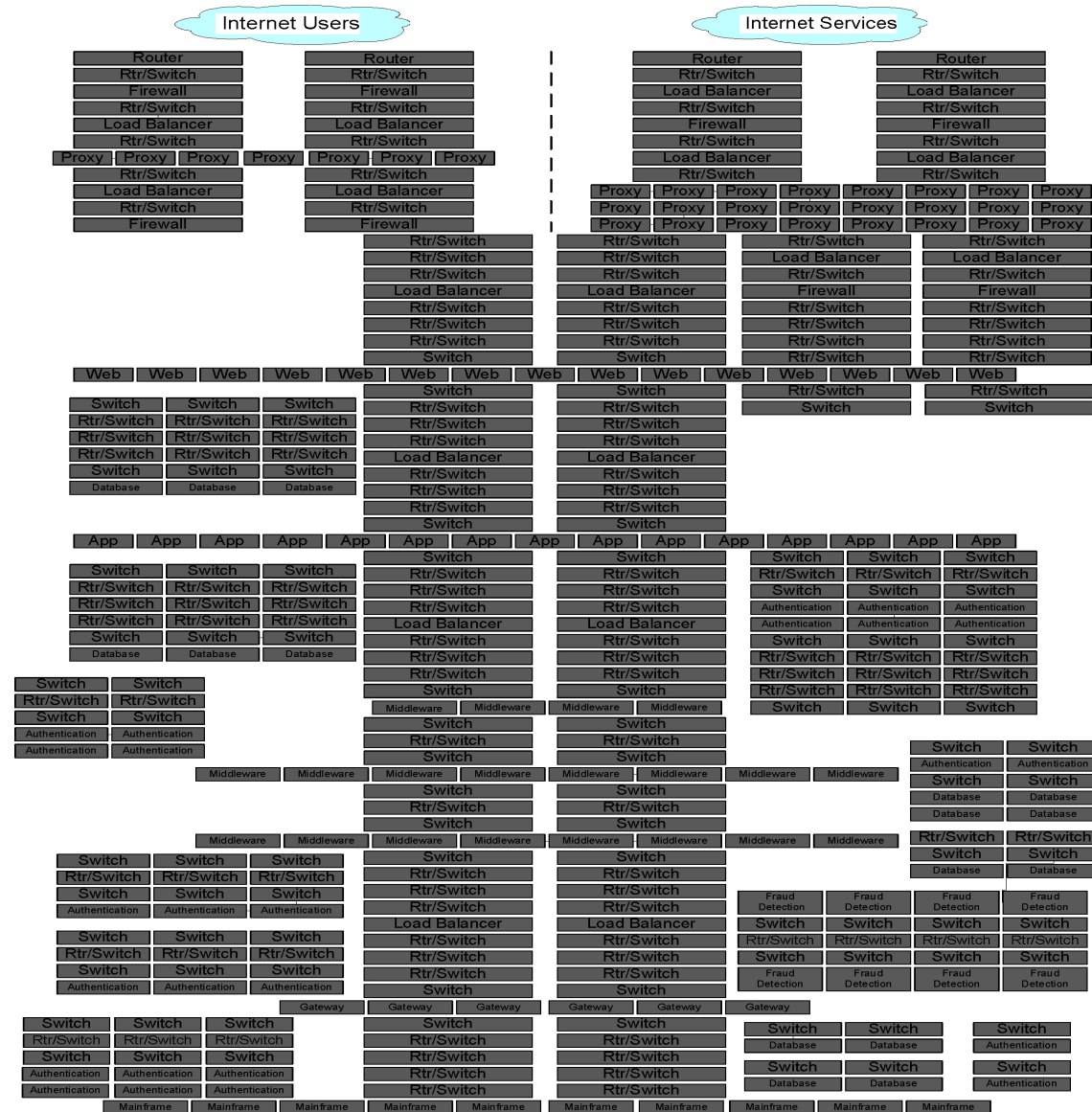


TLS 1.3 Operational Challenges

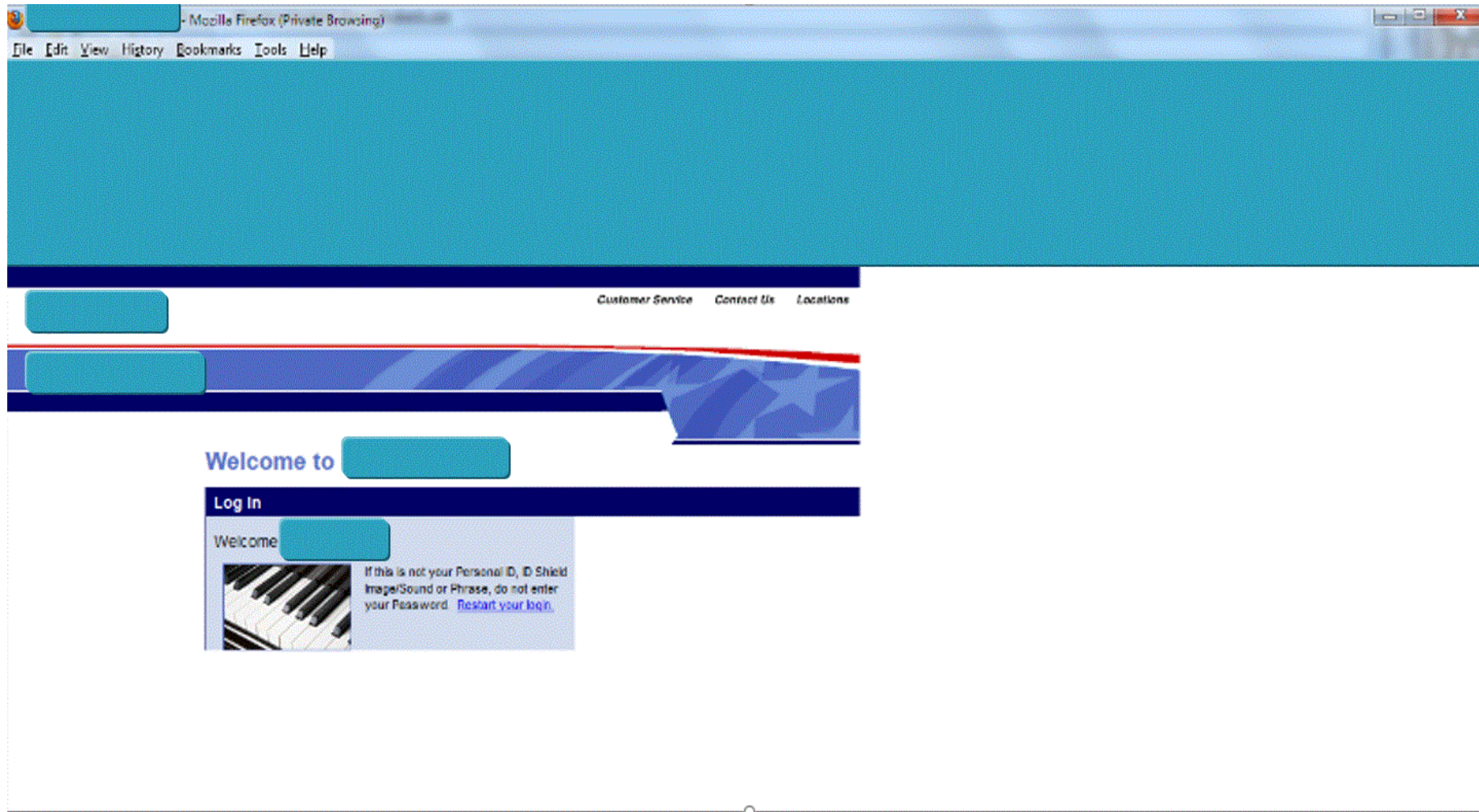
Steve Fenter

- 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





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

93	3d	b1	e1	d5	ff	28	45	2d	20	da	a2	77	6c	88	e5	=±áÕÿ(E- Úcwl á
a4	09	8a	66	78	c9	92	b6	49	09	8e	8c	27	d7	a6	37	¤. fxE'¶I. '× 7
04	90	e8	22	08	4c	a8	02	ca	29	9b	9f	fe	2a	07	27	.è".L'.Ê) p*.'
14	58	90	b6	a0	c6	46	8b	63	cb	2e	9a	69	e8	a3	05	.X¶ÆF cÊ. iè£.
7a	69	a6	75	b2	be	c6	0e	c0	ca	8c	48	ca	3d	8b	71	zi u²¾Æ.ÁÊ HÉ= q
21	03	61	b0	b7	1b	ac	c8	4e	3b	7b	6e	b9	2c	bd	22	!.a*.~.ÉN;{n¹.¾"
40	b6	fb	e2	65	ac	5f	cc	1e	c1	06	38	e0	21	8b	67	@¶ûâe~_l.Á.8à! g
c2	e5	fd	d1	25	9d	7e	2a	2f	57	75	f4	1f	89	15	cf	ÁâýÑ%~*/Wuô. .I
bc	fe	77	e1	a6	88	06	a9	d4	97	57	29	b4	03	e6	4a	¾pwá .©Ô W)' .æJ
f0	3c	b2	a3	e2	06	67	5d	16	1e	eb	40	7c	36	a0	10	ð<²£â.g]..è@ 6 .
f5	77	88	5b	d4	00	3c	68	60	9c	c6	b1	f5	28	75	70	ðw [Ô.<h` Æ±ð(up
80	2e	d1	91	6b	b8	16	01	b0	70	ec	14	4e	16	79	25	.Ñ'k, ... *pì.N.y%
1c	96	35	82	bb	1c	6d	6c	30	84	b0	51	a1	ea	11	0d	.. 5 >..ml0 °Qiè..
82	24	e1	b7	48	54	a7	31	77	08	91	61	1d	36	08	11	\$á·HT\$1w.'a.6..
08	5c	b7	0d	97	d3	c3	a2	f6	a6	31	d6	97	05	d7	6a	.\.. ÓÃ¢ö 10 .×j
05	96	97	93	cc	96	08	69	45	f1	b5	3b	21	93	84	30	.. l .iEñµ;!!!!0
28	3c	ea	22	55	67	d9	39	d6	3b	36	a6	05	82	15	10	(<è"UgÛ9Ö;6
34	00	35	d0	bf	27	ea	6c	36	51	ee	ef	b2	6d	a1	3d	4.5Ðç'èl6Qîi²mi=
23	7b	08	e7	cd	9d	a2	d1	f8	ab	d5	e8	79	e6	b0	7b	#{.çÍcÑø«Öèyæ°{
2e	70	d9	9c	59	af	3b	fa	96	c5	61	04	86	13	a5	75	.pÛ Y~;ú Áa. .¶u
78	7e	21	21	43	9a	c3	05	d4	27	0c	4b	42	75	b4	2b	x~!!C Á.Ô'.KBu'+
ee	1a	b6	3b	f4	cd	ca	fe	6f	b9	72	ce	26	f3	d8	54	î.¶;ôÍÊpø¹rÎ&óØT
db	11	89	43	db	e8	3e	63	0b	c5	8e	f3	3f	40	01	be	Û. CÛè>c.Á ó?@.¾
96	b4	8d	32	a9	76	68	73	a4	4d	55	95	b9	44	2c	20	'2@vhs¤MU ¹D.
bf	2a	08	7d	ff	d9	bb	43	c2	8e	6e	83	b0	16	b5	22	¿*.}ýÛ»CÃ n °.µ"
93	e3	03	06	04	0e	3a	5a	e6	f0	fa	b9	6e	3d	31	ff	ã. :Zæðú¹n=1ÿ
d9	47	51	7d	f3	b6	c7	0a	05	f8	0c	ff	d2	b1	37	f5	ÛGQ}ó¶Ç. .ø.ÿÒ±7ð
37	bc	f7	7a	2e	fe	1d	73	b2	e5	f5	46	fb	79	de	cb	7¾÷z .p.s²âðFûypÊ
bb	e0	1f	85	cd	42	23	9c	60	3e	ed	fe	b9	f5	eb	9c	>>à. ÍB# `>íp¹ðè
b8	73	59	5e	25	83	96	d9	1d	de	c5	f9	36	92	2c	8f	.sY^% Û. ÞÁù6'.
82	c4	a1	56	10	46	e4	63	b3	8a	92	03	b5	50	72	0e	ÁiV.Fâc³ '.µPr.
ea	2e	04	a5	d6	ce	9c	b9	e2	c5	4d	34	40	be	49	1e	è. .¶ÖÎ ¹âÂM4@¾I.
4c	5a	fc	27	ab	83	e1	e4	75	47	e8	5c	92	88	4b	27	LZü'<< áâüGè\` K'
06	27	e2	19	e3	df	84	be	50	e8	7b	7b	78	21	4d	22	.. â.ãß ¾Pè{ {x!M"

Decrypted Login Screen

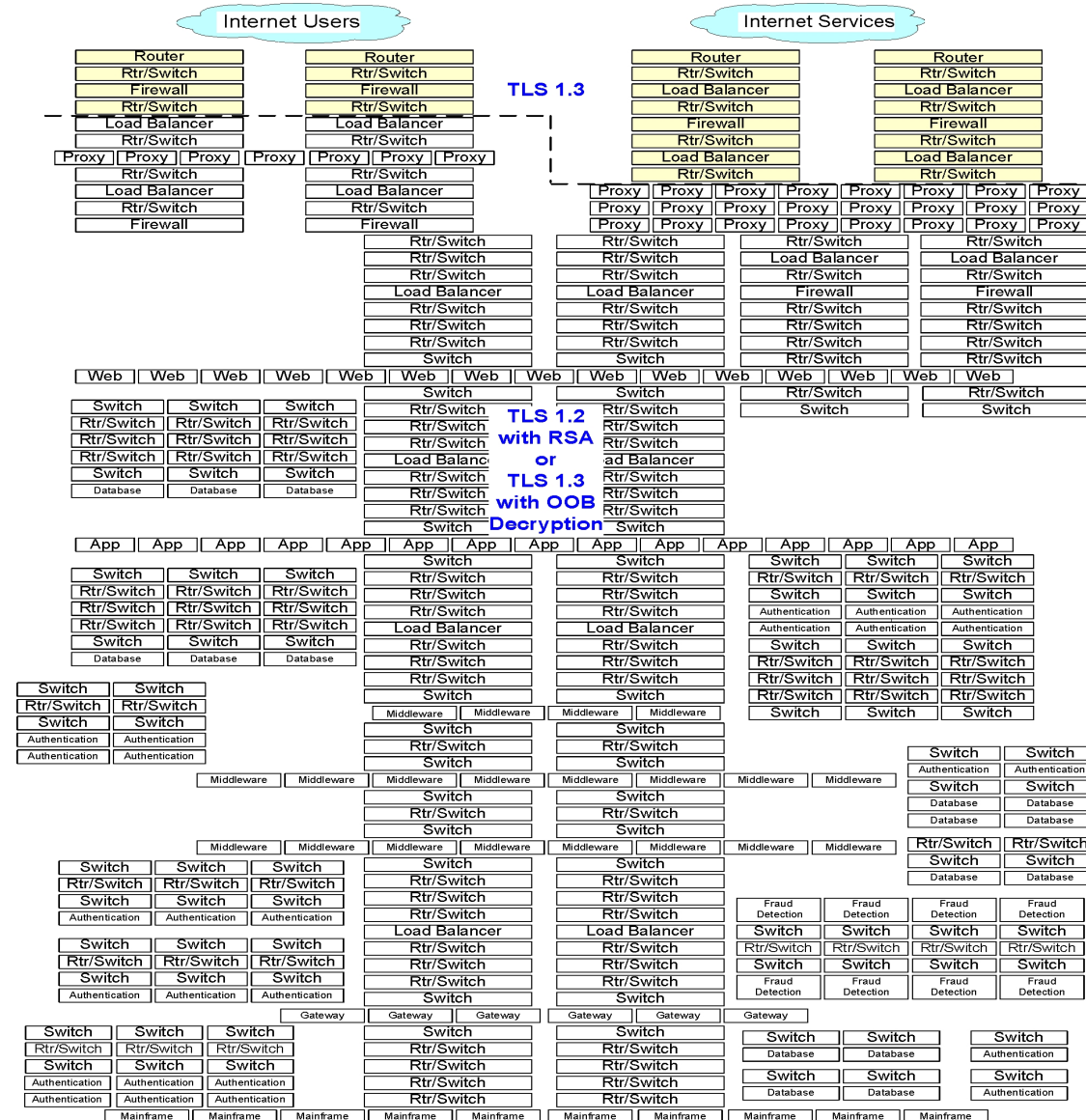
```
FP: 118:      <td class=f32 valign=bottom>Welcome to [REDACTED]
FP: 119:      </tr>\r\n
FP: 120:      <tr>\r\n
3d 22 66 33 22 20 68 65 69 67 68 74 3d 22 32 30 ="f3" height="20
22 3e [REDACTED] 3c 2f 74 64 3e 3c 2f 74 72 3e ">[REDACTED] /td></tr>
20 0d 0a 09 20 20 09 09 09 09 0d 0a 09 20 20 20
09 09 09 09 3c 74 72 3e 0d 0a 09 20 20 09 09
09 09 09 3c 74 64 20 77 69 64 74 68 3d 31 20 68
65 69 67 68 74 3d 31 30 20 63 6f 6c 73 70 61 6e
3d 34 3e 3c 69 6d 67 20 73 72 63 3d 27 2f [REDACTED]
[REDACTED] 53 74 61 61 [REDACTED] Sta
74 69 63 2f 69 6d 61 67 65 73 2f 73 70 61 63 65 tic/images/space
72 2e 67 69 66 27 20 77 69 64 74 68 3d 31 20 68 r.gif' width=1 h
65 69 67 68 74 3d 31 30 20 61 6c 74 3d 22 22 3e eight=10 alt="">
3c 2f 74 64 3e 0d 0a 09 20 20 09 09 09 09 3c 2f </td>...</td>
74 72 3e 0d 0a 09 20 20 09 09 09 09 3c 74 72 3e tr>...<tr>
0d 0a 09 20 20 09 09 09 09 09 3c 74 64 20 77
69 64 74 68 3d 38 20 76 61 6c 69 67 6e 3d 74 6f
20 3e 3c 69 6d 67 20 73 72 63 3d 27 2f [REDACTED]
[REDACTED] 53 74 61 74 [REDACTED] Stat
69 63 2f 69 6d 61 67 65 73 2f 61 72 72 6f 77 5f ic/images/arrow_
72 65 64 32 2e 67 69 66 27 20 76 73 70 61 63 65 red2.gif' vspace
3d 34 20 61 6c 74 3d 22 22 3e 3c 2f 74 64 3e 0d =4 alt=""></td>
0a 09 20 20 20 09 09 09 09 3c 74 64 20 63 6f ..<td co
6c 73 70 61 6e 3d 33 3e 3c 73 70 61 6e 20 63 6c lspan=3><span cl
61 73 73 3d 66 36 3e 50 61 73 73 77 6f 72 64 3c ass=f6>Password<
69 6d 67 20 73 72 63 3d 27 2f [REDACTED] img src='
[REDACTED] 53 74 61 74 69 63 2f [REDACTED] Static/
69 6d 61 67 65 73 2f 73 70 61 63 65 72 2e 67 69 images/spacer.gi
66 27 20 77 69 64 74 68 3d 34 32 20 68 65 69 67 f' width=42 heig
68 74 3d 31 20 61 6c 74 3d 22 22 3e 3c 2f 73 70 ht=1 alt=""></sp
61 6e 3e 0d 0a 09 20 20 09 09 09 09 3c 61 an>...<a
20 63 6c 61 73 73 3d 66 33 30 20 68 72 65 66 3d class=f30 href=
[REDACTED]
[REDACTED]
26 74 79 70 65 3d 70 61 73 73 77 6f 72 64 26 4c &type=password&L
4f 47 49 4e 41 53 53 49 53 54 41 4e 43 45 46 4c OGINASSISTANCEFL
41 47 3d 54 52 55 45 22 3e 46 6f 72 67 6f 74 20 AG=TRUE">Forgot
70 61 73 73 77 6f 72 64 3f 3c 2f 61 3e 3c 2f 74 password?</a></t
```

[REDACTED]

- 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).

- 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



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

- 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.

