

# Cybersecurity Incident Report

## Section 1: Identify the type of attack that may have caused this network interruption

The network interruption and connection timeout error message on the company's website are likely caused by a Distributed Denial of Service (DDoS) attack rather than a DoS attack. The logs reveal that the web server becomes unresponsive due to the overwhelming influx of SYN packet requests, indicating a form of DDoS attack known as SYN flooding. During this attack, a malicious actor sends an excessive number of SYN packets to the web server, exploiting the TCP handshake process. This overwhelms the server's resources and prevents it from responding to legitimate requests. To address the issue, I have temporarily taken the web server offline to allow it to recover and return to normal operation. Additionally, I have configured the firewall to block the IP address responsible for the abnormal SYN requests. However, it's important to note that this IP blocking solution may not provide long-term protection, as attackers can easily spoof other IP addresses. I recommend promptly alerting our manager about the ongoing DDoS attack, explaining the type of attack (SYN flooding) and its impact on the web server and employees. We should discuss the next steps to mitigate the attack, such as implementing traffic filtering or acquiring DDoS mitigation services to prevent similar incidents from occurring in the future.

## Section 2: Explain how the attack is causing the website malfunction

The website malfunction is caused by a SYN flood attack, which disrupts the TCP handshake process between website visitors and the web server.

Under normal circumstances, when a visitor attempts to establish a connection with the web server, a three-way handshake occurs using the TCP protocol. The handshake involves three steps:

- The visitor sends a SYN packet to the server, initiating the connection request.
- The server responds with a SYN-ACK packet, acknowledging the request and reserving resources for the connection.
- The visitor sends an ACK packet to the server, confirming the acceptance and establishing the connection.

However, in the case of a SYN flood attack, a malicious actor floods the server with an overwhelming number of SYN packets simultaneously, bypassing the completion of the handshake. This flood of SYN packets consumes all available server resources designated for reserving connections, leaving none for legitimate

TCP connection requests.

As a result, the web server becomes overwhelmed and unable to process the visitors' SYN requests. Consequently, when legitimate visitors attempt to establish a connection, they receive a connection timeout message because the server lacks the necessary resources to open new connections.

The logs provide evidence of this overwhelming situation, indicating that the server is unable to handle the flood of SYN packets and resulting in the inability to serve legitimate connection requests.

### Analyzed Network Wireshark TCP/HTTP Log:

No.	Time	Source	Destination	Protocol	Info
47	3.144521	198.51.100.23	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=120... 443->42584 [SYN, ACK] Seq=0 Win=5792 Len=120...
48	3.195755	192.0.2.1	198.51.100.23	TCP	
49	3.246989	198.51.100.23	192.0.2.1	TCP	42584->443 [ACK] Seq=1 Win=5792 Len=120...
50	3.298223	198.51.100.23	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
51	3.349457	192.0.2.1	198.51.100.23	HTTP	HTTP/1.1 200 OK (text/html)
52	3.390692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [SYN, ACK] Seq=0 Win=5792 Len=120...
53	3.441926	192.0.2.1	203.0.113.0	TCP	
54	3.49316	203.0.113.0	192.0.2.1	TCP	54770->443 [ACK] Seq=1 Win=5792 Len=0...
55	3.544394	198.51.100.14	192.0.2.1	TCP	14785->443 [SYN] Seq=0 Win=5792 Len=120... 443->14785 [SYN, ACK] Seq=0 Win=5792 Len=120...
56	3.599628	192.0.2.1	198.51.100.14	TCP	
57	3.664863	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
58	3.730097	198.51.100.14	192.0.2.1	TCP	14785->443 [ACK] Seq=1 Win=5792 Len=120...
59	3.795332	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
60	3.860567	198.51.100.14	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
61	3.939499	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=120...
62	4.018431	192.0.2.1	198.51.100.14	HTTP	HTTP/1.1 200 OK (text/html)
63	4.097363	198.51.100.5	192.0.2.1	TCP	33638->443 [SYN] Seq=0 Win=5792 Len=120... 443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120...
64	4.176295	192.0.2.1	203.0.113.0	TCP	
65	4.255227	192.0.2.1	198.51.100.5	TCP	443->33638 [SYN, ACK] Seq=0 Win=5792 Len=120...
66	4.256159	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
67	5.235091	198.51.100.5	192.0.2.1	TCP	33638->443 [ACK] Seq=1 Win=5792 Len=120...
68	5.236023	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
69	5.236955	198.51.100.16	192.0.2.1	TCP	32641->443 [SYN] Seq=0 Win=5792 Len=120...
70	5.237887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

71	6.228728	198.51.100.5	192.0.2.1	HTTP	GET /sales.html HTTP/1.1
72	6.229638	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->32641 [RST, ACK] Seq=0 Win=5792 Len=120...
73	6.230548	192.0.2.1	198.51.100.16	TCP	
74	6.330539	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
75	6.330885	198.51.100.7	192.0.2.1	TCP	42584->443 [SYN] Seq=0 Win=5792 Len=0...
76	6.331231	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
77	7.330577	192.0.2.1	198.51.100.5	TCP	HTTP/1.1 504 Gateway Time-out (text/html)
78	7.351323	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
79	7.360768	198.51.100.22	192.0.2.1	TCP	6345->443 [SYN] Seq=0 Win=5792 Len=0... 443->42584 [RST, ACK] Seq=1 Win=5792 Len=120...
80	7.380773	192.0.2.1	198.51.100.7	TCP	
81	7.380878	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
82	7.383879	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
83	7.482754	192.0.2.1	203.0.113.0	TCP	
84	7.581629	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
85	7.680504	192.0.2.1	198.51.100.22	TCP	443->6345 [RST, ACK] Seq=1 Win=5792 Len=0...
86	7.709377	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
87	7.738241	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
88	7.767105	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
89	13.895969	192.0.2.1	203.0.113.0	TCP	
90	13.919832	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
91	13.943695	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->32641 [RST, ACK] Seq=1 Win=5792 Len=120...
92	13.967558	192.0.2.1	198.51.100.16	TCP	
93	13.991421	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
94	14.015245	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
95	14.439072	192.0.2.1	203.0.113.0	TCP	
96	14.862899	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
97	14.886727	198.51.100.9	192.0.2.1	TCP	4631->443 [SYN] Seq=0 Win=5792 Len=0...
98	15.310554	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
99	15.734381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
100	16.158208	192.0.2.1	203.0.113.0	TCP	
101	16.582035	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
102	17.005862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
103	17.429678	192.0.2.1	203.0.113.0	TCP	
104	17.452693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
105	17.475708	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
106	17.498723	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
107	17.521738	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

108	17.544753	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
109	17.567768	192.0.2.1	203.0.113.0	TCP	
110	17.590783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
111	18.413795	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
112	18.436807	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
113	18.459819	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
114	18.482831	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
115	18.506655	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
116	18.529667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
117	18.552679	192.0.2.1	203.0.113.0	TCP	
118	18.875692	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
119	19.198705	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
120	19.521718	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
121	19.844731	192.0.2.1	198.51.100.9	TCP	443->4631 [RST, ACK] Seq=1 Win=5792 Len=0...
122	20.167744	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
123	20.490757	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0... 443->54770 [RST, ACK] Seq=1 Win=5792 Len=0...
124	20.81377	192.0.2.1	203.0.113.0	TCP	
125	21.136783	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
126	21.459796	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
127	21.782809	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
128	22.105822	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
129	22.428835	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
130	22.751848	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
131	23.074861	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
132	23.397874	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
133	23.720887	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
134	24.0439	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
135	24.366913	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
136	24.689926	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
137	25.012939	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
138	25.335952	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
139	25.658965	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
140	25.981978	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
141	26.304991	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
142	26.628004	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
143	26.951017	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
144	27.27403	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
145	27.597043	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
146	27.920056	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

147	28.243069	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
148	28.566082	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
149	28.889095	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
150	29.212108	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
151	29.535121	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
152	29.858134	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
153	30.181147	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
154	30.50416	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
155	30.827173	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
156	31.150186	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
157	31.473199	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
158	31.796212	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
159	32.119225	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
160	32.442238	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
161	32.765251	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
162	33.088264	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
163	33.411277	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
164	33.73429	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
165	34.057303	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
166	34.380316	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
167	34.703329	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
168	35.026342	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
169	35.349355	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
170	35.672368	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
171	35.995381	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
172	36.318394	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
173	36.641407	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
174	36.96442	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
175	37.287433	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
176	37.610446	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
177	37.933459	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
178	38.256472	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
179	38.579485	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
180	38.902498	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
181	39.225511	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
182	39.548524	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
183	39.871537	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
184	40.19455	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
185	40.517563	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
186	40.840576	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
187	41.163589	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...

188	41.486602	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
189	41.809615	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
190	42.132628	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
191	42.455641	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
192	42.778654	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
193	43.101667	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
194	43.42468	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
195	43.747693	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
196	44.070706	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
197	44.393719	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
198	44.716732	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
199	45.039745	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
200	45.362758	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
201	45.685771	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
202	46.008784	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
203	46.331797	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
204	46.65481	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
205	46.977823	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
206	47.300836	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
207	47.623849	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
208	47.946862	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
209	48.269875	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
210	48.592888	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
211	48.915901	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
212	49.238914	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
213	49.561927	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	49.88494	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.207953	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.530966	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	50.853979	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.176992	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.500005	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...
214	51.823018	203.0.113.0	192.0.2.1	TCP	54770->443 [SYN] Seq=0 Win=5792 Len=0...