A question on the firewall function of the ATS1500A-IP

Introduction

The ethernet connection of the ATS1500A-IP allows for a number of network functions, such as NTP time synchronization, connectivity to the UltraSync cloud and configuration / configuration management with a PC using ethernet.

One of the features of the ATS1500A-IP is a network “firewall”, which can be switched using setting 9.3.n.7. According tot the documentation, if enabled, the ATS1500A-IP firewall will only allow connections from IP addresses that that are configured as “PC-connection” using setting 9.4.1.n.4.

I found that, if enabled, the ATS firewall will also block network traffic from connections the panel itself initiates, such as NTP, UltraSync (and perhaps a PAC IP connection, I don’t have one to try this). Because of that, the ATS firewall is perhaps not as effective as it can be and hence my question.

My setup

For this question, I have configured the panel (running MR4.10, but the problem is also seen on MR4.8) as described below.
I have configured public DNS/NTP servers to make reproduction of the issue easier.

```
IP address: 192.168.178.8
Netmask:    255.255.255.240
Gateway:    192.168.178.1

NTP server: 193.79.237.14
DNS server: 8.8.8.8
ATS8500 PC: 192.168.178.4
```

Operation without firewall

Without firewall, the panel works as expected.

When connected by the ATS8500 downloader, the panel accepts a connection and allows the downloader to work:

```
16:27:06.074576 IP 192.168.178.4.49854 > 192.168.178.8.32000: Flags [S], seq 2359558971, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:27:06.075537 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [S.], seq 6510, ack 2359558972,
win 2920, options [mss 1460], length 0
16:27:06.076414 IP 192.168.178.4.49854 > 192.168.178.8.32000: Flags [.], ack 1, win 8192, length 0
16:27:06.251424 IP 192.168.178.4.49854 > 192.168.178.8.32000: Flags [P.], seq 1:11, ack 1, win 8192,
length 10
16:27:06.253957 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [.], ack 11, win 2910, length 0
16:27:06.255874 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [P.], seq 1:94, ack 11, win
2910, length 93
16:27:06.299437 IP 192.168.178.4.49854 > 192.168.178.8.32000: Flags [P.], seq 11:21, ack 94, win
8099, length 10
16:27:06.303621 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [.], ack 21, win 2900, length 0
16:27:06.306492 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [P.], seq 94:121, ack 21, win
2900, length 27
16:27:06.308900 IP 192.168.178.4.49854 > 192.168.178.8.32000: Flags [P.], seq 21:31, ack 121, win
8072, length 10
16:27:06.312959 IP 192.168.178.8.32000 > 192.168.178.4.49854: Flags [.], ack 31, win 2890, length 0
```

The panel does a NTP request/response every 20 minutes, and if the panel clock was deliberately set incorrectly, NTP will adjust / correct the time on the panel to match the NTP time:

```
16:17:37.558266 IP 192.168.178.8.49153 > 193.79.237.14.123: NTPv4, Client, length 48
16:17:37.568162 IP 193.79.237.14.123 > 192.168.178.8.49153: NTPv4, Server, length 48
```

When enabling Ultrasync, the panel will DNS-lookup the Ultrasync servers using the 8.8.8.8 DNS servers to find the IP address of the servers and then make a connection:

```
16:27:56.165531 IP 192.168.178.8.24619 > 8.8.8.8.53: 11980+ A? at1.ultraconnect.com. (38)
16:27:56.177766 IP 8.8.8.8.53 > 192.168.178.8.24619: 11980 1/0/0 A 34.247.100.105 (54)
16:27:56.189262 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [S], seq 6705, win 2920, options
[mss 1460], length 0
16:27:56.216882 IP 34.247.100.105.443 > 192.168.178.8.63790: Flags [S.], seq 505421703, ack 6706,
win 17922, options [mss 1452], length 0
16:27:56.219869 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [.], ack 1, win 2920, length 0
16:27:56.223366 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [P.], seq 1:78, ack 1, win 2920,
length 77
16:27:56.250084 IP 34.247.100.105.443 > 192.168.178.8.63790: Flags [.], ack 78, win 17922, length 0
16:27:56.250510 IP 34.247.100.105.443 > 192.168.178.8.63790: Flags [P.], seq 1:25, ack 78, win
17922, length 24
16:27:56.252293 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [.], ack 25, win 2896, length 0
16:27:56.253963 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [P.], seq 78:155, ack 25, win
2896, length 77
16:27:56.281787 IP 34.247.100.105.443 > 192.168.178.8.63790: Flags [P.], seq 25:77, ack 155, win
17922, length 52
16:27:56.282797 IP 192.168.178.8.63790 > 34.247.100.105.443: Flags [.], ack 77, win 2844, length 0
```

This is all as expected and correct.

Operation with firewall enabled

With the firewall enabled, things change.

If the ATS8500 downloader PC is not configured as “PC connection”, then the panel correctly ignores the connect requests:

```
16:41:31.052276 IP 192.168.178.4.49930 > 192.168.178.8.32000: Flags [S], seq 3460915123, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:41:32.062939 IP 192.168.178.4.49930 > 192.168.178.8.32000: Flags [S], seq 3460915123, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:41:34.063794 IP 192.168.178.4.49930 > 192.168.178.8.32000: Flags [S], seq 3460915123, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:41:38.063797 IP 192.168.178.4.49930 > 192.168.178.8.32000: Flags [S], seq 3460915123, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:41:46.078829 IP 192.168.178.4.49930 > 192.168.178.8.32000: Flags [S], seq 3460915123, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
```

When the ATS8500 PC is added as allowed PC connection (IP 192.168.178.4, port 32000), then the panel correctly accepts connect requests:

```
16:50:22.831335 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [S], seq 2895902663, win 8192,
options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
16:50:22.831952 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [S.], seq 8052, ack 2895902664,
win 2920, options [mss 1460], length 0
16:50:22.832833 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [.], ack 1, win 8192, length 0
16:50:22.854587 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [P.], seq 1:11, ack 1, win 8192,
length 10
16:50:22.857093 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [.], ack 11, win 2910, length 0
16:50:22.858972 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [P.], seq 1:94, ack 11, win
2910, length 93
16:50:22.863135 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [P.], seq 11:21, ack 94, win
8099, length 10
16:50:22.867185 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [.], ack 21, win 2900, length 0
16:50:22.870013 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [P.], seq 94:121, ack 21, win
2900, length 27
16:50:22.871314 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [P.], seq 21:31, ack 121, win
8072, length 10
16:50:22.876862 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [.], ack 31, win 2890, length 0
16:50:22.878732 IP 192.168.178.8.32000 > 192.168.178.4.49974: Flags [P.], seq 121:132, ack 31, win
2890, length 11
16:50:22.938427 IP 192.168.178.4.49974 > 192.168.178.8.32000: Flags [.], ack 132, win 8061, length 0
```

So far so good. However, other functions no longer work.

For instance, while NTP requests are still sent and responses received, **the panel does not adjust a deliberately incorrectly-set time and seems to ignore the NTP responses** (note that the packets look the same as the previous example, but on the UI display, the time certainly doesn’t update!):

```
16:52:37.262787 IP 192.168.178.8.49153 > 193.79.237.14.123: NTPv4, Client, length 48
16:52:37.272291 IP 193.79.237.14.123 > 192.168.178.8.49153: NTPv4, Server, length 48
```

Also, when enabling Ultrasync, the panel will do DNS requests over and over, and while responses are sent with the IP address of the server to connect, **the panel seems to ignore the DNS responses to it’s own DNS queries and will not initiate a connection to the Ultrasync servers:**

```
16:55:36.021616 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:36.033875 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:36.423775 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:36.436067 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:37.424777 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:37.433897 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:39.424729 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:39.436916 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:43.426707 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:43.444244 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
```

```
16:55:44.426688 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:44.438661 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:46.427670 IP 192.168.178.8.35741 > 8.8.8.8.53: 36793+ A? at1.zerowire.com. (34)
16:55:46.436537 IP 8.8.8.8.53 > 192.168.178.8.35741: 36793 1/0/0 A 54.194.13.93 (50)
16:55:52.021540 IP 192.168.178.8.4234 > 8.8.8.8.53: 30249+ A? at1.ultraconnect.com. (38)
16:55:52.033666 IP 8.8.8.8.53 > 192.168.178.8.4234: 30249 1/0/0 A 34.247.100.105 (54)
16:55:52.430636 IP 192.168.178.8.4234 > 8.8.8.8.53: 30249+ A? at1.ultraconnect.com. (38)
16:55:52.442819 IP 8.8.8.8.53 > 192.168.178.8.4234: 30249 1/0/0 A 34.247.100.105 (54)
16:55:53.431622 IP 192.168.178.8.4234 > 8.8.8.8.53: 30249+ A? at1.ultraconnect.com. (38)
16:55:53.443359 IP 8.8.8.8.53 > 192.168.178.8.4234: 30249 1/0/0 A 34.247.100.105 (54)
16:55:55.432577 IP 192.168.178.8.4234 > 8.8.8.8.53: 30249+ A? at1.ultraconnect.com. (38)
16:55:55.441452 IP 8.8.8.8.53 > 192.168.178.8.4234: 30249 1/0/0 A 34.247.100.105 (54)
```

I have done some more experiments. One was to add the IP addresses of the DNS server, NTP server and Ultrasync rendez-vous servers as “PC-connections”. That would be incorrect because the Port parameter of the “PC connection” would be the port number on the panel, which in case of an outgoing (NTP, DNS, Ultrasync) connection would be dynamically allocated. But I tried 123 (NTP), 53 (DNS) and 443 (HTTPS).
In any case, that doesn’t solve the problem, which frankly is not totally unexpected.

As a second experiment, I left the Port parameter at 0 (zero), configuring just the IP address in the “PC connections” menu, but again that didn’t work.

Discussion

It seems that the firewall feature as built in the ATS1500A/IP firmware may not work as perhaps expected.

Comparing the functionality to the firewall in well-known IP-to-home routers (ADSL, VDSL, fiber, DOCSIS), in the latter case outgoing connections from home to the internet are always allowed but to allow incoming connections they need to be explicitly configured.
However, the ATS1500A/IP firewall does not seem to cater for outgoing connections that are initiated by the panel itself, and hence those outgoing connections fail if the firewall is enabled. And I’m not sure how to configure the ATS firewall to allow for these connections.

Those connections would include a connection to a PAC via IP. I did not try this, but I expect this connection to (also) fail.

Adding functionality to add filtering of the allowed IP addresses of outgoing connections is probably ill advised, because the IP addresses of the Ultrasync servers then also need to be configured in customer’s panels and then no longer can change (currently, the servers are located by DNS hostnames and hence the IP address of the servers can change).
But adding functionality to always allow a connection that is initiated from the panel would be beneficial because then the ATS firewall can be used to filter incoming network connections to the panel.

When asking my supplier, I was told that for them normally the firewall is left switched off. That results in an installation that functions, however it means the additional security of the firewall in the panel is not used.

And hence my question. I am surprised that the ATS firewall doesn’t seem to cater for connections initiated by the same ATS panel, and wonder if I am doing something wrong, or if the panel firmware perhaps can be improved by adding functionality to allow outgoing connections initiated by the same panel.

Am I perhaps doing something wrong?