SonicWall firewall 6.1/6.2 and above to block LM communication due to "content filtering" on HTML

KB0016964

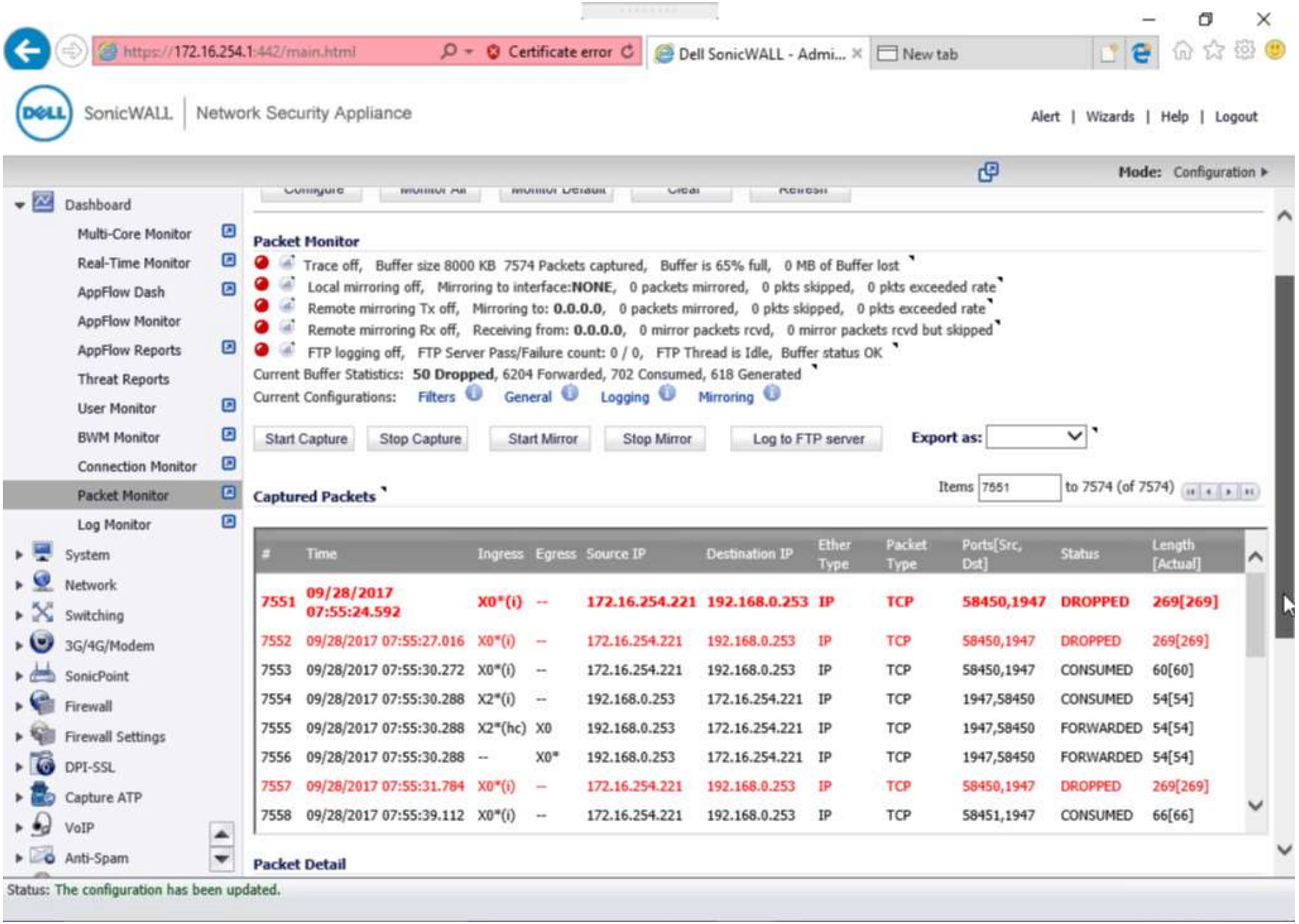
Issue aspect and footprints

Some recent firewalls from SonicWall are blocking the communication from LDK Admin License Manager regardless of the platform.

The first handshake among LDK API and License Manager is done properly; however, as soon as the API and the License Manager start exchanging data, the packets are blocked/dropped by the firewall.

This occurs because the Admin License Manager and LDK API embed some HTML data into TCP/UDP protocols and, at the same time, some versions of SonicWall firewalls have HTML filtering active (Gemalto can't exclude that other firewall products will have similar default settings).

Regarding SonicWall only, dropped packets should be logged into SonicWall Packet Monitor, like in the below image:


https://172.16.254.1:442/main.html
Certificate error
Dell SonicWALL - Admi...
New tab
SonicWALL | Network Security Appliance
Alert | Wizards | Help | Logout
Mode: Configuration
Dashboard
Multi-Core Monitor
Real-Time Monitor
AppFlow Dash
AppFlow Monitor
AppFlow Reports
Threat Reports
User Monitor
BWM Monitor
Connection Monitor
Packet Monitor
Log Monitor
System
Network
Switching
3G/4G/Modem
SonicPoint
Firewall
Firewall Settings
DPI-SSL
Capture ATP
VoIP
Anti-Spam
Packet Monitor
Trace off, Buffer size 8000 KB 7574 Packets captured, Buffer is 65% full, 0 MB of Buffer lost
Local mirroring off, Mirroring to interface:NONE, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Tx off, Mirroring to: 0.0.0.0, 0 packets mirrored, 0 pkts skipped, 0 pkts exceeded rate
Remote mirroring Rx off, Receiving from: 0.0.0.0, 0 mirror packets rcvd, 0 mirror packets rcvd but skipped
FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer status OK
Current Buffer Statistics: 50 Dropped, 6204 Forwarded, 702 Consumed, 618 Generated
Current Configurations: Filters General Logging Mirroring
Start Capture
Stop Capture
Start Mirror
Stop Mirror
Log to FTP server
Export as:
Captured Packets
Items 7551 to 7574 (of 7574)
Time Ingress Egress Source IP Destination IP Ether Type Packet Type Ports[Src, Dst] Status Length [Actual]
7551 09/28/2017 07:55:24.592 X0*(i) -- 172.16.254.221 192.168.0.253 IP TCP 58450,1947 DROPPED 269[269]
7552 09/28/2017 07:55:27.016 X0*(i) -- 172.16.254.221 192.168.0.253 IP TCP 58450,1947 DROPPED 269[269]
7553 09/28/2017 07:55:30.272 X0*(i) -- 172.16.254.221 192.168.0.253 IP TCP 58450,1947 CONSUMED 60[60]
7554 09/28/2017 07:55:30.288 X2*(i) -- 192.168.0.253 172.16.254.221 IP TCP 1947,58450 CONSUMED 54[54]
7555 09/28/2017 07:55:30.288 X2*(hc) X0 192.168.0.253 172.16.254.221 IP TCP 1947,58450 FORWARDED 54[54]
7556 09/28/2017 07:55:30.288 -- X0* 192.168.0.253 172.16.254.221 IP TCP 1947,58450 FORWARDED 54[54]
7557 09/28/2017 07:55:31.784 X0*(i) -- 172.16.254.221 192.168.0.253 IP TCP 58450,1947 DROPPED 269[269]
7558 09/28/2017 07:55:39.112 X0*(i) -- 172.16.254.221 192.168.0.253 IP TCP 58451,1947 CONSUMED 66[66]
Packet Detail
Status: The configuration has been updated.

Solution

On September 28th 2017, SonicWall Technical Support informed users that only firewall versions 6.1, 6.2, or above have HTML content filtering active by default.

These filters can be disabled into the proper menu under Security Services, Content filter, CFS Policies.

To be exact, SonicWall technical support instructed users to disable the following three options:

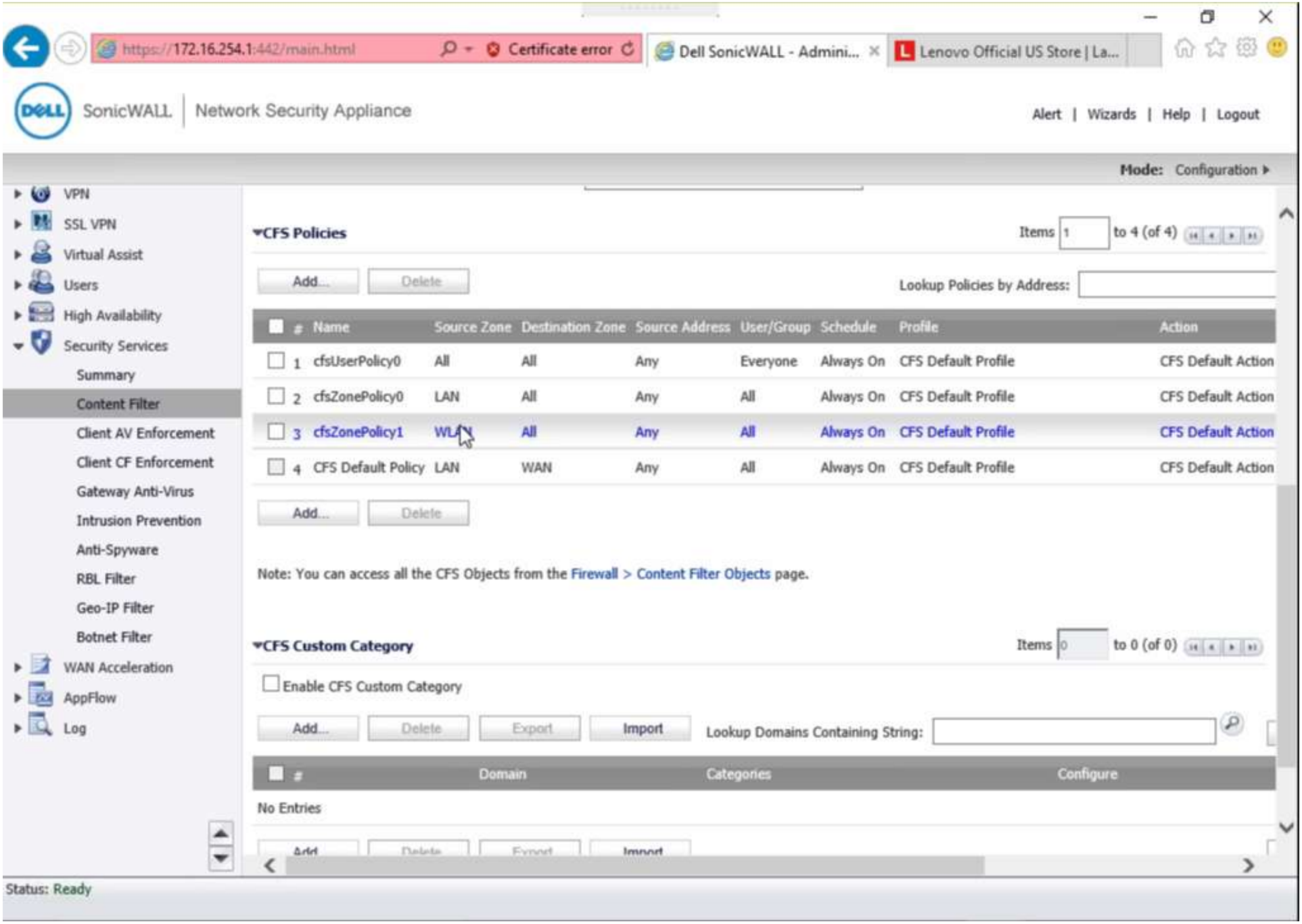
- cfsUserPolicy0
- cfsZonePolicy0
- cfsZonePolicy1

This solved the problem all times that the issue occurred until the date this article was created.

Please see the image below to better identify where the options are located.

Notes:

- SonicWall might have changed the GUI layout since September 28, 2017.
- Gemalto has no exact information on what these filters are meant to achieve and Gemalto is unaware of security side-effects (apart from that our License Manager HTML communication was allowed).
- Gemalto cannot assist on SonicWall product configuration. Screenshots and details related to SonicWall products are given from a real use case with 6.1 and 6.2 firewalls but are meant to be an example only. Please consult with SonicWall directly if assistance is required to disable HTML filtering.


https://172.16.254.1:442/main.html
Certificate error
Dell SonicWALL - Admini...
Lenovo Official US Store | La...
SonicWALL | Network Security Appliance
Alert | Wizards | Help | Logout
Mode: Configuration
VPN
SSL VPN
Virtual Assist
Users
High Availability
Security Services
Summary
Content Filter
Client AV Enforcement
Client CF Enforcement
Gateway Anti-Virus
Intrusion Prevention
Anti-Spyware
RBL Filter
Geo-IP Filter
Botnet Filter
WAN Acceleration
AppFlow
Log
CFS Policies
Items 1 to 4 (of 4)
Add... Delete
Lookup Policies by Address:
Name Source Zone Destination Zone Source Address User/Group Schedule Profile Action
1 cfsUserPolicy0 All All Any Everyone Always On CFS Default Profile CFS Default Action
2 cfsZonePolicy0 LAN All Any All Always On CFS Default Profile CFS Default Action
3 cfsZonePolicy1 WLAN All Any All Always On CFS Default Profile CFS Default Action
4 CFS Default Policy LAN WAN Any All Always On CFS Default Profile CFS Default Action
Add... Delete
Note: You can access all the CFS Objects from the Firewall > Content Filter Objects page.
CFS Custom Category
Items 0 to 0 (of 0)
Enable CFS Custom Category
Add... Delete Export Import
Lookup Domains Containing String:
Domain Categories Configure
No Entries
Add Delete Export Import
Status: Ready