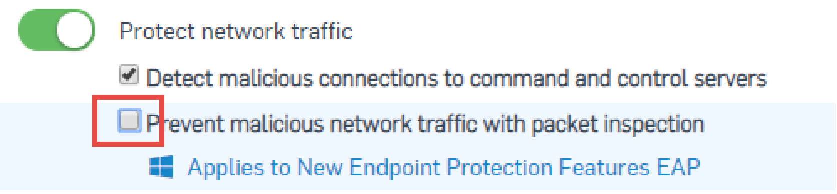
Known Issues List for AMSI and IPS EAP

Date: 20 January 2020

Enhanced Protection EAP with AMSI and IPS.

Endpoint

(See further for Server)

Issue	Details	Notes
[Update][AMSI] No detections for .NET assemblies	In order to mitigate an issue where AMSI incorrectly identifies certain applications as threats, detections for .NET assemblies have temporarily been disabled.	All endpoints have been updated with the fix, so detection for .NET assemblies has been enabled again.
[Update] [IPS] On some devices the Wi-Fi adapter has issues connecting	Certain devices with IPS have issues with the Wi-Fi network adapter. Connections can be made, but are interrupted after a few minutes. Network connections with ethernet cables are not affected. To mitigate the issue disable the IPS setting for those machines:  Protect network traffic ☑ Detect malicious connections to command and control servers □ Prevent malicious network traffic with packet inspection Applies to New Endpoint Protection Features EAP	The January EAP update to Core Agent 2.5.5 BETA should solve this issue.
[UPDATE] [IPS] Device shows “Bad Health	After joining the Early Access Program (EAP) for Enhanced Protection/ IPS and AMSI, the endpoint may report a Bad health state due to Sophos Snort service not starting until after a reboot.	See also this post.

State” after client installation	A reboot is required to complete the install of the new IPS and AMSI components. This will be fixed in the next release of the Core Agent in November 2019.	This issue has been solved with the release containing Core Agent 2.5.4 BETA in the beginning of December 2019
[IPS] IPS fails to attribute traffic to correct application due to packet modification	When certain applications such as NetBalancer are installed on the endpoint, IPS fails to correctly identify the source application of the malicious traffic. IPS still detects and blocks the malicious traffic, but fails to report the name of the application, nor can it block the application.	

Server

Issue	Details	Notes
[AMSI] AMSI missing on Server Core installations for 32-bit applications	When installing Windows Server 2016 and Windows Server 2019, in Server Core, native Microsoft AMSI support is missing for 32-bit applications.	As Powershell is the most important 32-bit application that should call AMSI, we recommend using AppLocker to disable this instance (for example using %windir%\SysWoW64\WindowsPowerShell\*). Note that this does not mitigates all risks.