ESET Tech Center

Knowledgebase > Legacy > Create IDS rules for client workstations in ESET PROTECT (8.x)

Create IDS rules for client workstations in ESET PROTECT (8.x)

Steef | ESET Nederland - 2020-12-10 - Comments (0) - Legacy

Solution

Create IDS exclusions in ESET PROTECT

- 1. <u>Open ESET PROTECT Web Console</u> in your web browser and log in.
- Click Policies → ESET Endpoint for Windows, then click the ellipses next to the policy you want to edit and click Edit.

ese	PROTECT		
==		Policies	ACCESS GROUP Select 🖀 SHOW UNASSIGNED 💟 🔯 ESET Endpoint for
G		Policies	NAME POLICY PRODUCT TAGS
	DTITICIIONS Reports Tasks Installers Pakcies Notifications Status Overview More	 Al ✓ Cutan Rolcias D. ELT Deport for Windows D. ELT Paragement Apent ✓ Built-Project for Andreid (L*) D. ELT Deport for Medicas (L*) D. ELT Paragement Paragement Apent D. ELT Functions D. ELT Functions for Windows D. ELT Functions for Medicas (L*) D. ELT Management Apent 	Note: Petter Nacional HTTP Proyuesge ESET Engloint for Windows Actions ESET Engloint for Windows Boots ESET Engloint for Windows Boots ESET Engloint for Windows Actions ESET Engloint for Windows Actions ESET Engloint for Windows Actions ESET Engloint for Windows Access Right ESET Engloint for Windows Access Right ESET Engloint for Windows Access Right ESET Engloint for Windows ESET Dynamic Trives Delew ESET Engloint for Windows ESET Dynamic Trives Delew ESET Engloint for Windows ESET Dynamic Trives Delew ESET Engloint for Windows
e	COLLAPSE	This is where you can see the list of your spatied tops and quickly filter them.	ACTIONS TO NEW FOLICY ASSON TO

3. Click Settings → Network Protection → Network attack protection and click Edit next to IDS exceptions.

Subscription Edit Policy Conservats Exist Policy A generone Exist Policy	A administratio
Cut None None ▲ generous Antime Antime	
Cup countries	
Basic ESET Endpoint for Windows Q, Type to sear	
La Repub	
Co Tasia Margo DETICTION (MORE CO E NETWORK ATTACK PROTECTION O • •	
Image: Summary LPOLTI 0 ● f balk hours proteins (50) Image: Constraint of the sum of the s	
Dukies O = + IDS rules Ext	
Non-Access Trace Trace	
P Status Denview	
- More >> With Mod DMA, Co	
TOOLS USER INTERVACE	
Ostra militava. Overson Moor	
UVENDE MODE	
S COLLARS BACK CONTINUE SAVE SAVE CONTINUE	

4. Click Add.

IDS rules						? 🗆 X
The IDS rules are evaluated from top to bo log) separately.	ottom. They can be used to customiz	e firewall behaviour upon various IDS detect	tions. First matching exception is ap	oplied for each ac	ion type (block,	notify,
Detection	Application	Remote IP	Block	Notify	Log	Q
Add Edit Remove			*		•	¥
					Save	Cancel

5. Select the **Alert**, type the **Remote IP address** (IP address of the machine with the software that scans the network).

Alternatively, to set up an IDS exclusion for a locally installed application, type the full path to the .exe file in **Application** (e.g. C:\Windows\system32\cmd.exe).

6. In the Action section, select No from each drop-down menu. Click $OK \rightarrow Save \rightarrow Finish$ to save the policy. If this is a new policy, assign the policy to the correct groups. After the computers check in, they will get the policy change.

Add IDS rule			? 🗆 X
Detection		Any alert	×
Threat name	(@ ≥ 6.6	-	
Direction	(Both	~
Application			
	5	192.168.1.5	
Remote IP address			0
Profile		Any profile	~
ACTION			
Block		No	~
Notify	6	No	~
Log	_	No	~
			ОК