ESET Tech Center

Kennisbank > 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 - Reacties (0) - Legacy

Solution

Create IDS exclusions in ESET PROTECT

- 1. Open ESET PROTECT Web Console 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.

(CS e	PROTECT		
		Policies	ACCESS GROUP Select 🖹 SHOW UNASSONED 💟 DJ EST Endpoint for (14) Tapin
돠		Policies A	NAME POLICY PRODUCT TAGS
▲ 3 8 8 8 9 × 1	DTITCHONS Reports Tasks Installers Policies Status Overview More	Au Au Cuton Rolices Di EST Endpoint for Windows Di EST Endpoint for Windows Di EST Endpoint for Andrea (2+) Di EST Endpoint for Andrea (2+) Di EST Endpoint for Microsoft Sci Di EST Endpoint for Microsoft Sci Di EST Mail Security for Microsoft Sci Di EST Management Agent	Note: POLIC I Moderal HTTP Program ESET Endpoint for Windows Actions ESET Endpoint for Windows Boarde ESET Endpoint for Windows Charge Augment ESET Endpoint for Windows Actions (Acting Augment ESET Endpoint for Windows Actions Rights ESET Endpoint for Windows
c	COLLAPSE	Dis is where you can see the lat of your spatied togs and quickly filter them.	ESET Dynamic Threat Defe. ESET Engount for Windows Actions: * NEW POLICY

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

(65)01	PROTECT				Q Computer Name	QUICK LINKS * O HELP *	A ADMINISTRATOR
		Edit Policy					
Gð		Policies > Antivirus - Balanced					
▲		Basic	ESET Endpoint for Windows			Q. Type to search	
~		Settings	DETECTION ENGINE	NETWORK ATTACK PROTECTION		0	
6		Assign	UPDATE	O ⊕ ∮ Enable Network attack protection (IOS)		0	
۲	Policies		NETWORK PROTECTION	O ⊕ ∲ Enable Botnet protection O ⊕ ∲ IDS nules	Est	0	
¢			Preval Network attack protection	ADVANCED OPTIONS	-	0.0 # 0	
			WEB AND EMAL				
			DEVICE CONTROL				
			USER INTERFACE				
			OVERRIDE MODE				
		-					
න			BACK CONTINUE FINISH	SAVE AS CANCEL			

4. Click Add.

I	IDS rules						? 🗆 X
	The IDS rules are evaluated from top to bottom. They can be used to customize firewall behaviour upon various IDS detections. First matching exception is applied for each action type (block, no log) separately.						
	Detection	Application	Remote IP	Block	Notify	Log	Q
	Add Edit Remove			4			¥
						Save	Lancei

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).

In the Action section, select No from each drop-down menu. Click OK → Save →
 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		au alast	
Detection		ny alert	<u> </u>
Threat name	(@ ≥ 6.6		
Direction	Bo	oth	~
Application			
Remote IP address	3 19	12.168.1.5	•
Profile	Ar	ny profile	~
ACTION	_		_
Block		io	~
Notify	(6)	o	~
Log	Ne	lo	~
		<u> </u>	- 1
		\sim	ОК