Update Firewall Rules on the Endpoint

Create Date: Author: September 13, 2013 Cammi Derr Last saved: Last saved by:

9/17/2013 Cammi Derr

Overview:

The information provided in this document describes the process used to allow firewall exceptions for remote access and ping capabilities for applications on a local endpoint.



Update Firewall Rules on the Endpoint

Create Date: Author: September 13, 2013 Cammi Derr Last saved: Last saved by: 9/17/2013 Cammi Derr

5. Click the Network Packet Rules tab	Frewall Vetwork packet rules Metwork packet rules Configure network packet rules Kaspersky Endport Security 10 for Windows montors ribound and outbound network activities by using network packet indices reate 10 yeld fault. You can create a new set of conditions and actions to take on network packets and data streams by adding or edimg network packet rules. Image: Add C Edit Delete More was Move down Address Requests to DNS server over TOP Sending emails Of Any network activity Any network activity Image: Adv and the packet of the p		
 Select Remote Desktop network activity if it contains a and click Edit Click Allow. Click OK. 	Network rule × Action: Allow • Name: Remote Desktop network activity • Ø Protocol: TCP • Direction: Inbound • Remote ports: • • Local ports: 3389 • Address: Any address • Help OK Cancel		
 9. Select Incoming ICMP stream if it contains a and click Edit 10. Click Allow. 11. Click OK. 	Network rule × Action: Allow ▼ Name: Incoming ICMP stream • Ø Protocol: ICMP ▼ Direction: Inbound (packet) ▼ I CMP type: Echo Reply ▼ I CMP code: code 0 ▼ Address: Any address ▼ Help OK Cancel		

\\ctis\dfsroot\archive\documentation\kaspersky\Kaspersky_AllowExecution_EUInstructions.docx

Update Firewall Rules on the Endpoint

Create Date:	September 13, 2013	Last saved:	9/17/2013			
Author:	Callini Dell	Last saved by:	Camini Den			
12. Click	OK when all items have bee	n edited, 🛛 🙀	wall			
there will be green check marks.						
			Application control rules inerviolic packet rules inerviolic			
			Configure network packet rules Kaspersky Endpoint Security 10 for Windows monitors inbound and outbound network activities by using network packet rules created by default. You can create a new set of conditions and actions to take on network packets and data streams by adding or editing network packet rules.			
			🕂 Add 🖉 Edit 💥 Delete 🗌	Move up 🛛 🕹 Move down	Additional	
		100	Network servic	ce 🕂 Permission	Address E 🔺	
			Requests to DNS server over ICP	•••		
			Sending e-mails	₩		
			Any network activity	✓	Trusted networks	
			Any network activity	₩	Local networks	
			Remote Desktop network activity TCP connections through local ports	v		
ł			UDP connections through local ports	ő	=	
			Incoming TCP stream	₩		
			Incoming UDP stream	•		
			ICMP Destination Unreachable incomin	ng responses		
			ICMP Ecro Reply incoming packets	ses 🗸		
			Incoming ICMP stream	×		
			ICMPv6 Echo Request incoming packe	ts Ø		
			 allowed () - blocked I - process 	according to the application rule		
		telp			OK <u>C</u> lose	
14 Click	Save					
14. CIICK		K	aspersky	KSN Reputation Service	_ ×	
15. Whe	en both the Save and Cancel l	outtons	Endpoint Security 10	1	Reports 🚱 Quarantine	
are	araved out you may close the	- f	or Windows			
			ataction and Control	CTIS\derrcammi. v	ou are working under a policy 🛱	
Казр	ersky Settings window.	PI	otection and control	Settings		
			Endpoint control	📝 Start Kaspersky Endpoint Security 10 for Windows of	on computer startup	
			File Anti-Virus	Enable Advanced Disinfection technology		
			Mail Anti-Virus	Detection of the following object types is enable	led:	
			Web Anti-Virus	- Viruses, worms, Trojans, and malicious tools		
			IM Anti-Virus Eirewall	- Adware and auto-dialers		
			Network Attack Blocker	- Packed files that may cause harm, and multi-packed fi	les	
			System Watcher	Settings		
			Scheduled tasks	– Exclusions and trusted applications		
		2	Advanced Settings	Rules: 10 (total 10)	Settings	
				Trusted applications: 9 (total 9)		
				- Monitored ports		
				Monitor <u>all</u> network ports Monitor <u>only</u> selected ports	Settings	
					Save Cancel	
		Hol	n Sunnort License			
		, Hei	p Support License			