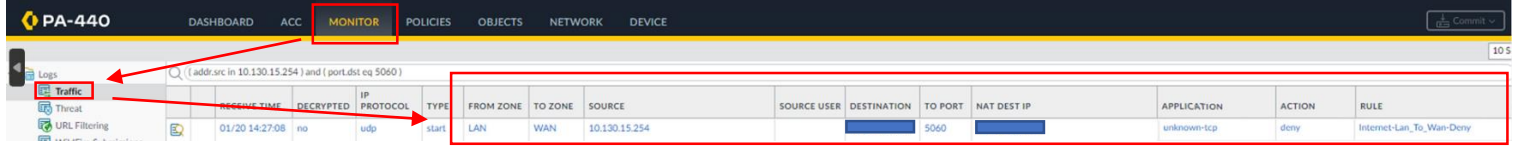


Cihazımı ilk olarak açtığımda “MONITOR” sekmesinden “Traffic” seçeneğine geliyorum.

Arama kısmına (addr.src in 10.130.15.254) and (port.dst eq 5060) ilgili cihazınım local ip adresi ve santralimin iletişim için kullandığı port numarasını yazıyorum.

Hangi kuralın “Deny” verdiğini denetliyorum.



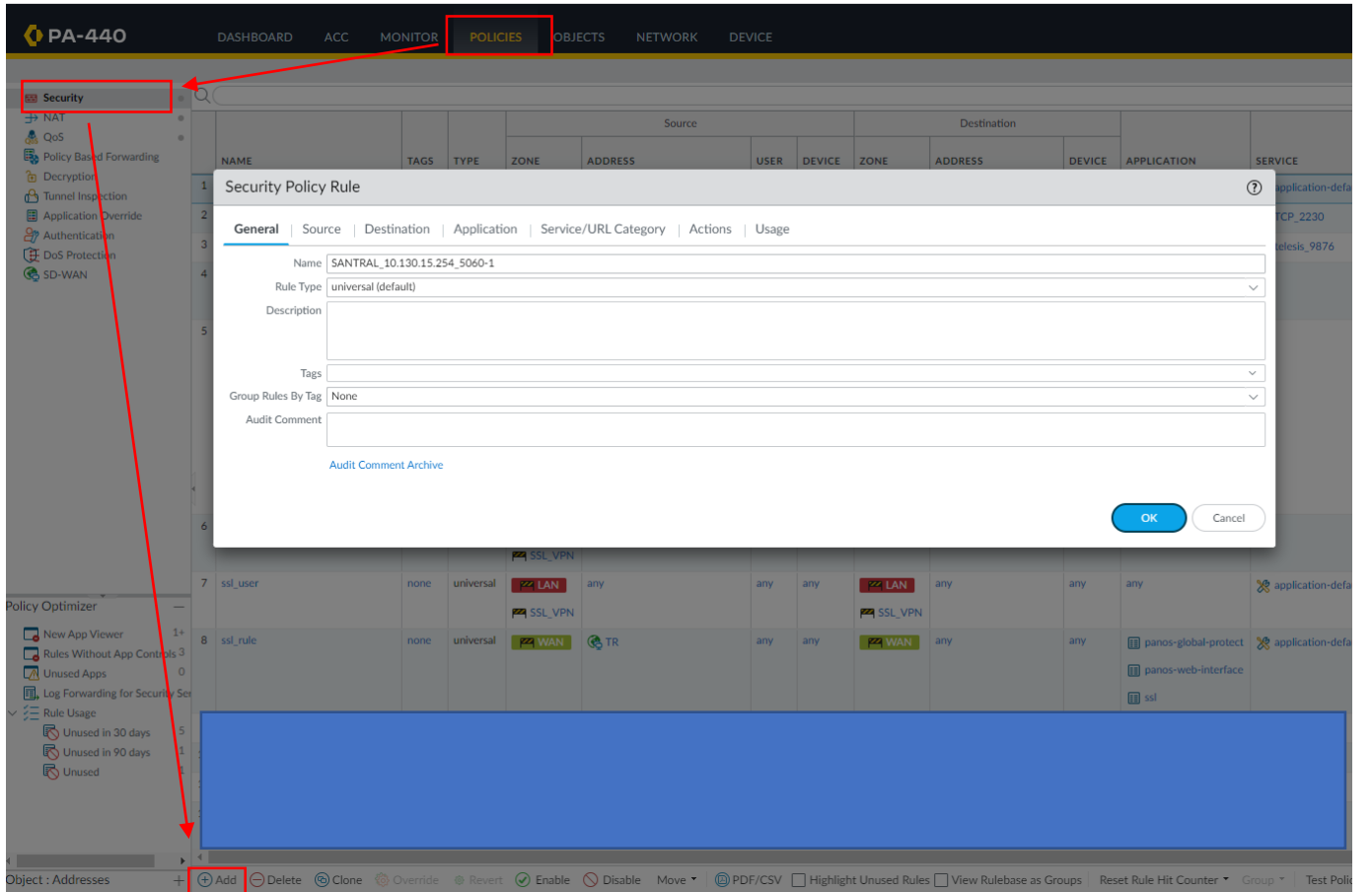
LOGS	SEARCH	ASSIGNED TIME	DECRYPTED	IP	PROTOCOL	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	NAT DEST IP	APPLICATION	ACTION	RULE
105	(addr.src in 10.130.15.254) and (port.dst eq 5060)	01/20 14:27:08	no	udp	start		LAN	WAN	10.130.15.254		5060			unknown-tcp	deny	Internet-Lan_To_Wan-Deny

Artık sorunumuzun ne olduğunu anladığımıza göre çözüme geçebiliriz.

İstisnasız tüm firewall cihazlarında hiyerarşi üstten başlar yani en yukarıdaki kural ilk çalışandır.

Bu nedenle 5060 nolu portuma doğru Palo Alto cihazımda bir kural yazacağım.

Firewall Arayüzden “POLICIES” sekmesine ve oradan “Security” seçeneğine gelip “Add” diyerek yeni bir kural oluşturuyorum.



PA-440 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Security

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: SANTRAL_10.130.15.254_5060-1

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

Audit Comment Archive

OK Cancel

Object: Addresses

Add Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy

Karşıma gelen ekrandan "General" sekmesinde kuralıma isim veriyorum.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: SANTRAL_10.130.15.254_5060-1

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

Audit Comment Archive

OK Cancel

Aynı ekrandan "Source" sekmesine geliyorum. Sekmeden zone seçiyorum. Ben iç networkden internete doğru bir kural yazacağım için kaynak networkümü "LAN" olarak seçiyorum. Ayrıca Sadece "Santral" cihazımın bu kurala tabi olması için "Source Address" kısmında belirtiyorum.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

SOURCE ZONE: LAN

SOURCE ADDRESS: SANTRAL_IP_10.130.15.254

SOURCE USER: any

SOURCE DEVICE: any

Negate

OK Cancel

Aynı ekrandan "Destination" sekmesine geliyorum. "Destination Zone" hedef networkümü wan olarak internete çıkış zonu olarak tanımlıyorum.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

DESTINATION ZONE: WAN

DESTINATION ADDRESS: Any

DESTINATION DEVICE: any

Negate

OK Cancel

Sonraki adımda işin en önemli kısmı bu PALO ALTO firewall da APP ID bazlı bir sistem var.

Bu nedenle 5050 portu palo alto firewall da "Sip" app olarak tanımlanmış.

Add diyerek "sip" servisini seçiyorum.

The screenshot shows the 'Security Policy Rule' configuration page with the 'Application' tab selected. The 'APPLICATIONS' section on the left has a search bar and a list of applications. The 'sip' application is highlighted with a red box. A red arrow points from the 'Add' button at the bottom left to the 'sip' application. Another red arrow points from the 'Add' button to the 'Application' tab header. The 'DEPENDS ON' section on the right is empty. The 'Add To Current Rule' and 'Add To Existing Rule' buttons are at the bottom right. The 'OK' and 'Cancel' buttons are at the bottom right.

Sonraki adımda "Actions" sekmesine geliyorum. Kuralımı devreye almak için "Action" kısmını allow deyip, aynı zamanda logları görmek için log seçeneğimi seçtikten sonra "Ok" diyerek işlemimi tamamliyorum.

The screenshot shows the 'Security Policy Rule' configuration page with the 'Actions' tab selected. The 'Action Setting' section on the left has a dropdown menu set to 'Allow' and a checkbox for 'Send ICMP Unreachable' which is unchecked. The 'Log Setting' section on the right has a checkbox for 'Log at Session Start' which is checked, and a checkbox for 'Log at Session End' which is unchecked. The 'Log Forwarding' dropdown is set to 'None'. The 'Other Settings' section has a 'Schedule' dropdown set to 'None' and a 'QoS Marking' dropdown set to 'None'. The 'Disable Server Response Inspection' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right. Red arrows point from the 'Log at Session Start' checkbox to the 'Log at Session End' checkbox, and from the 'Log at Session End' checkbox to the 'OK' button.

Aşağıda görüldüğü üzere kuralım oluştu ve sıralama en yukarıda.

The screenshot shows the Palo Alto PA-440 dashboard with the 'POLICIES' tab selected. The 'Security Policy Rule' configuration is visible in the table below.

	NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	SANTRAL_10.130.15.254_5060-1	none	universal	LAN	SANTRAL_IP_10.130.15.254	any	any	WAN	any	any	sip	application-default	Allow	none	

İşlem başarılı.

PA-440 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Logs (addr.src in 10.130.15.254) and (port.dst eq 5060) 10 Second

	RECEIVE TIME	DECRYPTED	IP PROTOCOL	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	NAT DEST IP	APPLICATION	ACTION	RULE
01/20 14:27:08	no	udp	start	LAN	WAN	10.130.15.254	SOURCE		5060			sip	allow	SANTRAL_10.130.15.254_5060-1