epati

Dynamic Reports Product: Antikor v2 - Next Generation Firewall Guides



www.epati.com.tr

epati Dynamic Reports



18 different types of report are dynamically displayed and listed here.

- Anti SPAM Reports
- Cluster Reports
- DNS Filter Reports
- Hotspot log
- Ipsec Service Reports
- Package filtering reports
- PPP Debug Logs
- PPP Reports
- AV, Appid, IPS, DOS Logs
- SSH Inspection Reports
- SSH Protection reports
- Traffic Session Reports
- · Virtual cable reports
- Web Access Reports
- Web Server Security Reports
- WF (Web Filtering) Content and Antivirus Scan Reports
- WF (Web Filtering) URL Filter Reports
- Banned Users Reports

Anti Spam Reports	Cluster Reports	DNS Filter Reports
Hotspot Reports	R IPsec Service Logs	Packet Filter Reports
💅 PPP Debug Logs	PPP Reports	AV, AppID, IPS, DoS Logs
SSH Inspection Reports	SSH Protection Reports	Traffic Session Reports
	Web Access Reports	Web Server Security Reports
WF Content and Antivirus Scan Reports	WF URL Filter Reports	Banned Users Reports

Cluster Reports

It reports the situations related to the Cluster and the interfaces in which the situations take place according to history.

uster Reports															
CSV DPDF DXLS	HTML							Reco	rds per Page	50	Show	@ Show / Hide	e ← \$Sorti	ng 🕶 🛛 🔻 i	iltering 🥒
Timestamps € \$ Ø €		Ac 4	tion		Last S ∉≑⊲	tate 9 ->	Pre e	ev State ≑ ≪ →		Desci ∉≑⇒	ription % ->			Details (- \$ ≪ -}	
						4 C 3 3									G
ers can do	wnload	these	repor	ts in cs	sv, pd	f, xls a	and ht	ml forn	nats.						
PP Debug Log	S														Return to Repor
CSV 🕼 PDF 🕅 XLS	HTML							Recor	rds per Page	50	Show	@ Show / Hide	+ \$Sortin	g 🕶 🛛 🔻 Fi	tering 🥒
	Timestamp ∉≑ ⊕ →							Me «	essage ≑ ≪ →						
						11 1 2 2									Gol
ow many ree	cords w	ill be s	shown	n on ea	ich pa	ge after the	he pag 's value	e of the	e value	e is er	ntere	ed and t	the re	gistra	tion
ow many ree tton is pres	cords w sed; Da	ill be s ita is s	showr	n on ea	ich pag ich as	ge after the user	he pag 's value	e of the	e value	e is er Defa	ntere	ed and f	the re	gistra	tion • Return to Report
ow many red itton is pres W, AppID, IPS,	cords w sed; Da DoS Log	ill be s ita is s	showr shown	n on ea	ich pag uch as	ge after the user	he pag 's value •	e of the e is ent	e value ered. (e is er Defa	ntere ult 5	ed and t D.)	the re	gistra 	tion
W many realist Itton is pres	DoS Log	s S	shown shown	n on ea as mu src IP Src ≪≎ Port Ø⇒ ≪≎	t Dst est	ge after the user the user the user the user the user	he pag 's value • •	e of the e is ent e is ent Reco Network Interface €≎ Ø →	e value ered. (^{rds per Page}	e is er Defa Defa Appl0 ⇔≑⊕	ntere ult 5 show Rule ⊕ ⇒	ed and f 0.) ●Show/Hide Description ♦≑®⇒	the re	gistra gistra g∙ ŢF Record ID 4 ≎ ∞	tion E Return to Report

With the Show/Hide button, the columns can be hidden and the hidden columns can be shown again. The upper arrow buttons can also be replaced by the columns.

WF	URL Filter Re	eports							← Retur	n to Reports
∎ CS	/ 🗋 PDF 🕅 XLS	HTML			Records	s per Page 50 Show	Show / Hide ◆ Sorting	· T	Filtering	<i>a</i> c
#	Timestamp	Action	User	Client IP Address	WF Profile	Category	Timestamp	•	•	1
	$\Leftarrow \Leftrightarrow \diamondsuit \Rightarrow$	€ ≑ Ø >	\leftarrow	$\Leftarrow \diamondsuit \diamondsuit \blacklozenge$	$\Leftarrow \Rightarrow \ll \Rightarrow$	$\langle \Rightarrow \Leftrightarrow \Rightarrow$	Action	•	٠	
							👁 User	•	*	
				6C C 3 30			Client IP Address	•	٠	Go 🖉
							WF Profile	+	•	
							@ Category	•	*	
							HTTP Method	+	•	
							@ URL	+	•	

When we click the sort icon in the screenshot below, the entire table will be sorted by the values in the column.

SSH Protection Reports

← Return to Reports

← Return to Reports

🖹 CSV 🔀 PDF	₩XLS ₩HTML	Records per Page 50	Show Show / Hide 🗸 💠 Sorting 🗸 🦉 🖉
#	Timestamp $\Leftrightarrow \Rightarrow \phi \Rightarrow$	Operation € 🖶 🗇 ⇒	IP Address
1	2020-10-09 14:23:38	release	10.2.1.23
2	2020-10-09 14:21:33	block	10.2.1.23
3	2020-10-09 13:51:51	release	10.2.1.23
4	2020-10-09 13:49:46	block	10.2.1.23

SSH Protection Reports

🖹 CSV 🔀 PDF	RXLS BHTML		Records per Page 50 Show / Hide + Sorting + Filtering
#	Timestamp $\Leftrightarrow \Rightarrow \Rightarrow$	Operation ← 📴 Ø →	IP Address
1	2020-10-09 14:21:33	block	10.2.1.23
2	2020-10-09 13:49:46	block	10.2.1.23
3	2020-10-09 14:23:38	release	10.2.1.23
4	2020-10-09 13:51:51	release	10.2.1.23

You can change the column sorting priority with the up and down arrow buttons in the sorting.

SSH Prote	SH Protection Reports]						
🖹 CSV 🔀 PDF	CSV DPDF Dr XLS De HTML Records per Page 50 Show Show/Hide Show														
#	Timestamp	Operation			IP Address		IP Address		IP Address		LE Ope	eration	•	*	Û
	◆ 珪 の ⇒	< 4 ∞ >					J <u>≜</u> Timestamp		•	•					
1	2020-10-09 13:49:46	block			10	.2.1.23									
2	2020-10-09 14:21:33	block			10	.2.1.23									
3	2020-10-09 13:51:51	release			10	.2.1.23									
4	2020-10-09 14:23:38	release			10	.2.1.23									

You can remove the sort filter for the column with buttons with the garbage icon in the sort.

SSH Protection Reports								← Return	n to Rep	ports]							
BCSV BPDF DXLS BHTML Show / Hide+ Show / Hide+ Trittering Image: Comparison of the state o																		
#	Timestamp	Operation IP Address		IP Address		IP Address		IP Address		IP Address		IP Address		ss		*	*	â
	◆ 珪 の ⇒	< 1± ∅ →			4≞ Tim	estamp	•			*	۰							
1	2020-10-09 13:49:46	block			10	.2.1.23												
2	2020-10-09 14:21:33	block			10	.2.1.23												
3	2020-10-09 13:51:51	release			10	.2.1.23												
4	2020-10-09 14:23:38	release			10	.2.1.23												

With the filtering button, you can filter the data in the table according to the specified criteria.

We	b Server Secu	urity Reports							€ Return t	to Reports
	CSV QPDF XXLS RHTML						50 Show	● Show / Hide → Sorting →	▼ Filtering	e 0
#	Timestamp & ≎ Ø ⇒	Client & \$ ⊕ ⇒	$ \ll \ \diamond \ \diamondsuit \ \diamond \ \circ \ \ \circ \ \diamond \ \circ \ \diamond \ \diamond \ \diamond \ \diamond \ \diamond \ \circ \ \ \diamond \ \circ \ \ \ \ \ \ \ \ \ \ \ \ \ $	Request $\Leftrightarrow \Rightarrow \ll \Rightarrow$	Category $\ll \Rightarrow \ll \Rightarrow$	Message ∉ ≑ ⊗ →	Analysis	Severity $\Leftrightarrow \Rightarrow \circledast \Rightarrow$	Tags $\langle\!\!\!\!\!\langle \div \ll \Rightarrow \rangle\!\!\!\!$	
				a c	3 30					Go 🗗

Filtering

Timestamp	🝠 Clear 🔹 Add
(a) 21.03.2023 03:45:08,026	v ! 🧷
Client	Clear + Add
Host	Clear + Add
Request	Clear 🕇 Add
Category	ZClear + Add
Message	Clear + Add
Analysis	Clear + Add
Severity	Clear + Add
Tags	Clear + Add
	Apply

When entering the criteria, you will need to pay attention to the maximum, as it will filter according to the pop - up list next to it.

Filtering			×
Timestamp			🝠 Clear 🕇 Add
21.03.2023 03:57:32,902	•	in Date in Date	¥ ! 🧷
Client		Before Date After Date	er 🕇 Add
Host			🥒 Clear 🕈 Add
Request			Clear + Add
Category			Clear + Add
Message			Clear + Add
Analysis			Clear + Add
Severity			Clear + Add
Tags			Clear + Add
			Apply
Filtering			×
Timestamp			Clear + Add
21.03.2023 03:57:32,902		in Date	¥ ! 🖉
Client			🖉 Clear 🕇 Add
Α	T	Including	¥ ! 🖉
Host		Starting With	ar 🕇 Add
А		Exactly Comma Separa	ted

×

Tags	🥭 Cle	ar 🕇 Add
=	Covered 🗸	1
	Covered	-
	Including	
	Exactly	Apply
	Including	

After the filters required for the table are entered, the Apply Definition button must be pressed.

Filtering		×
Timestamp		🝠 Clear 🕇 Add
	After Date	v ! 🥑
Client		Clear + Add
Host		🥒 Clear 🕈 Add
Request		Clear + Add
Category		Clear + Add
Message		Clear + Add
Analysis		Clear + Add
Severity		Clear + Add
Tags		Clear + Add
=	Covered	¥ ! 🥖
		Apply

To remove the filters made for the table, just click on the button with the eraser icon.

WF	URL Filter Re	ports						← Return to Reports
∎ cs	V 🖾 PDF 🕅 XLS	HTML			Records	per Page 50 Show	Ø Show / Hide → Sorti	ing 🗸 🛛 🕇 Filtering 🥒 🕄
#	$ \begin{array}{c} Timestamp \\ \Leftarrow \Leftrightarrow \oslash \Rightarrow \end{array} $	$ \begin{array}{c} \text{Action} \\ \Leftrightarrow \Leftrightarrow \circledast \twoheadrightarrow \end{array} $	User $\Leftrightarrow \Rightarrow \Rightarrow$	Client IP Address $\Leftrightarrow \Leftrightarrow \diamondsuit \Rightarrow$	WF Profile $\Leftrightarrow \Rightarrow $	$ \begin{array}{c} Category \\ \Leftrightarrow \Leftrightarrow \Leftrightarrow \end{array} \right) \\$	HTTP Method $\ll \Leftrightarrow \ll \Rightarrow$	URL ⊕ ≑ ⊗ ⇒
				« < > »				Go 🖾

To see the newly incoming values to the table, the Refresh button must be pressed.

A	V, AppID,	IPS, D	oS Log	S														•	Return to Reports
	CSV DPDF	₽ XLS	HTML									Rec	ords per Page	50	Show	● Show / Hide ◄	\$ Sorting	g 🕶 🛛 🔻 Filt	tering 🥒 🕄
#	Timestamp & ≎ ⊗ →	Action ∉≎⊚ ⇒	Decision	Protocol ≪ ≎ ⊗ ⇒	Src User ∉≑ ⊗ →	$\begin{array}{c} Src IP \\ \Leftrightarrow \Leftrightarrow \\ \ll \twoheadrightarrow \end{array}$	Src Port ∉≑ ⊗ →	Dst User ∉ ≑ Ø ⋺	Dst IP ∉≎ ⊗ ⇒	Dst Port ∉ ≑ ⊗ →	Service	Network Interface €\$⊕∳	VLAN ≪ ≎ ⊗ ⇒	AppID	Rule ∉≑ ⊗-≯	$ \begin{array}{c} \text{Description} \\ \Leftrightarrow \diamondsuit \twoheadrightarrow \end{array} $	System € \$ Ø ⇒	Record ID ♦ \$ \$ \$	QoS Information ∉ ≑ Ø ⇒
									-K - K	> >									Go 🗗

With the Return to Reports, you can return to the dynamic reports menu and check out other reports

We	eb Acc	ess Repo	rts												← Return	to Reports
	SV 🖾 P	DF 🕅 XLS 🔒	HTML						R	ecords per Page	50	Show	Show / Hide +	♦ Sorting +	▼ Filtering	Ø 0
#	Date Time ∉≑≪ →	Client IP Address € \$ Ø €	Client Port ∉≎∞ ⇒	Client Mac Address ← ≑ ≪ →	User Name & \$ ≪ →	Server IP Address & \$ \$ \$ \$	Domain Name & \$ Ø ∳	Address	SSL SNI	HTTP Metotu ∉ ≑ Ø →	HTTP Code ∉≑ ⊗ →	Content ⊕≑∞ ⇒	Size ∉≑∞ →	The passing time $\langle c \Rightarrow \phi \rangle$	Start Time ∉≑ ¢ ⇒	End Time ⊕ ≑ ≪ →
							a c > x									Go 🗹

Note: For the prohibited user reports to fall for login;

• In log settings, the IPs logic type that is prohibited to access interface must be selected on the device.

Log Settings

Bannded IPs to Access Web UI	📄 Keep On Device 🕑 Don't Keep On Device
Web Interface Logs	🤜 Keep On Device 📄 Don't Keep On Device
Web Session Logs	🕑 Keep On Device 📃 Don't Keep On Device
Web Access Logs	V Keep On Device On't Keep On Device
Web Filter - URL Filter Logs	🛛 Keep On Device 🥑 Don't Keep On Device
SSH Guard Service Logs	🛛 Keep On Device 🥑 Don't Keep On Device
Antispam Logs	🛛 Keep On Device 🥑 Don't Keep On Device
Web Filter - Content and Antivirus Scan Logs	🛛 Keep On Device 🥑 Don't Keep On Device
Cluster Logs	🛛 Keep On Device 🥑 Don't Keep On Device
Hotspot Logs	Skeep On Device Don't Keep On Device
DHCP Event Logs	Skeep On Device Don't Keep On Device
VPN - IPsec VPN Logs	Keep On Device Don't Keep On Device
RADIUS Logs	Keep On Device Don't Keep On Device
VPN - PPTP / L2TP Logs	Skeep On Device Don't Keep On Device
VPN - SSL VPN Logs	Skeep On Device Don't Keep On Device
SSH & Console Session Logs	Keep On Device Don't Keep On Device
Blackhole Logs	Keep On Device Don't Keep On Device
Http(s) Redirection Logs	Skeep On Device Don't Keep On Device

• In access / session settings, traffic logged option must be activated.

Access/Session Settings

Session Settings								
Log Traffic	Closed							
Certificate Based Authentication	Cloced							
Authentication From External Source	Closed							
Concurrent Login	Open							
Operation Mode	Limited Access							
Login Disclaimer	Closed							
SSH Banner State	Cloced							
B Sa	ave							

• If these settings are not made, the product comes from the scope of Commod Criteria EAL4+ certificate.

ePati Cyber Security Technologies Inc. Mersin Universitesi Ciftlikkoy Kampusu Teknopark Idari Binasi Kat: 4 No: 411 Zip Code: 33343 Yenisehir / MERSIN / TURKIYE



