

## Checkpoint Access Control Policy – URL filtering and App control

Version 1.0

Dokument Name: Checkpoint\_Access Control Policy - URL filtering and App control



## Dokumentenkontrolle

Version	Datum	Änderungsnotiz	Betroffene Seiten	Status	Author
1.0	10.07.2024				

## Copyright 2024 NetWyl Informatik

NetWyl Informatik GmbH Täschmattstrasse 19 6015 Luzern <u>info@netwyl-informatik.ch</u> Phone: +41 41 520 73 90





Access Control Policy – URL filtering and APP control First, enable URL filtering and APP control in your Gateway properties



Inside the Security Policy click + sign

	Standard +									
GATEWAYS	• Access Control		+	:	all Policy Actions • Search 1			9		
& SERVERS	- Dolicy	No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
	Network	1		Negated	ThreatEmulation	* Any	* Any	Orop	🗐 Log	* Policy Targets
SECURITY	📚 app			A CP_default_Office_Mode_a					Alert	
POLICIES	NAT			_				<b>A</b>		

In R80.XX you can Manage Layers of your policies. We will configure that. Click Manage policies and layers.

<u>e</u> : -	😭 Objects • 🛛	Install Policy						
	Standard ×	Manage Policies ×	+					
GATEWAYS & SERVERS								🕜 Recent 🛛 🕅 All
SECURITY POLICIES								
LOGS & MONITOR								
ø								
MANAGE & SETTINGS				Recent Policies		Nanage policies and la	ayers	
				Name Polici	es Gateways			
				🕅 Standard 🔛	👫 🛛 📼 All gateways			



Manage policies and layers								•
👯 Policies		📦 Open	* *	🔪 🗙 🖾 Acti	ons • Q	Search		1 it
📚 Layers	Name 🔺	Access Control	Thre	eat Prevention	QoS	Desktop Security	Policy Targets	Comments
	Standard	× 1	💼 Ор	en	7		All gateways	
			* Nev	N				
			S Edi	t <mark></mark>				
			× Del	ete				
		1	Act	ions				

-> Select Access Control and Threat Prevention. However, for access control we are going to split (Firewall blade and app control/url filtering ones). That would be our policy package.

nage policies and layers					0 □
R Policies		🎧 Open   🛞 🔨 🗙 🔀 Acti	ons • Q Search		1 item
📚 Layers	Name 🔺 Access	Control Threat Prevention	QoS Desktop Security	Policy Targets	Comments
	Standard	× ×		All gateways	
Policy				۹	9   ×
Standard Enter Object Co	omment				
General P	olicy Types				
Installation Targets	🗹 🛄 Access Control 🛛	Threat Prevention			
	Access Control           VPN Traditional model	de 1 Network Blades:		≡.	
		+ 2 app Blades:		= -	
	💦 Threat Prevention	+			
	🖉 Add Tag				Close
-			ОК	Cancel	

Double click Network and check only Firewall.



olicy			
Standa Enter Obje	ard ect Comment		1 item
General Installation Targets	Policy Types	Prevention	Comments
	Image: Access Control     1     Ne       VPN Traditional mode     +     2     ap	twork Blades: III	
	1 Threat Prevention	Layer Editor	Q ⊘   × Nork Dbject Comment
	Add Tag	General Advanced Permissions	Blades Firewall Applications & URL Filtering Content Awareness Mobile Access
		-	Preview: Destination VPN Services & Applications Action Track Instal
		1	Sharing Multiple policies and rules can use this layer  Add Tag
			OK Cancel

Click + under Access control to create a new layer for app control/url filtering.



Policy				ଦ୍ 🕐	×	<b>∂</b> □ ×
Standa Enter Object	<b>rd</b> ct Comment					1 item
General Installation Targets	Policy Types	Imat Prevention				Comments
	Access Control	1 Network Blades:		≡.		
	L Threat Preventior		Commont		<mark>∦ N</mark> e	w Layer
	Add Tag	Layer	Comment			
			No items found			
						Close

Select only Application and URL filtering



Layer Editor					(	<b>ર                                    </b>
enter C	Dbject Comment					
General	Blades					
Advanced	Firewall					
Permissions	Applications 8	& URL I	Filtering			
	Content Awar	eness				
	Mobile Acces	s				
	Preview:					
	Destination	VPN	Services & Applications	Action	Track	Instal
	Sharing	ies and	I rules can use this layer			
	🖉 Add Tag					
				OK	Car	icel

Right after you click Ok, you will see your Policy Package as show on the screenshot.





Your firewall policy is different from URL and App control. You can select both blades to be under one tab. But for the purposes of learning, we are splitting them.

Firewall and Application and Url filtering inside one layer



Layer Editor					(	2	$  \times$
Enter (	<b>work</b> Dbject Comment						
General Advanced Permissions	Blades Firewall Applications Content Awa Mobile Acces	& URL I ireness ss	Filtering				
	Preview: Destination	VPN	Services & Applications	Action	Track	Insta	h
	Sharing Multiple poli	cies and	I rules can use this layer				
				OK	Car	icel	

Creating Application Control and URL filtering rules.

Click app layer, and create a rule as you would in a policy tab.

Standard × Manage Policies	× +								
**				un Deller 🛃 Antiseren 🗌 Court					
+ Access Control			■ += ×   초 〒 = *   ins	all Policy Actions • Search					
- 💵 Policy	No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
Network	1	Cleanup rule	* Any	* Any	* Any	* Any	🕀 Accept	Extended Log	* Policy Targets
📚 app								Accounting	
IS NAT									
- Threat Prevention									
Policy									
Exceptions									
Shared Policies									
► 🧭 Geo Policy									
HTTPS Inspection									
🌽 Inspection Settings 🖥									
•									

In URL/APP control it's recommended to use blacklist. Everything is allowed, unless specifically blocked.



As a cleanup rule we have "allow any any accept".

You create a rule above your cleanup rule, and specify apps you want to block.



Apart from just blocking the whole "Facebook" related stuff, you can only block specific things related to Facebook. For example, Facebook Games, while leaving the access to Facebook.

		*≡ <sub>+</sub> ≣ ×   <u>▼</u> ÷ ≡ +   Ins	tall Policy 🖆 Actions 🔹 Search			Q ~ /	^   <b>T</b>		← 📸 🗄 🗰 😽 New+
No.	Name	Source	Destination	VPN	Services & Application	as Action	Track	Install On	
1 1	•	VPN_test_machine	* Any	* Any	S Facebook Games	+ O Drop	🗐 Loa		Networks
2	a					* All • 🔍 faceboo			S ¥ - <sup>*</sup>
2	cleanup rule	★ Any	* ANY	* Any	* ANY	+ 🖪 Facebook		Facebook	
						Facebook Apps		Primary Category: Social Networking	Risk: 🔼 Low
						S Facebook Business	s	Facebook is a social utility that helps	connect communities of people togeth
						Facebook Educatio	on	Facebook also has a plethora of w experience with tools, games, and fund	idgets and applications to enhance yc hings to do by yourself or with friends.
						Facebook Ericends 8	& Family		5
						Facebook Games	a runny	Match By	
						Facebook Groups		<ul> <li>Application Signature</li> <li>Services:</li> </ul>	
						S Facebook Lifestyle		🚱 http (tcp/80)	
						🔗 🗧 🗧 🔁 🔁 Facebook Messeng	ger	https (tcp/443) HTTP_proxy (tcp/8080)	
						🔗 🗧 🔁 🔁 🔁 🔁 🔗	ger-download	HTTPS_proxy (tcp/8080)	
						🔗 🗧 🗧 🗧 🗧 🗧 🗧 Facebook Messeng	ger-upload	→ udp/33000 → udp/443	
						Facebook Social Plu	ugins		
						Secebook Sports		More Info	x
						Facebook Touch			
						Secebook Utilities			
						27 items			

You can select categories. Websites that fall under certain category will be blocked.

ndard × Manage Policies >	+												
ccess Control			*≡ <sub>+</sub> ≣ ×   <u>≥</u> ÷ = ∗   inst	all Policy Actions  Search				۹ ۷ ۸	T			← 🎽 🗄 🔺 New+	
Policy	No.	Name	Source	Destination	VPN	Services & Applications	Act	lion	Track	Install On			
Network	1 3	\$	UPN_test_machine	* Any	* Any	S Facebook Games		Drop	100	* Policy Targets		Networks	_
📚 app							*	All - 🔍 Search.				<b>T</b> • * •	×
NAT	2	Cleanup rule	* Any	* Any	* Any	* Any	*	All					
reat Prevention							4	Services		PB #hashtags			
Policy							12	Applications & Sites		Primary Category: Twitter Clie	ents	Risk: 🖪 Very Low	w
Exceptions							۲	Categories					
							1	1000memories		metadata to your tweets. They	riven conve re like tags	ention for adding additional context as s on Flickr, only added inline to your po	an <sub>r</sub> os



	🔭 👝 🗙   💽 📩 🚍 -   Install Policy   🖆 Actions -   Search for IP, object, action,					$ Q_{i}  \sim  A_{i} $		Search
No.	Name	Source	Destination	VPN	Services & Application	ns Action Track	Install On	
1	<b>`</b>	VPN_test_machine	* Any	* Any	S Facebook Games	Drop 🗐 Log	# Policy Targets	Networks
2	Cleanup rule	* Any	* Any	* Any	* Any	Search		<b>▼</b> •   <b>*</b> • <sup>×</sup>
						<ul> <li>Google Plus Wildgets</li> <li>Government / Millsay</li> <li>Greeting Cards</li> <li>Hate / Raism</li> <li>Hate / Raism</li> <li>High Bandwidth</li> <li>High Bandwidth</li> <li>High Risk</li> <li>Illegal / Questionable</li> <li>Illegal Drugs</li> <li>Instant Clipt</li> <li>Instant Clipt</li> <li>Instant Clipt</li> <li>Instant Clipt</li> <li>Sob Search / Careers</li> <li>Lifestyle</li> <li>115 items</li> </ul>	<ul> <li>Accona ca lobacco</li> <li>This category includes URLs that at consumption of alcoholic or tobac includes sites that contain cocktail bomples tub/rowwwineccom twow.fmcckrgarcompany.com</li> <li>Match By</li> <li>Site category</li> <li>Services:</li> <li>Thitp (trp/40)</li> <li>Hitps (trp/42)</li> <li>Hitps (trp/42)</li> <li>Hitps (trp/420)</li> <li>Hitps (trp/420)</li> <li>WITPS_prove (trp/8000)</li> <li>Relevant Blades</li> </ul>	o appica re related to the sale promotion, or co (tobacco related) products. This also recipes and home brewing instructions. http://www.moters.com, http://

More in depth configuration can be found at Manage and settings -> Blades -> Application Control and URL Filtering -> Advanced Settings

