

Expedition

TechNote: Managing Service Objects

Revised: April 2019 For Version: update 1.1.x



paloalto NETWORKS 3000 Tannery Way Santa Clara, CA 95054 www.paloaltonetworks.com

© 2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. You can find a list of our trademarks at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.



TECHNOTE SUMMARY	
SECTION 1	ERROR! BOOKMARK NOT DEFINED.
SECTION 2	ERROR! BOOKMARK NOT DEFINED.
SECTION 3	ERROR! BOOKMARK NOT DEFINED.
SECTION 4	ERROR! BOOKMARK NOT DEFINED.
SECTION 5	ERROR! BOOKMARK NOT DEFINED.
APPENDIX A – <description></description>	ERROR! BOOKMARK NOT DEFINED.
APPENDIX B – <description></description>	ERROR! BOOKMARK NOT DEFINED.



TechNote: Managing Service Objects

This document will describe how to optimize the services and services group objects.

Remove unused objects

Unused services and services group objects are marked with a red mark.

*	services + -									
			Name	Protocol	Dst Port	Vsys	src File			
	•	•	application-default	tcp	0	shared	predefined			
	•	ø	application-default	ТСР	1-1	vsys1	CSV			
	•	n P	Citrix TCP			vsys1	MT_Panorama			
	٠		Citrix TCP (Session Reliability)			vsys1	MT_Panorama			
	•	-1 ¹⁹	Citrix UDP			vsys1	MT_Panorama			

These objects can be removed in bulk by clicking on the remove unused objects in the lower right hand corner.

	Hide Parents	Remov	e Unu	sed Ob	ojects	L.
-	vsys1	-			X	to: [
						10. F

Clicking on this will also remove the unused address and address group objects.

Search for duplicate services

User the predefined filter to search for services that have the same value.



For the found duplicated services, use the 'Search and Replace' to consolidate the services.



Highlight the services to combine.

•	٥	HTTPS	ТСР	443-443	vsys1	CSV
٠	٥	HTTPS Management	ТСР	443-443	vsys1	CSV
٠	•	HTTP Management	ТСР	80-80	vsys1	CSV
٠	•	НТТР	ТСР	80-80	vsys1	CSV

Right click on the highlighted objects and choose "Search and Replace".



From the results, choose which service objects you will want to remove and replace with an existing service objects with the same value.

Ø DA	HBOARD IMPORT PLUGINS BEST	PRACTICES M. LEARNING MONITOR	POLICIES	OBJECTS NETWORK DEVICE TOOLS EXPORT	CSVImport 🔻
SEARC	H RESULTS		• • Ø	OPTIONS	•
	Name	Value	Vsys	PREFIX/SUFFIX/REPLACE	Extern
	Services (2)			FOUND IN REPLACE (0)	
	HTTP Management	TCP/80-80	vsys1	Security Policy (1) 🐉 NAT Policy (0) 🦉 App Override Policy (0)	
	HTTP	TCP/80-80	vsys1		
				Is not in Groups	

The 'FOUND IN' window on the right hand side will display where the selected service object is in use.

OP	IONS	•
	PREFIX/SUFFIX/REPLACE 🔁 RENAME 🕘 SEARCH & REPLACE	Extend
FOL	ND IN REPLACE (0)	ded Info
5	Objects Groups (0) 🧱 Security Policy (1) 🐇 NAT Policy (0) 🧮 App Override Policy (0)	ormatic
	Name Position Vsys	5
	🇶 HTTP Management (1)	
V	14] Web-Management Service vsys1	
Ð	Add to Replace	4



Select all references and click on 'Add to Replace' for each configuration where the service object will be replaced.



After choosing all the configurations where the object will be replaced, click on the 'REPLACE' tab.

Under 'Replace By:' select services and in the 'To:' select the service with the same value to use as a replacement.

OPTIONS	OPTIONS										
PREFIX	(/SUFFIX/REPLACE 🔁 RENAME	SEARCH & REPLACE									
FOUND IN			REPLACE (1)								
	Objects	Position	Vsys	Replace by:							
🗖 🗶 НТ	TP Management (1)			Services 💌							
S	14] Web-Management	Service	vsys1	То:							
				нттр т							
- Clear				💽 Replace All							

Click on 'Replace All' to replace the service. An indicator will pop up displaying the completion of the replacement.





The service will now be marked as red (meaning unused) and can be removed using the remove unused object option from the previous step.

SEA	SEARCH RESULTS								
		Name	Value	Vsys					
	火 S	ervices (2)							
	•	HTTP Management	TCP/80-80	vsys1					
	•	HTTP	TCP/80-80	vsys1					

Convert services to App-ID using Search and Replace

To convert services to App-ID, the services can be highlighted from the 'Services' tab or they can be filtered directly from the Security policies page.

A filter can be created to display all security policies where a service object is in use.

GLOBAL SEARCH & OBJECTS MERGE				×
T FILTERS			O Clear	All
Security Policies 🗶			v	
Service	▼ contains	-	HTTP Case Sensitive 🕂	
LIBRARY		- 0	▼ FILTERS + - ;	C
🔹 🗁 AVAILABLE		Û	▼ 🗁 ACTIVE	I
			▼ Service contains "HTTP" on "Security Policies" on vsys 1	T
			Close Y APPLY FILTER	R

The filter above will search and display only the security policies where the service 'HTTP' is in use.

-	Security 🛃 Nat 📕	Application Override	QoS 🔯 Policy Based Forwa	rding 💣 Decryption 🔒	Tunnel Inspection 🏻 ಿ Auth	nentication 🛛 💽 DoS Protection			T Filters [Activate	ed] 🖉 Clear All
-	r security policies + − ≡									
	id] Name	Tag	From	Source	То	Destination	Application	Service	Description	vsys/DG
۰	Pre-rulebase vsys1: (2)								
0	13) EWeb- management none m/VPN any m/VPN any OHTTP vsys1 0 HTTPs vsys1 OHTTPs vsys1									
0	14]	none	1 VPN	any	1 VPN	any	any	O HTTP		vsys1

To convert the service 'HTTP' to web-browsing, right click on the service and choose 'Search and Replace'.

The following steps will be similar to the previous example of how to use the search and replace, but instead of consolidating services, this example will convert the service to an equivalent App-ID.



Service			Description	vsys/D
онтт онтт	P PS			vsys1
O HTZ	-0			veve1
		Menu Options		
	٢	Rule Actions		•
	an C	Bulk Changes		•
	ul ^{li.}	Machine Learni	ng	•
	ηl^{μ}	Rule Enrichmen	t	•
	ul^{μ}	App-ID Adoptio	'n	•
	Ø	3rd Party Optio	ns	•
		Auto Zone Assig	gn	
	x	Export to Excel		
		Advanced Opti	ions	
	€	Search & Replac	e	
	T	Add to Filters		
	T	Select Predefine	ed Filter	•
C01 v	m	Add to Cron Job)S	•

Choose the service 'HTTP', the 'FOUND IN' window will display the configurations where the service is in use. Click through the options and choose where to replace the service. Click on 'Add to Replace' in each section.

SEA	RCH	RESULTS		▼ ⊘	ΟΡΤΙΟ	ONS						
		Name	Value	Vsys	PI	REFIX /	/ SUFFIX / REPL			CH & REPL	ACE	
۰	💼 S	ecurity Policies (1)			FOUN	DIN				REPLACE	(2)	
	٠	HTTP-Management		vsy	5 o	biects	Groups (1)	Security Policy (1)	🕸 NAT P	olicy (0)	App Over	ride Policy (0)
	火 S	ervices (1)				,		,	a	, (,		,,
	٠	HTTP	TCP/80-80	vsy			Group Name					Vsys
						e htt	TP (1)					
						R	web-managem	nent				vsys1
«	<	1 of 1 >	» 200 a	- 3 of 3	₽ A	dd to R	Replace	Add to Filter				

After choosing the configuration where the service will be replaced, choose the following. 'Replace By:' choose 'Applications'



'To:' (choose the app-ID to replace the service) in this case web-browsing is the equivalent to 'HTTP' service which is defined in this configuration as TCP/80.

A fill list of applications and their protocol/port configurations can be found from the applipedia page:

https://applipedia.paloaltonetworks.com/

Or by searching the 'Applications' from the web user interface of Panorama or the firewall.

OPTIONS										
ΣΞ	PREFIX/SUFFIX/REPLACE 🔁 RENAME 🤤 SEARCH&REPLACE									
FOU	ND IN									
		Objects	Position	Vsys	Replace by:					
	火 нт	TP (2)			Applications					
	-	14] HTTP-Management	Service	vsys1	То:					
		7] web-management	Groups	vsys1	web-browsing					
					Options Split rules when needed Remove Service from Group					
	Clear				💽 Replace All					

There are 2 default actions that will be applied when converting services to applications.

'Split rules when needed' – if the service is used in a policy where there are multiple services similar to the policy below. Checking this box will clone the existing policy and apply the App-ID to the cloned policy.

'Remove Service from Group' – if the service is used in a service group, checking this box will remove the service from the group and will clone the existing policy and apply the App-ID to the cloned policy.

The policies before the service to App-ID conversion is shown below.

0	13]	none	🟦 VPN	any	1 VPN	any	any	© web-management	vsys1
0	14]	none	🏛 VPN	any	1 VPN	any	any	¢ HTTP	vsys1



The services group 'web-management' is shown below:

👷 SERVICES GROUPS + - 🚍								
			Name	Members	Vsys	src File		
	•	o;	name	members	vsys1	CSV		
	•	os	SonicWALL SSO Ag		vsys1	CSV		
	•	¢\$	SonicWALL TS Age		vsys1	CSV		
	•	o,	Terminal Services	Terminal Services Terminal Services T	vsys1	CSV		
	•	o;	web-management	✿ HTTP ✿ HTTPS	vsys1	default		

After clicking 'Replace All' the resulting policies and services groups are shown below.

The service 'HTTP' has been removed from the services group it was previously a member of.

🦹 SERVICES GROUPS + - 🚍								
			Name	Members	Vsys	src File		
	٠	o;	name	members	vsys1	CSV		
	•	¢\$	SonicWALL SSO Ag		vsys1	CSV		
	•	¢\$	SonicWALL TS Age		vsys1	CSV		
	•	o,	Terminal Services	Terminal Services Terminal Services T	vsys1	CSV		
	•	Q ⁰	web-management	HTTPS	vsys1	default		

The resulting policies are now. Policy 15 was added automatically from the default actions to split the policies and remove the service from the services group.

0	15]	none	🏛 VPN	any	🏦 VPN	any	web-browsing	o application-default
0	13]	none	🏛 VPN	any	🏛 VPN	any	any	© ; web-management
0	14]	none	🏛 VPN	any	🏛 VPN	any	web-browsing	o application-default

The actions to convert services to App-ID must be performed on per service. But the changes where the services are used are made in bulk.