Expedition

TechNote: Managing Service Objects

Revised: April 2019
For Version: update 1.1.x

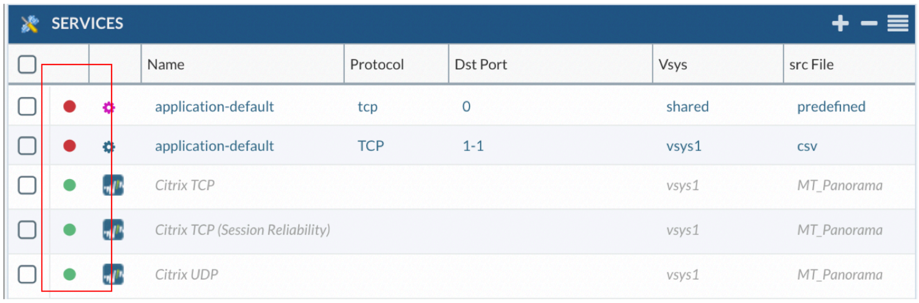
paloalto NETWORKS
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

TechNote: Managing Service Objects

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

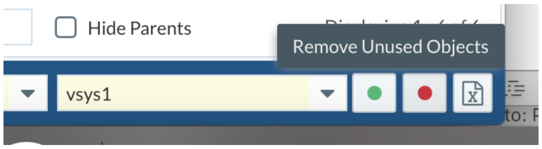
Remove unused objects

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



□			Name	Protocol	Dst Port	Vsys	src File
□	●		application-default	tcp	0	shared	predefined
□	●		application-default	TCP	1-1	vsys1	csv
□	●		Citrix TCP			vsys1	MT_Panorama
□	●		Citrix TCP (Session Reliability)			vsys1	MT_Panorama
□	●		Citrix UDP			vsys1	MT_Panorama

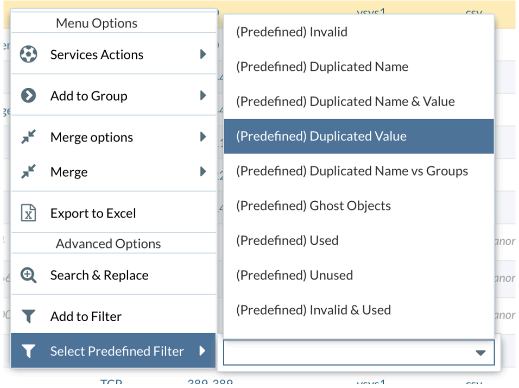
These objects can be removed in bulk by clicking on the remove unused objects in the lower right hand corner.



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

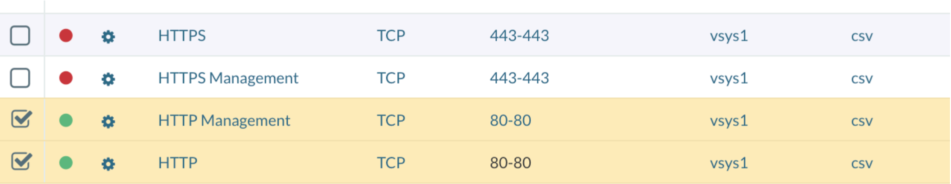
Search for duplicate services

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



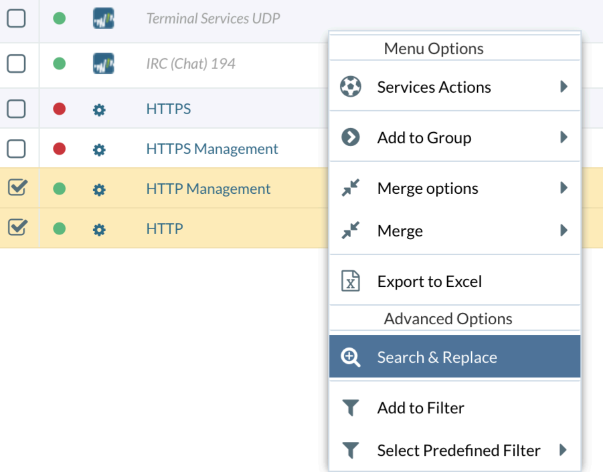
For the found duplicated services, use the 'Search and Replace' to consolidate the services.

Highlight the services to combine.



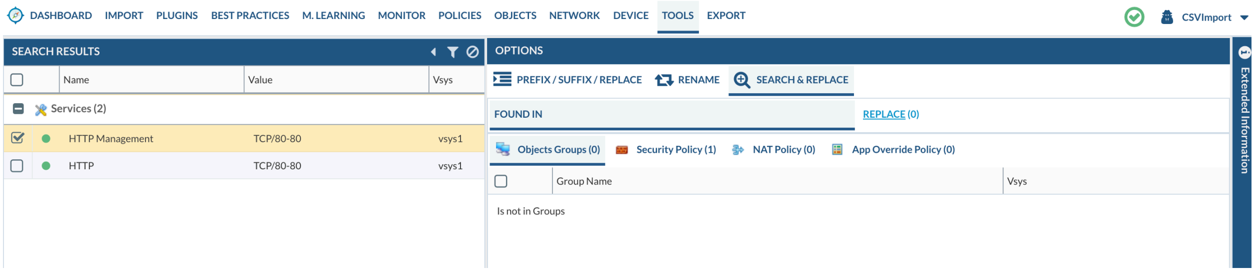
☐	●	⚙	HTTPS	TCP	443-443	vsys1	csv
☐	●	⚙	HTTPS Management	TCP	443-443	vsys1	csv
☑	●	⚙	HTTP Management	TCP	80-80	vsys1	csv
☑	●	⚙	HTTP	TCP	80-80	vsys1	csv

Right click on the highlighted objects and choose “Search and Replace”.



☐	●	*Terminal Services UDP*
☐	●	*IRC (Chat) 194*
☐	●	HTTPS
☐	●	HTTPS Management
☑	●	HTTP Management
☑	●	HTTP

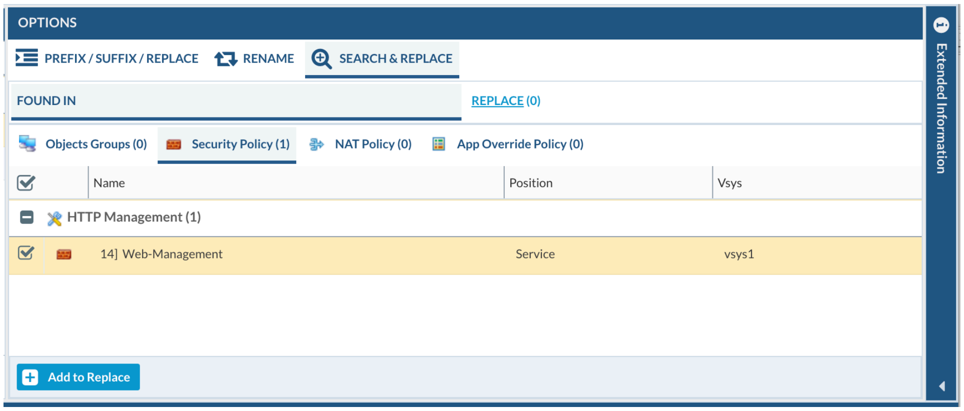
From the results, choose which service objects you will want to remove and replace with an existing service objects with the same value.



☐		Name	Value	Vsys
⊟		Services (2)		
☑	●	HTTP Management	TCP/80-80	vsys1
☐	●	HTTP	TCP/80-80	vsys1

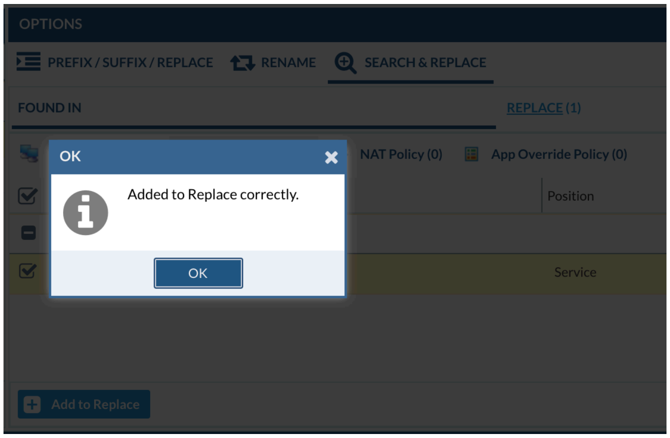
☐	Group Name	Vsys
Is not in Groups		

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



☑		Name	Position	Vsys
⊟		HTTP Management (1)		
☑		14] Web-Management	Service	vsys1

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



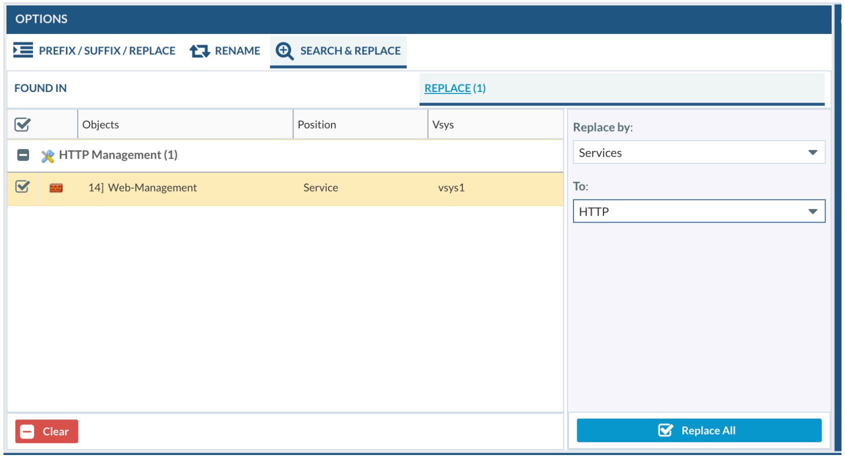
OK

Added to Replace correctly.

OK

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.

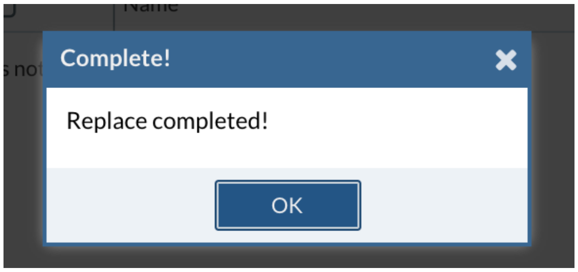


☑	Objects	Position	Vsys
	HTTP Management (1)		
☑	14] Web-Management	Service	vsys1

Replace by: Services

To: HTTP

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

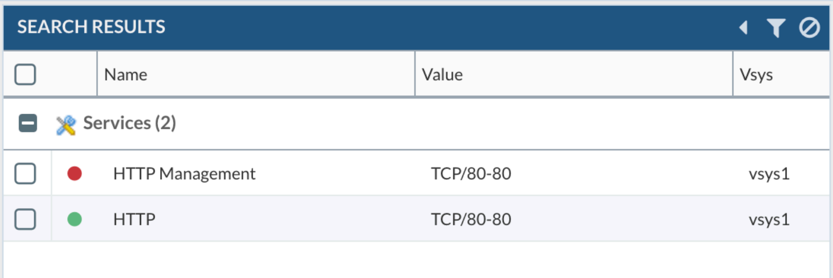


Complete!

Replace completed!

OK

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

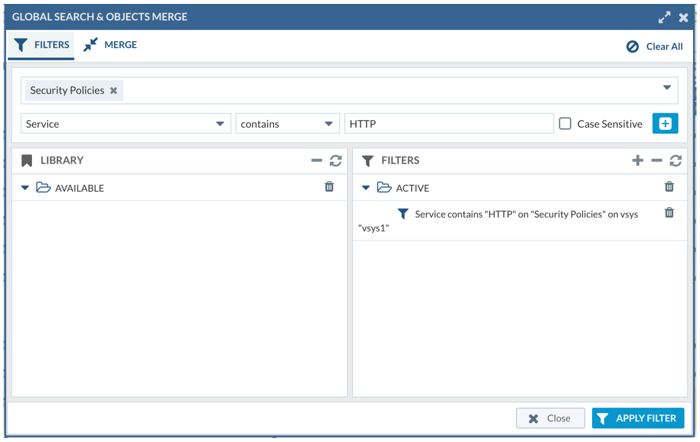


□		Name	Value	Vsys
⊟		Services (2)		
□	🔴	HTTP Management	TCP/80-80	vsys1
□	🟢	HTTP	TCP/80-80	vsys1

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.

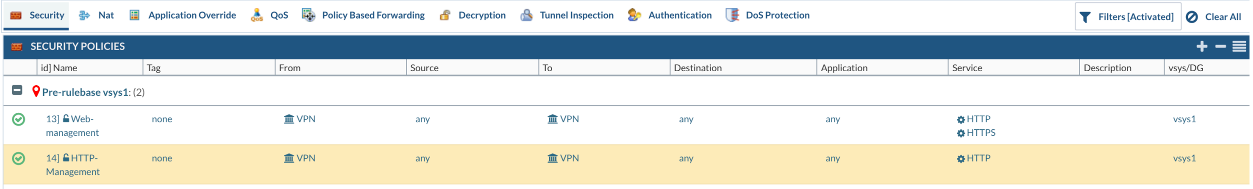


Security Policies ✖

Service | contains | HTTP | □ Case Sensitive

Service contains "HTTP" on "Security Policies" on vsys "vsys1"

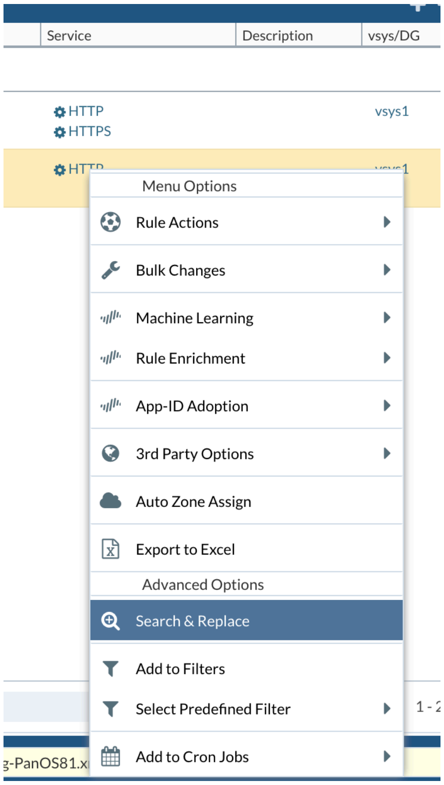
The filter above will search and display only the security policies where the service ‘HTTP’ is in use.



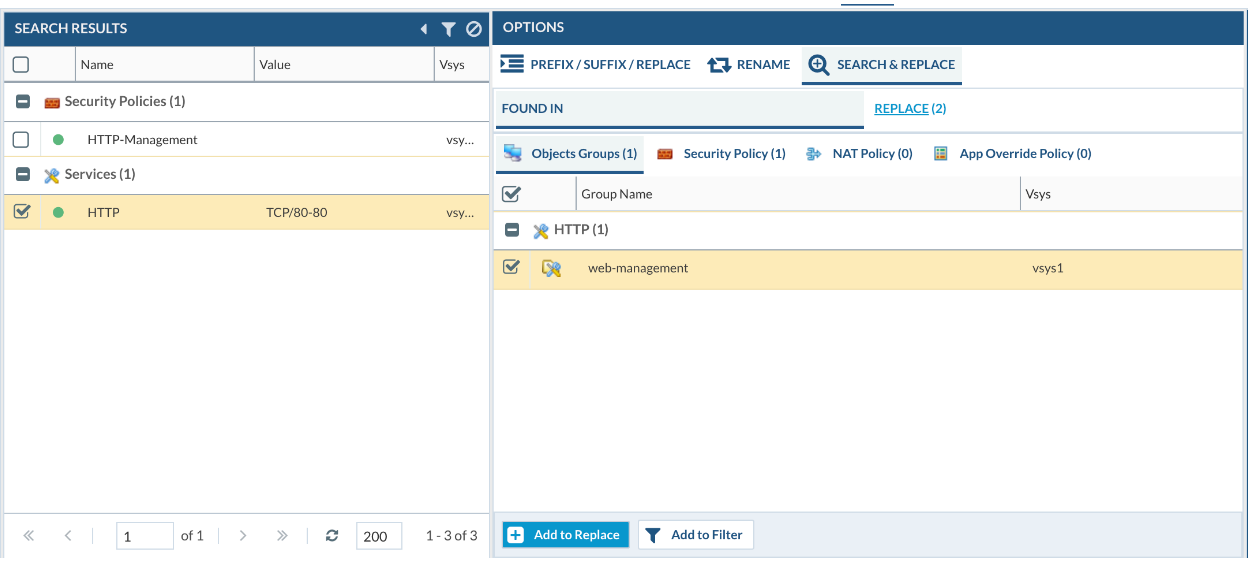
id] Name	Tag	From	Source	To	Destination	Application	Service	Description	vsys/DG
Pre-rulebase vsys1: (2)									
13] Web-management	none	VPN	any	VPN	any	any	HTTP HTTPS		vsys1
14] HTTP-Management	none	VPN	any	VPN	any	any	HTTP		vsys1

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.



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.



☐	Name	Value	Vsys
⊟	Security Policies (1)		
☐	● HTTP-Management		vsy...
⊟	Services (1)		
☑	● HTTP	TCP/80-80	vsy...

☑	Group Name	Vsys
⊟	HTTP (1)	
☑	web-management	vsys1

After choosing the configuration where the service will be replaced, choose the following.

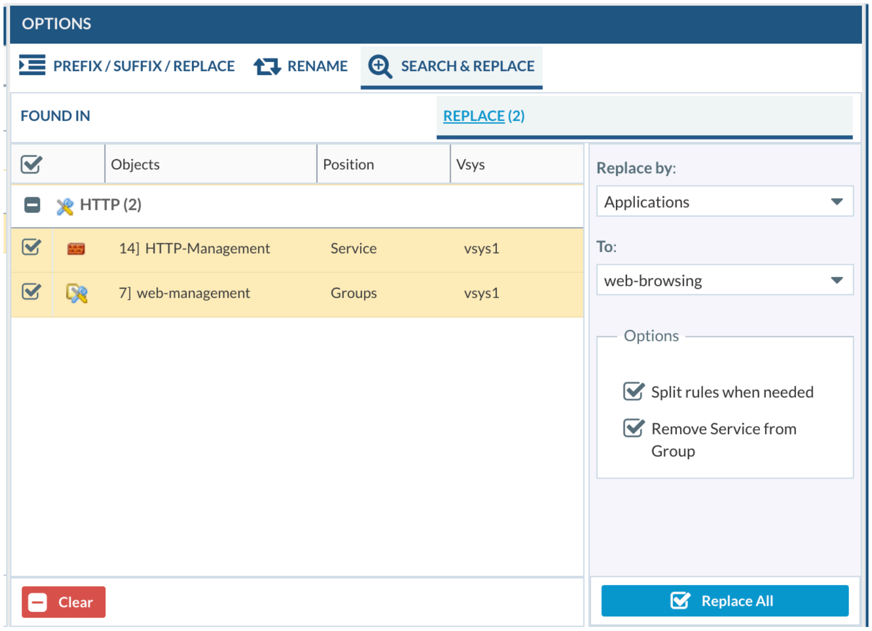
'Replace By:' choose 'Applications'

'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

PREFIX / SUFFIX / REPLACE | RENAME | SEARCH & REPLACE

FOUND IN | REPLACE (2)

☑	Objects	Position	Vsys
⊟	HTTP (2)		
☑	14] HTTP-Management	Service	vsys1
☑	7] web-management	Groups	vsys1

Replace by: Applications

To: web-browsing

Options

☑ Split rules when needed

☑ Remove Service from Group

Clear

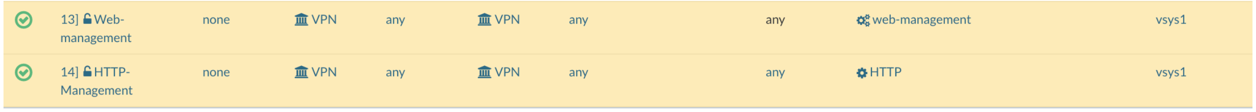
Replace All

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.

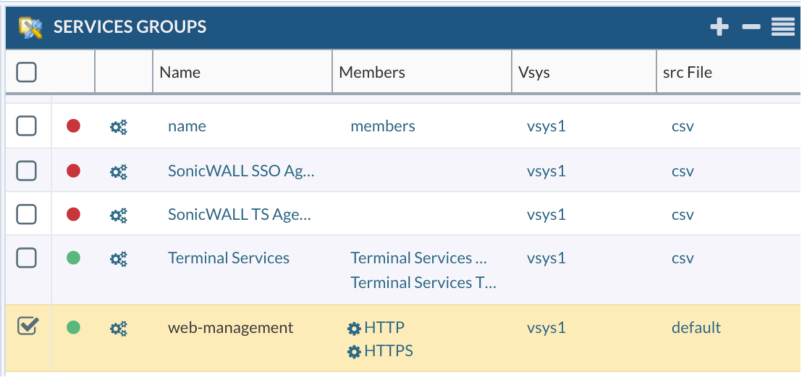
'Remove Service from Group' – if the service is used in a service group, checking this box will remove the service from the group and will clone the existing policy and apply the App-ID to the cloned policy.

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



✓	13] Web-management	none	VPN	any	VPN	any	any	web-management	vsys1
✓	14] HTTP-Management	none	VPN	any	VPN	any	any	HTTP	vsys1

The services group ‘web-management’ is shown below:

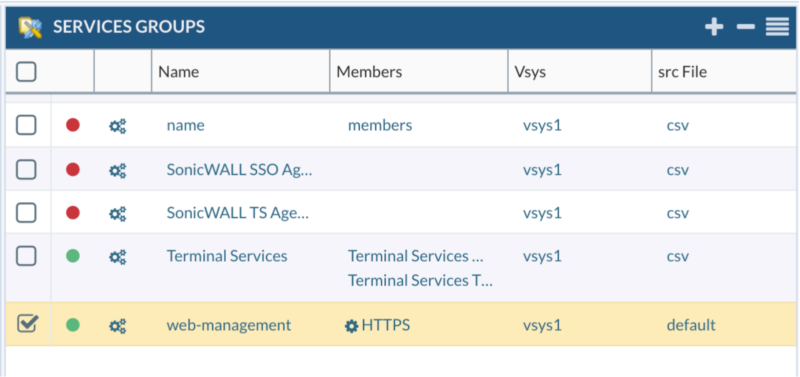


SERVICES GROUPS

□			Name	Members	Vsys	src File
□	🔴	⚙	name	members	vsys1	csv
□	🔴	⚙	SonicWALL SSO Ag...		vsys1	csv
□	🔴	⚙	SonicWALL TS Age...		vsys1	csv
□	🟢	⚙	Terminal Services	Terminal Services ... Terminal Services T...	vsys1	csv
☑	🟢	⚙	web-management	⚙HTTP ⚙HTTPS	vsys1	default

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

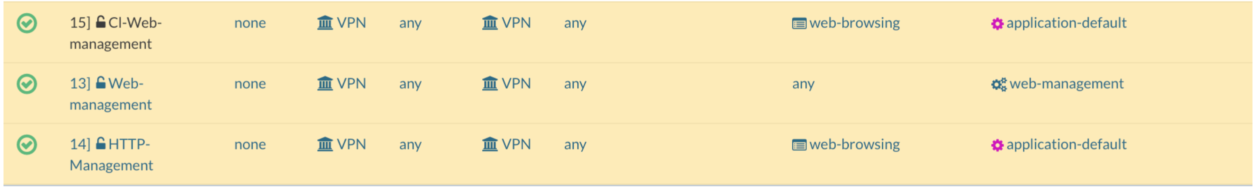
The service ‘HTTP’ has been removed from the services group it was previously a member of.



SERVICES GROUPS

□			Name	Members	Vsys	src File
□	🔴	⚙	name	members	vsys1	csv
□	🔴	⚙	SonicWALL SSO Ag...		vsys1	csv
□	🔴	⚙	SonicWALL TS Age...		vsys1	csv
□	🟢	⚙	Terminal Services	Terminal Services ... Terminal Services T...	vsys1	csv
☑	🟢	⚙	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.



✓	15] 🔒CI-Web-management	none	VPN	any	VPN	any	web-browsing	application-default
✓	13] 🔒Web-management	none	VPN	any	VPN	any	any	⚙web-management
✓	14] 🔒HTTP-Management	none	VPN	any	VPN	any	web-browsing	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.