

Configuration d'un Firewall

Stormshield

Afin de vérifier les règles d'utilisation des ressources numériques, on met en place un filtrage sur notre firewall Stormshield comme ci-dessous :

The screenshot shows the Stormshield Network Security v4.3.16 interface. The left sidebar contains a navigation menu with sections like CONFIGURATION, SECURITY POLICY, and APPLICATION PROTECTION. The main panel is titled 'SECURITY POLICY / FILTER - NAT' and displays a table of 14 rules. The table columns include Name, Status, Action, Source, Destination, Dest. port, Protocol, Security inspection, and Comments. Rules 1 through 14 are listed, with rule 9 highlighted in green. At the bottom, there is a 'CONFIGURATION VALIDATOR' section with 'CANCEL' and 'APPLY' buttons.

Name	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
interne_dns	on	pass	Network_In	srv_dns_priv	dns		IP3	Created on 2024-11...
interne_http	on	pass	Network_In	srv_web_priv	http		IP3	Created on 2024-11...
interne_webmail	on	pass	Network_In	srv_web_priv	webmail		IP3	Created on 2024-11...
bloque_pc_200_ftp	on	block	pc_200	Any	ftp		IP3	Created on 2024-11...
interne_ftp	on	pass	Network_In	srv_ftp_priv	ftp		IP3	Created on 2024-11...
interne_smtp	on	pass	Network_In	srv_mail_priv	smtp		IP3	Created on 2024-11...
bloque_Coree_Sud	on	block	Network_In	Internet geo	http https		IP3	Created on 2024-11...
bloque_cnn_http(s)	on	block	Network_In	rgw www.cnn.com	http https		IP3	Created on 2024-11...
autorise_http_filtrage_url	on	pass	Network_In	Internet	http		IP3	Created on 2024-11...
autorise_https_filtrage_ssl	on	decrypt	Network_In	Internet	https		IP3	Created on 2024-11...
autorisation_ftp	on	pass	Network_In	Internet	ftp		IP3	Created on 2024-11...
autorise_ping	on	pass	Network_In	Any	Any	icmp (Echo request)	IP3	Created on 2024-11...
autorisation_ssh	on	pass	Network_In	Internet	ssh		IP3	Created on 2024-11...
autorise_srvsmtppriv_smtp	on	pass	Network_In	Internet	smtp		IP3	Created on 2024-11...

This screenshot shows the same Stormshield Network Security interface, but with a different set of rules displayed in the 'SECURITY POLICY / FILTER - NAT' section. The table now contains 19 rules, with rule 9 highlighted in green. The 'CONFIGURATION VALIDATOR' section at the bottom still shows 'CANCEL' and 'APPLY' buttons.

Name	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
interne_smtp	on	pass	Network_In	srv_mail_priv	smtp		IP3	Created on 2024-11...
bloque_Coree_Sud	on	block	Network_In	Internet geo	http https		IP3	Created on 2024-11...
bloque_cnn_http(s)	on	block	Network_In	rgw www.cnn.com	http https		IP3	Created on 2024-11...
autorise_http_filtrage_url	on	pass	Network_In	Internet	http		IP3	Created on 2024-11...
autorise_https_filtrage_ssl	on	decrypt	Network_In	Internet	https		IP3	Created on 2024-11...
autorisation_ftp	on	pass	Network_In	Internet	ftp		IP3	Created on 2024-11...
autorise_ping	on	pass	Network_In	Any	Any	icmp (Echo request)	IP3	Created on 2024-11...
autorisation_ssh	on	pass	Network_In	Internet	ssh		IP3	Created on 2024-11...
autorise_srvsmtppriv_smtp	on	pass	Network_In	Internet	smtp		IP3	Created on 2024-11...
autorise_internet_vers_http	on	pass	Internet	Firewall_Out	http		IP3	Created on 2024-11...
autorise_internet_vers_ftp	on	pass	Internet	srv_ftp_public	ftp		IP3	Created on 2024-11...
autorise_internet_vers_smtp	on	pass	Internet	srv_mail_public	smtp		IP3	Created on 2024-11...
autorise_internet_vers_ssh/https_firewall_Out	on	pass	Internet	Firewall_Out	Any	icmp (Echo request)	IP3	Created on 2024-11...
autorise_internet_vers_ssh/https_firewall_Out	on	pass	Internet	Firewall_Out	ssh https		IP3	Created on 2024-11...

root@172.16.15.254 Administrateur

Non sécurisée https://172.16.15.254/admin/admin.html#sslfiltering/0

STORMSHIELD Network Security v4.3.16

MONITORING CONFIGURATION EVA1 root

admin WRITING LOGS RESTRICTED ACCESS

CONFIGURATION

Search...

Temporary accounts

Access privileges

Authentication

Enrolment

Directories configuration

SECURITY POLICY

Filter - NAT

URL filtering

SSL filtering

SMTP filtering

QoS

Implicit rules

APPLICATION PROTECTION

Applications and protection

Protocols

Inspection profile

Vulnerability manager

Host reputation

OBJECTS

SECURITY POLICY / SSL FILTERING

(0) SSLFilter_00 Edit URL database provider: Embedded URL database

+ Add X Delete Up Down Cut Copy Paste + Add all predefined categories Check URL classification

Status	Action	URL - CN	Comments
1 on	Pass without decrypting	White-list	don't decrypt some specific ssl servers
2 on	Block without decrypting	Black-list	default rule (decrypt all)
3 on	Block without decrypting	shopping	
4 on	Block without decrypting	news	
5 on	Pass without decrypting	Any	

ERRORS WERE FOUND IN THE SSL FILTER POLICY

URL CATEGORIES

CANCEL APPLY

8°C Nuageux

Rechercher

21:54 15/11/2024

root@172.16.15.254 Administrateur

Non sécurisée https://172.16.15.254/admin/admin.html#urlfiltering/0

STORMSHIELD Network Security v4.3.16

MONITORING CONFIGURATION EVA1 root

admin WRITING LOGS RESTRICTED ACCESS

CONFIGURATION

Search...

Temporary accounts

Access privileges

Authentication

Enrolment

Directories configuration

SECURITY POLICY

Filter - NAT

URL filtering

SSL filtering

SMTP filtering

QoS

Implicit rules

APPLICATION PROTECTION

Applications and protection

Protocols

Inspection profile

Vulnerability manager

Host reputation

OBJECTS

SECURITY POLICY / URL FILTERING

(0) URLFilter_00 Edit URL database provider: Embedded URL database

+ Add X Delete Up Down Cut Copy Paste + Add all predefined categories Check URL classification

Status	Action	URL category	Comments
1 on	BlockPage_00	blacklist	authorize the URLs of authentication_bypass group
2 on	BlockPage_00	news	default rule (pass all)
3 on	BlockPage_00	shopping	
4 on	Pass	Any	

ERRORS FOUND IN THE URL FILTER POLICY

URL CATEGORIES

CANCEL APPLY

8°C Nuageux

Rechercher

21:53 15/11/2024

De plus, on met en place une blacklist de site web :

The screenshot shows the Stormshield Network Security v4.3.16 Configuration page. The left sidebar contains a navigation menu with sections: CONFIGURATION (High Availability, Management Center, CLI), NETWORK (Interfaces, Virtual interfaces, Routing, Multicast routing, Dynamic DNS, DHCP, DNS cache proxy), OBJECTS (Network, URL, Certificates and PKI), and USERS (Users and Groups, Temporary accounts). The main content area is titled 'OBJECTS / URL' and has tabs for 'URL', 'CERTIFICATE NAME (CN)', 'GROUPS OF CATEGORIES', and 'URL DATABASE'. The 'URL' tab is active, showing a table with columns 'URL category' and 'Comments'. The table lists 'vpnsel_owa', 'antivirus_bypa...', 'authentication...', 'blacklist' (highlighted in green), 'news', and 'shopping'. To the right, the 'Authorized characters' section shows the allowed character set: '* ? / : ; , [a - z] [0 - 9]' with an example 'www.google.com/*' or '*.yahoo.com/*'. Below this, the 'URL CATEGORY: BLACKLIST' section has an 'Add a URL' button and a table with columns 'URL' and 'Comments'. The table contains one entry: '*neverssl.com/*'. The bottom status bar shows '8°C Nuageux' and the date '15/11/2024'.

The screenshot shows the Stormshield Network Security v4.3.16 Configuration page, specifically the 'CERTIFICATE NAME (CN)' category configuration. The left sidebar is identical to the previous screenshot. The main content area is titled 'OBJECTS / URL' and has tabs for 'URL', 'CERTIFICATE NAME (CN)', 'GROUPS OF CATEGORIES', and 'URL DATABASE'. The 'CERTIFICATE NAME (CN)' tab is active, showing a table with columns 'Certificate name (CN) category' and 'Comments'. The table lists 'shopping', 'proxysl_bypass', 'news', 'White-list' (highlighted in green), and 'Black-list'. To the right, the 'Authorized characters' section shows the allowed character set: '* ? / : ; , [a - z] [0 - 9]' and '*' are allowed. The character '*' is only valid if placed at the beginning of the URL and immediately followed by a dot. Below this, the 'CERTIFICATES CATEGORY: WHITE-LIST' section has an 'Add a certificate name' button and a table with columns 'Certificate name (CN)' and 'Comments'. The table contains three entries: 'bbc.co.uk', '*.bbc.com', and '*.bbc.co.uk'. The bottom status bar shows '8°C Nuageux' and the date '15/11/2024'.