



DFL-200/700/1100

Konfiguracja Content Filtering

1. Należy zalogować się za pomocą przeglądarki internetowej Internet Explorer do urządzenia na konto administratora (domyślny adres: 192.168.1.1).
2. Po prawidłowej autoryzacji przejść do zakładki firewall i następnie do opcji Services:

D-Link
Building Networks for People

DFL-700
Network Security Firewall

System **Firewall** Servers Tools Status Help

Services Settings

Pick a service to edit from the below list:

Help

Defined services

Name	Parameters	
igmp	IP Protocol: 2	[Edit]
rsvp	IP Protocol: 46	[Edit]
gre-encap	IP Protocol: 47	[Edit]
ipsec-esp	IP Protocol: 50	[Edit]
ipsec-ah	IP Protocol: 51	[Edit]
ipsec-nat	UDP: All -> 4500	[Edit]
ipip-encap	IP Protocol: 94	[Edit]
ipcomp	IP Protocol: 108	[Edit]
l2tp-encap	IP Protocol: 115	[Edit]
echo	TCP/UDP: All -> 7	[Edit]
chargen	TCP/UDP: All -> 19	[Edit]
ssh	TCP: All -> 22	[Edit]
ssh-in	TCP: All -> 22 SYN Relay	[Edit]
telnet	TCP: All -> 23	[Edit]
smtp	TCP: All -> 25	[Edit]
smtp-in	TCP: All -> 25 SYN Relay	[Edit]

3. Wybrać opcję Add New i wypełnić formularz następującymi danymi:

- Name: http-all-content-ALG
- Zaznaczyć opcje TCP
- Destination port: 80
- ALG: http/html Content Filtering

The screenshot shows the Mikrotik WinBox interface for configuring a service. The left sidebar contains navigation buttons for Policy, Port Mapping, Users, Schedules, Services (highlighted in yellow), VPN, Certificates, and Content Filtering. The main window has a menu bar with System, Firewall, Servers, Tools, Status, and Help. The 'Services Settings' section is active, showing the following configuration:

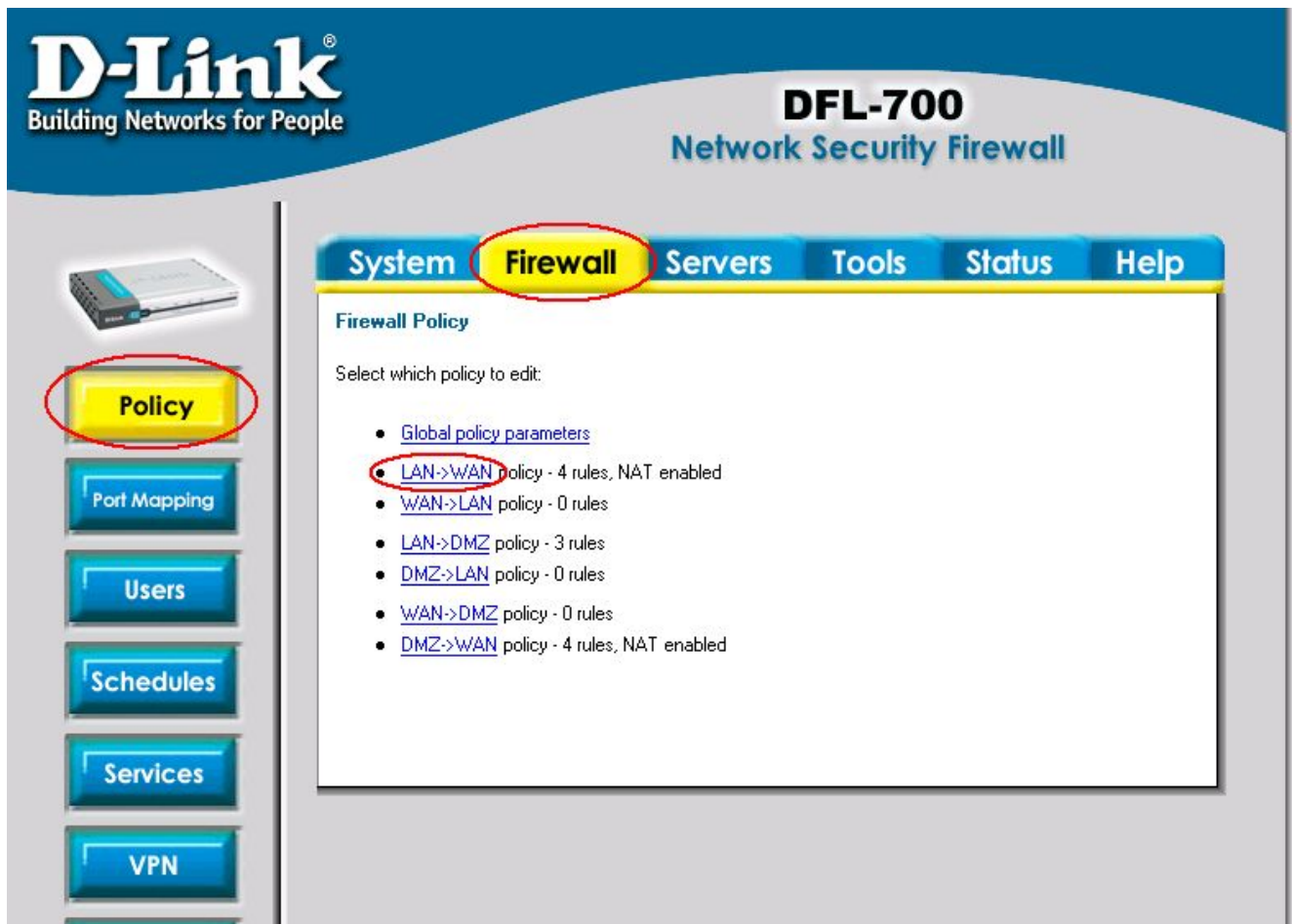
- Name:** http-all-content-ALG
- TCP / UDP Service:** Selected radio button.
- Protocol:** TCP, UDP
- Source Ports:** (empty field)
- Destination Ports:** 80
- SYN Relay:** Protect the destination from SYN flood attacks
- ICMP Echo (Ping):**
- IP Protocol:**
 - Protocols:** (empty field)
 - Example: "1-5, 9, 15, 50-51"
- Group:**
 - Services:** (empty field)
 - Comma-separated list of services or service groups.

Protocol-independent settings:

- ICMP Errors:** Allow ICMP errors from the destination to the source
- ALG:** HTTP/HTML Content Filtering
- Max ALG Sessions:** 100

Application Layer Gateways (ALGs) implement extra application logic that is needed for some protocols to work properly, like for instance FTP, which needs to open up dynamic data channels in addition to the command channel.

4. Wejść do opcji Policy, a następnie do ustawień LAN->WAN:



5. Nacisnąć Edit przy wpisie allow_standard:

LAN->WAN Policy					
Name	Action	Source	Destination	Service	
#1 drop_smb-all	Drop	Any	Any	smb-all	↓ [Edit]
#2 allow_ping-outbound	Allow	Any	Any	ping-outbound	↑↓ [Edit]
#3 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	↑↓ [Edit]
#4 allow_standard	Allow	Any	Any	All Protocols	↑ [Edit]
[Add new]					

6. Następnie zaznaczyć opcję: Delete this rule i potwierdzić Apply:

Intrusion Detection / Prevention:
Mode:
Alerting: Enable IDS/IDP alerting via email for this rule

Traffic shaping - limits and guarantees for WAN traffic:
Limit Guarantee
Upstream: kbit/s kbit/s
Downstream: kbit/s kbit/s
Priority:

Note that priorities and guarantees will only work if the traffic limits for the WAN interface are configured correctly. Simple limits will however always work.

Delete this rule

Apply **Cancel** **Help**

LAN->WAN Policy

Name	Action	Source	Destination	Service	
#1 drop_smb-all	Drop	Any	Any	smb-all	↓ [Edit]
#2 allow_ping-outbound	Allow	Any	Any	ping-outbound	↑↓ [Edit]
#3 allow_ftp-passthrough	Allow	Any	Any	ftp-passthrough	↑↓ [Edit]
#4 allow_standard	Allow	Any	Any	All Protocols	↑ [Edit]

[Add new]

Order of evaluation ↓

7. Następnie dodać dwie nowe reguły:

a) reguła allow_dns

- name allow_dns

- action: allow

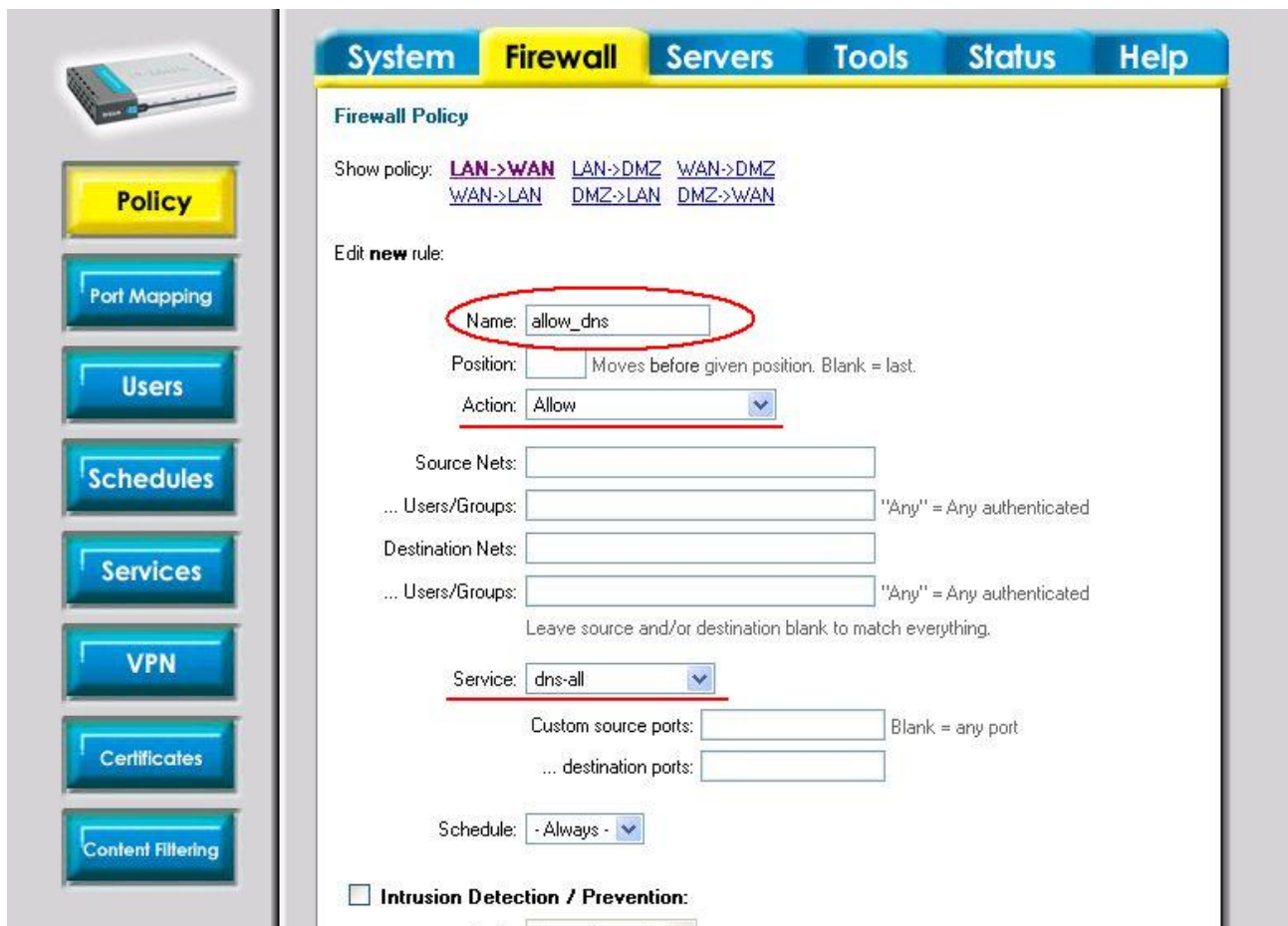
- service: dns_all

b) reguła allow_http

- name: allow_http

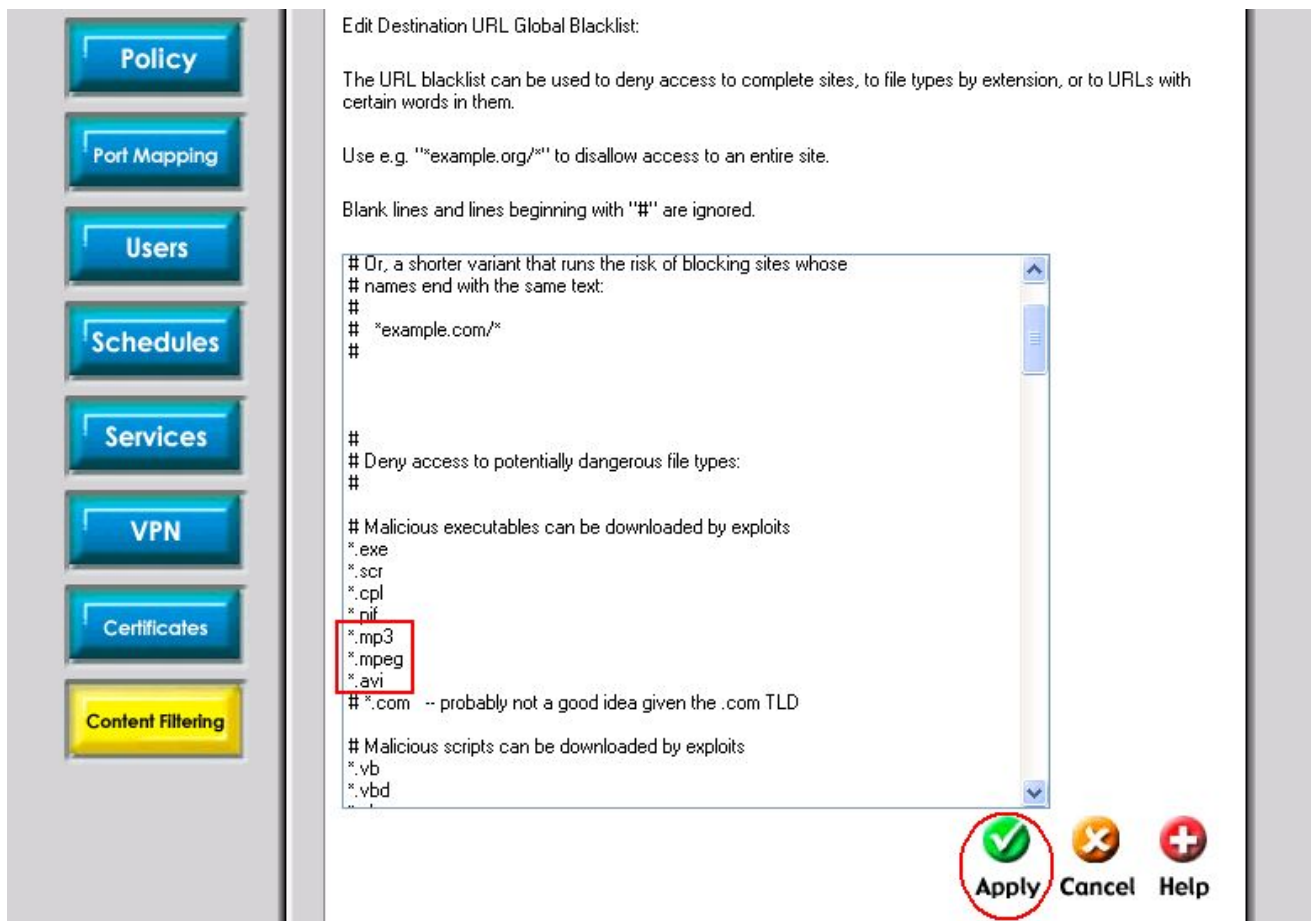
- action: allow

- service: http-all-content-ALG



8. Następnie wybieramy opcję Content Filtering po lewej stronie.

9. Wchodzimy do zawartości URL Blacklist i dodajemy typy plików, które mają być zablokowane np. *.mp3, *.mpeg, *.avi



10. Po wszystkim klikamy na Activate, aby zatwierdzić wszystkie zmiany:





D-Link Polska

ul. Waliców 11
00-851 Warszawa

Telefon: (022) 583-92-75

Fax: (022) 583-92-76



FixIT Sp. z o.o.
ul. Czerwone Maki 65
30-392 Kraków

Wsparcie Techniczne D-Link: (012) 25-44-000

- czynne w godzinach 08-20 w dni powszednie
- koszt połączenia według stawek operatora