



Пример настройки межсетевых экранов D-Link NetDefend

**Как запретить доступ пользователям к
определённым веб сайтам**

Межсетевые экраны: DFL-260E/860E/1660/2560

Прошивка: 2.60.02 и выше.

На межсетевых экранах D-Link NetDefend доступ к веб сайтам ограничивается при помощи HTTP ALG.

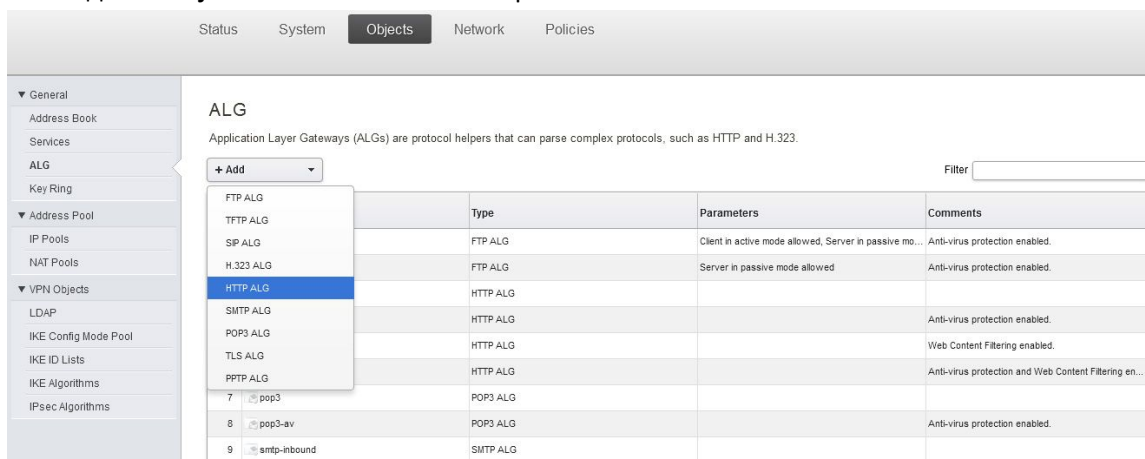
HTTP ALG на межсетевых экранах DFL-210/260/800/860/1600/2500, а также на прошивках ниже 2.60 для устройств DFL-260E/860E/1660/2560 не может анализировать https трафик. Как запретить доступ к сайтам, работающим по протоколу https на DFL-210/260/800/860/1600/2500 или на более ранних прошивках для DFL-260E/860E/1660/2560 смотрите в соответствующем FAQ

<http://www.dlink.ua/sites/default/files/dfl/How%20to%20restrict%20access%20to%20facebook.pdf>.

Запретить доступ к сайтам на прошивках 2.60 и выше можно тремя способами, при помощи функций: Application Control, Web Content Filtering и URL Filter. Функции Application Control и Web Content Filtering требуют приобретения дополнительных подписок, так как функция Application Control использует набор сигнатур для блокировки определённых сайтов или приложений, а функция Web Content Filtering использует внешнюю категоризированную базу URL ресурсов. В данном примере мы рассмотрим, как запретить доступ к сайтам при помощи функции URL Filter.

Инструкция создана для прошивки 2.60. На более ранних прошивках отсутствует функция Application Control и веб интерфейс устройств имеет немного другой вид, но идея настройки блокировки сайтов, работающих по протоколу http остаётся той же.

1. Заходим в **Objects>General>ALG** и выбираем **Add>HTTP ALG**



The screenshot shows the D-Link NetDefend web interface. The top navigation bar has tabs for Status, System, Objects, Network, and Policies. The left sidebar shows a tree view with 'General' expanded, containing Address Book, Services, ALG, and Key Ring. The main content area is titled 'ALG' and contains a description: 'Application Layer Gateways (ALGs) are protocol helpers that can parse complex protocols, such as HTTP and H.323.' Below this is a '+ Add' button and a 'Filter' input field. A table lists existing ALG entries:

	Type	Parameters	Comments
FTP ALG	FTP ALG	Client in active mode allowed, Server in passive mo...	Anti-virus protection enabled.
TFTP ALG	FTP ALG	Server in passive mode allowed	Anti-virus protection enabled.
SP ALG	HTTP ALG		Anti-virus protection enabled.
H.323 ALG	HTTP ALG		Web Content Filtering enabled.
HTTP ALG	HTTP ALG		Anti-virus protection and Web Content Filtering en...
SMTP ALG	POP3 ALG		
POP3 ALG	POP3 ALG		Anti-virus protection enabled.
TLS ALG	POP3 ALG		
PPTP ALG	SMTP ALG		
7 pop3	POP3 ALG		
8 pop3-av	POP3 ALG		Anti-virus protection enabled.
9 smtp-inbound	SMTP ALG		

2. На открывшейся странице (на вкладке **General**) в поле **Name:** вводим **http_block**

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring

▼ Address Pool
IP Pools
NAT Pools

▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG

Use an HTTP Application Layer Gateway to filter HTTP traffic.

General File Integrity Web Content Filtering Anti-Virus URL Filter

Name:

Allowed Protocols: ⚠ For HTTPS only Web Content Filtering and URL Filter are supported. Anti-Virus scanning, Active Content Handling and File Integrity settings will not be applied on HTTPS connections.

Active Content Handling

☐ Strip ActiveX objects (including Flash)

☐ Strip Java applets

☐ Strip Javascript/VBScript

☐ Block Cookies

SafeSearch

☐ Force SafeSearch on Google™, Bing™ and Yahoo!™ search engines

3. Переходим на вкладку **URL Filter** и в появившемся окне выбираем **Add>HTTP ALG URL**

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring

▼ Address Pool
IP Pools
NAT Pools

▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG

Use an HTTP Application Layer Gateway to filter HTTP traffic.

General File Integrity Web Content Filtering Anti-Virus **URL Filter**

+ Add Filter

Action	URL	Comments
HTTP ALG URL		

Right-click on a row for additional options.

OK Cancel

4. В появившемся окне оставляем **Action: Blacklist**, а в поле URL вводим сайт, который необходимо заблокировать и нажимаем **OK**. Например, мы хотим заблокировать сайт `odnoklassniki`, соответственно вводим ***odnoklassniki***. Знак "*" означает наличие любого символа. Т.е. перед текстом "odnoklassniki" и после него могут находиться любые символы. В результате будет заблокирован любой url, в котором встретится текст "odnoklassniki". Блокировать данный сайт лучше именно так, так как он присутствует во многих региональных доменах: ru, ua, kz и т.д. Заблокировав сайт в домене ru, например, вот так ***odnoklassniki.ru*** вы оставите его доступным через другие домены. Также, лучше не прописывать так, как приведено в примере на самой странице HTTP ALG URL, т.е. ***.odnoklassniki.ru/***, так как многие сайты не содержат знак "/" и в частности, сайт `odnoklassniki`. Т.е. в этом случае он, вообще, не будет заблокирован.

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG URL

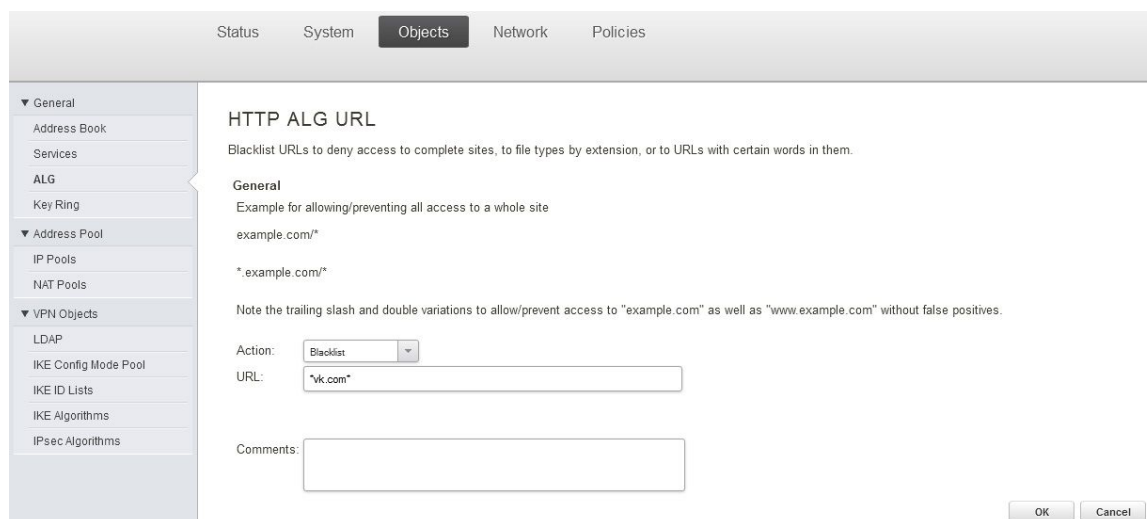
Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

General
Example for allowing/preventing all access to a whole site
`example.com/*`
`*.example.com/*`
Note the trailing slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positives.

Action: Blacklist
URL:
Comments:

OK Cancel

5. Аналогичным способом добавляем другие сайты. Например, необходимо добавить сайт "вконтакте". Для этого в поле URL мы напишем ***vk.com***. Данный сайт лучше блокировать именно так, потому что присутствует он только в домене com. Указывать ***vk*** нельзя, так как данная комбинация встречается в очень многих словах, а соответственно и url запросах, в результате чего будет заблокировано довольно большое количество разрешённых сайтов.



Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG URL

Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

General
Example for allowing/preventing all access to a whole site
example.com/*
.example.com/
Note the trailing slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positives.

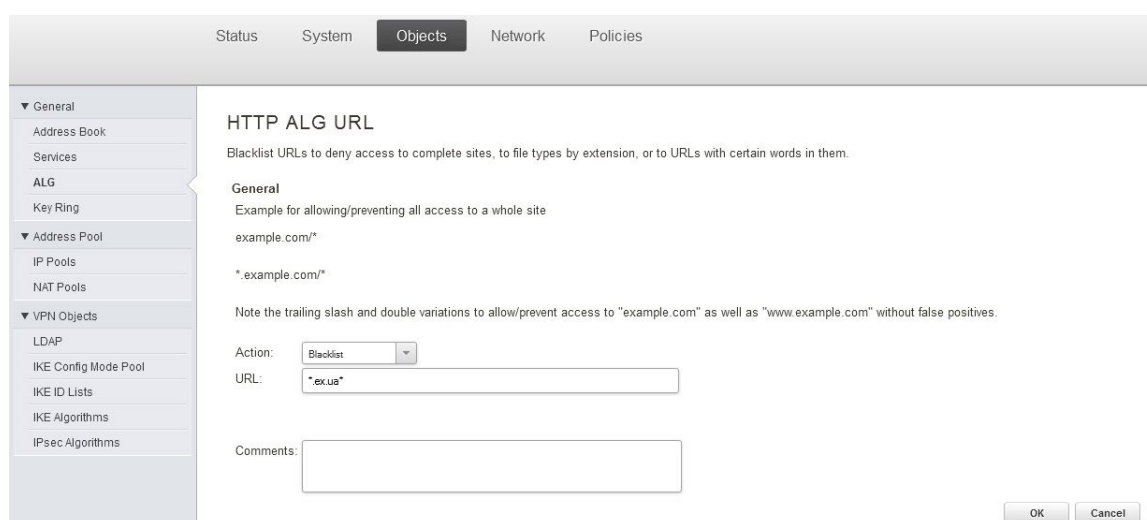
Action:

URL:

Comments:

OK Cancel

6. Рассмотрим ещё один пример добавления сайта. Например, необходимо заблокировать сайт "ex.ua". Комбинация "ex" ещё более популярна, чем ***vk***. Мало того, в домене "ua" присутствует сайт, который тоже заканчивается на ex.ua – это yandex.ua. Т.е. если мы укажем в поле url ***ex.ua***, то сайт yandex.ua тоже будет заблокирован. Поэтому для ex.ua мы укажем ***.ex.ua***. Второй способ, при помощи которого можно заблокировать ex.ua, но разрешить доступ к yandex.ua – это добавление yandex.ua в whitelist. Если в одном http alg встречаются white и black листы, то white листы имеют более высокий приоритет перед black листами.



Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG URL

Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

General
Example for allowing/preventing all access to a whole site
example.com/*
.example.com/
Note the trailing slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positives.

Action:

URL:

Comments:

OK Cancel

7. Добавим для примера ещё один сайт – facebook. Для него укажем *facebook*.

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

HTTP ALG URL

Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them.

General
Example for allowing/preventing all access to a whole site
example.com/*
.example.com/

Note the trailing slash and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positives.

Action: Blacklist

URL:

Comments:

OK Cancel

В результате получаем вот такой список запрещённых сайтов.

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

http_block

Use an HTTP Application Layer Gateway to filter HTTP traffic.

General File Integrity Web Content Filtering Anti-Virus **URL Filter**

+ Add Filter

Action	URL	Comments
Blacklist	*odnoklassniki*	
Blacklist	*vk.com*	
Blacklist	*ex.ua*	
Blacklist	*facebook*	

Right-click on a row for additional options.

OK Cancel

8. Теперь, необходимо создать сервис, к которому привязать, созданный выше http alg. Для этого заходим в **Objects> General>Services** и выбираем **Add>TCP/UDP Service**

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool
IKE ID Lists
IKE Algorithms
IPsec Algorithms

Services

Services are pre-defined or user-defined objects representing various IP protocols, such as HTTP, FTP and Telnet.

+ Add Filter

Type	Parameters	Protocol	ALG Info	Comments
TCP/UDP Service				
ICMP Service				
IPv6-ICMP Service	Group	ICMPv6		L2TP control and transport, unen...
IP Protocol Service	IPProto	50		IPsec ESP (encrypted and auth...
Service Group	IPProto	51		IPsec AH (authenticated only)
4 IPsec-nat	UDP	4500		IPsec NAT-traversal (through ud...
5 IPsec-suite	Group	IPsec-nat, IPsec-ah, IPsec-esp, IP...		The IPsec-RE suite
6 ftp-passthrough-av	TCP	21	ftp-passthrough-av - AV Protect	FTP - unrestricted - allows all tra...
7 ftp-outbound-av	TCP	21	ftp-outbound-av - AV Protect	FTP - protects client against data...
8 http-outbound	TCP	80	http-outbound	HTTP via HTTP ALG

9. Указываем:

Name: http_block

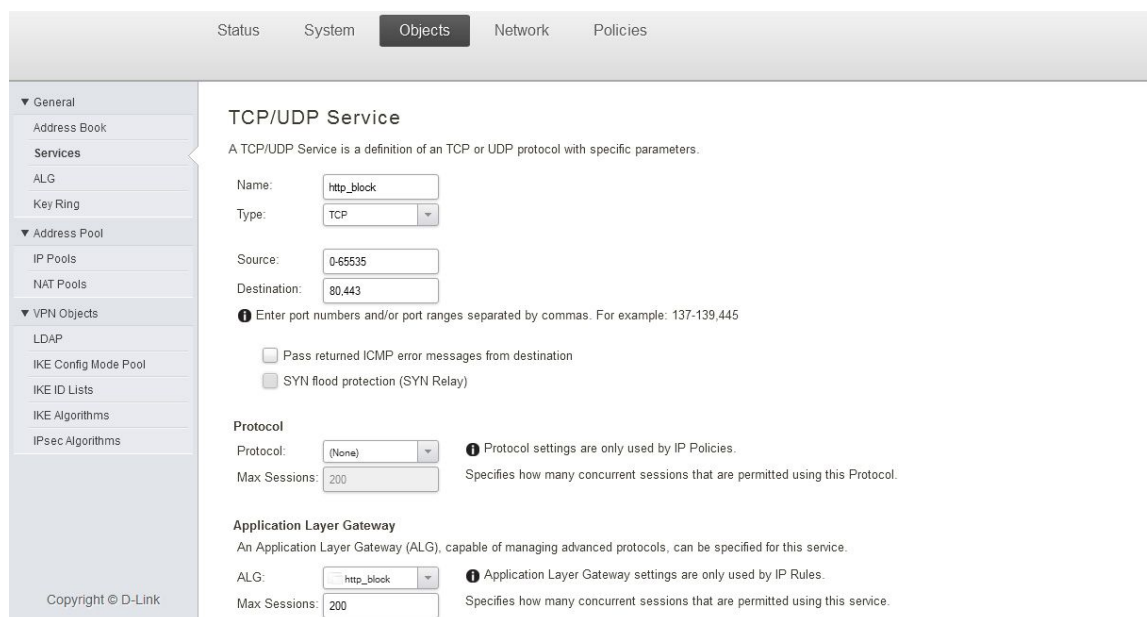
Type: TCP

Source: 0-65535

Destination: 80,443

ALG: http_block

и нажимаем **ОК**.



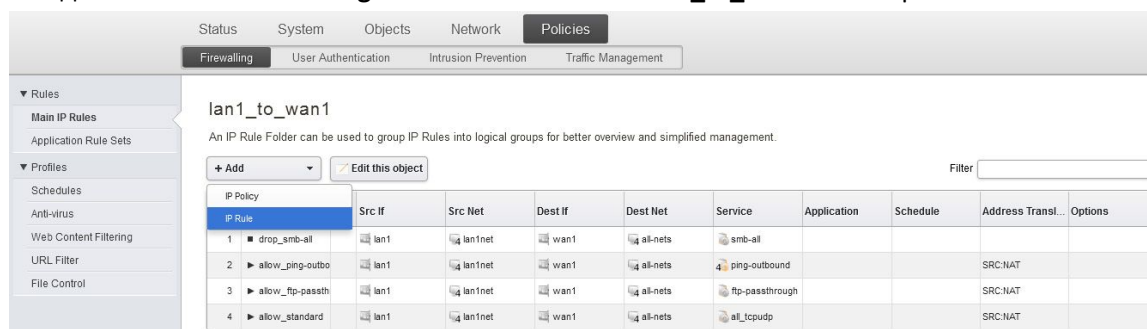
The screenshot shows the 'Objects' tab in the D-Link web interface. The left sidebar contains a tree view with 'General' expanded, showing 'Address Book', 'Services', 'ALG', 'Key Ring', 'Address Pool', 'VPN Objects', 'LDAP', 'IKE Config Mode Pool', 'IKE ID Lists', 'IKE Algorithms', and 'IPsec Algorithms'. The main content area is titled 'TCP/UDP Service'. It contains the following fields and options:

- Name:** http_block
- Type:** TCP
- Source:** 0-65535
- Destination:** 80,443
- Protocol:** (None)
- Max Sessions:** 200
- Application Layer Gateway (ALG):** http_block
- Max Sessions:** 200

There are also checkboxes for 'Pass returned ICMP error messages from destination' and 'SYN flood protection (SYN Relay)'. Informational text states: 'A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.' and 'Protocol settings are only used by IP Policies. Specifies how many concurrent sessions that are permitted using this Protocol.'

10. Теперь необходимо создать правило.

Заходим в **Policies>Firewalling>Rules>Main IP Rules>lan1_to_wan1** и выбираем **Add>IP Rule**



The screenshot shows the 'Policies' tab in the D-Link web interface. The left sidebar contains a tree view with 'Rules' expanded, showing 'Main IP Rules', 'Application Rule Sets', 'Profiles', 'Schedules', 'Anti-virus', 'Web Content Filtering', 'URL Filter', and 'File Control'. The main content area is titled 'lan1_to_wan1'. It contains the following fields and options:

- IP Policy:** IP Rule
- Src If:** lan1
- Src Net:** lan1net
- Dest If:** wan1
- Dest Net:** all-nets
- Service:** smb-all
- Application:** ping-outbound
- Schedule:** (empty)
- Address Transl...:** SRC:NAT
- Options:** (empty)

There are also buttons for '+ Add' and 'Edit this object'. A table at the bottom lists the rules:

IP Policy	Src If	Src Net	Dest If	Dest Net	Service	Application	Schedule	Address Transl...	Options
1	drop_smb-all	lan1	lan1net	wan1	all-nets	smb-all			
2	allow_ping-outbo	lan1	lan1net	wan1	all-nets	ping-outbound		SRC:NAT	
3	allow_ftp-passth	lan1	lan1net	wan1	all-nets	ftp-passthrough		SRC:NAT	
4	allow_standard	lan1	lan1net	wan1	all-nets	all_tcpudp		SRC:NAT	

11. Указываем:

Name: http_block

Action: NAT

Service: http_block

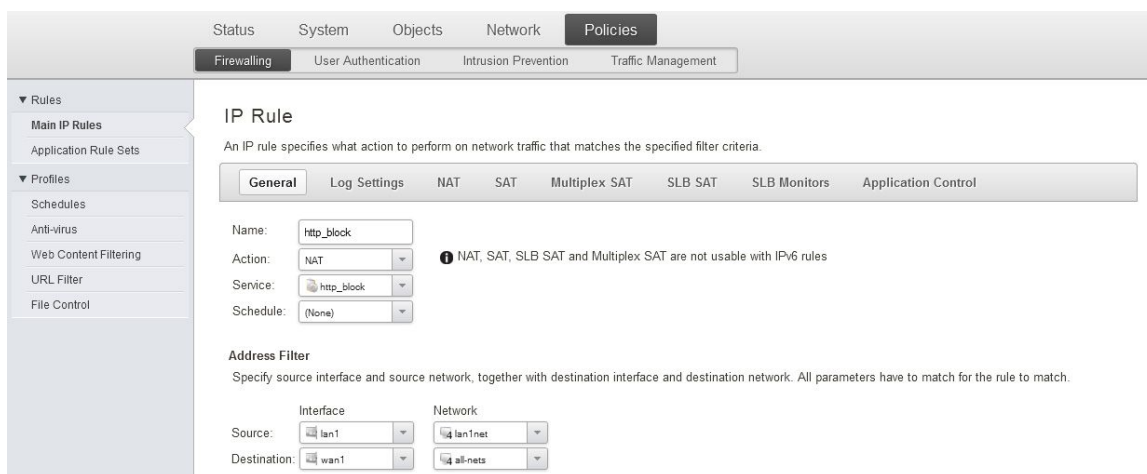
Source Interface: lan1

Source Network: lan1net

Destination Interface: wan1

Destination Network: all-nets

и нажимаем **ОК**.



IP Rule

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT SLB SAT SLB Monitors Application Control

Name:

Action: 1 NAT, SAT, SLB SAT and Multiplex SAT are not usable with IPv6 rules

Service:

Schedule:

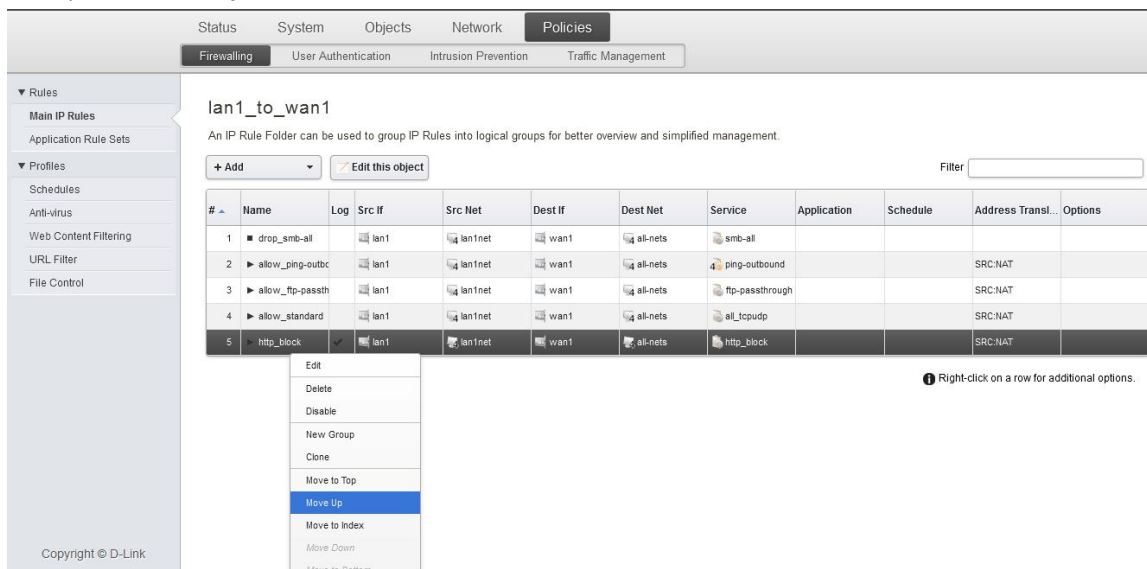
Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: Interface Network

Destination:

12. На созданном правиле нажимаем правой кнопкой мышки и в появившемся меню выбираем **Move Up**.



lan1_to_wan1

An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

#	Name	Log	Src If	Src Net	Dest If	Dest Net	Service	Application	Schedule	Address Transl...	Options
1	drop_smb-all		lan1	lan1net	wan1	all-nets	smb-all				
2	allow_ping-outbc		lan1	lan1net	wan1	all-nets	ping-outbound			SRC:NAT	
3	allow_ftp-passth		lan1	lan1net	wan1	all-nets	ftp-passthrough			SRC:NAT	
4	allow_standard		lan1	lan1net	wan1	all-nets	all_tcpudp			SRC:NAT	
5	http_block		lan1	lan1net	wan1	all-nets	http_block			SRC:NAT	

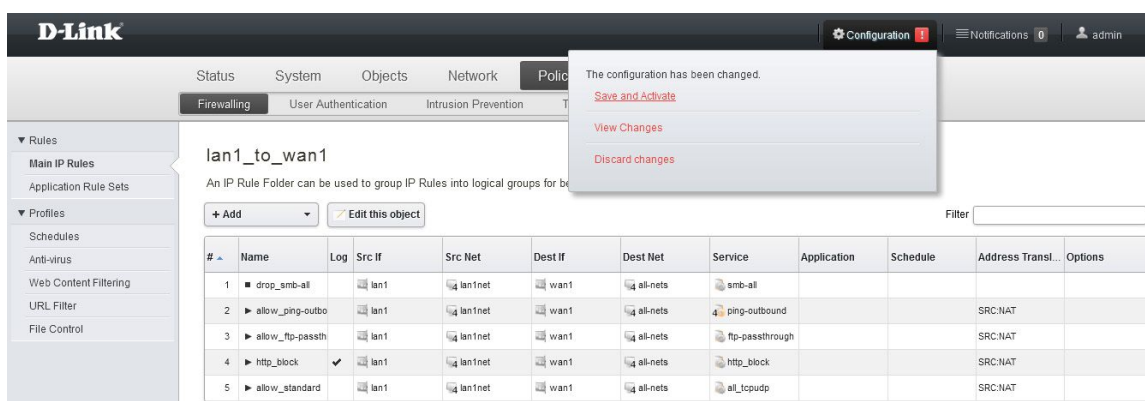
1 Right-click on a row for additional options.

Context menu options: Edit, Delete, Disable, New Group, Clone, Move to Top, **Move Up**, Move to Index, Move Down, Move to Bottom

13. В результате должны получить вот такой вот список правил

#	Name	Log	Src If	Src Net	Dest If	Dest Net	Service	Application	Schedule	Address Transl...	Options
1	drop_smb-all		lan1	lan1net	wan1	all-nets	smb-all				
2	allow_ping-outbo		lan1	lan1net	wan1	all-nets	ping-outbound			SRC:NAT	
3	allow_ftp-passth		lan1	lan1net	wan1	all-nets	ftp-passthrough			SRC:NAT	
4	http_block	<input checked="" type="checkbox"/>	lan1	lan1net	wan1	all-nets	http_block			SRC:NAT	
5	allow_standard		lan1	lan1net	wan1	all-nets	all_tcpudp			SRC:NAT	

14. Сохраняем и активируем конфигурацию. Заходим в **Configuration>Save and Activate** и нажимаем **OK**.



Теперь, если пользователь попытается получить доступ к одному из запрещённых сайтов по протоколу http, то он получит вот такое сообщение в браузере.

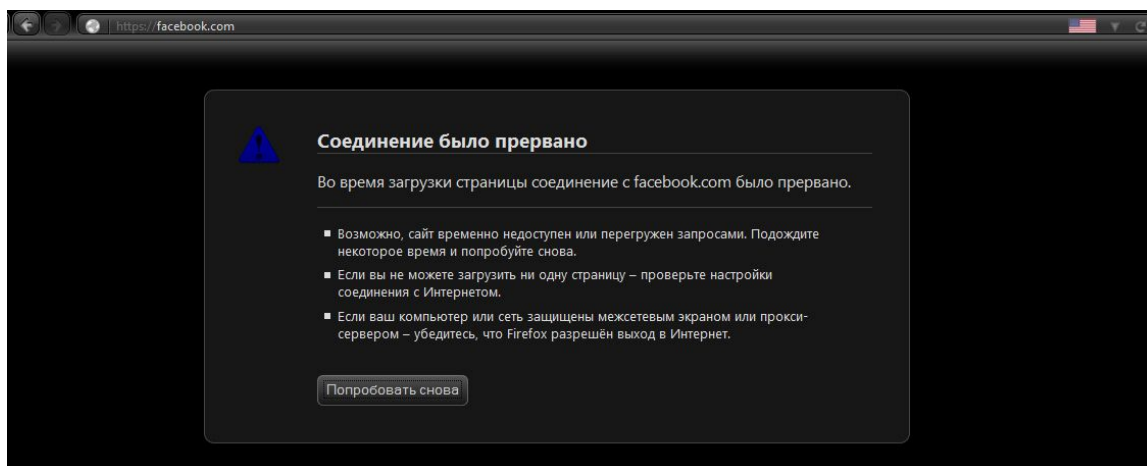


Forbidden:

Access to the location: <http://facebook.com/>

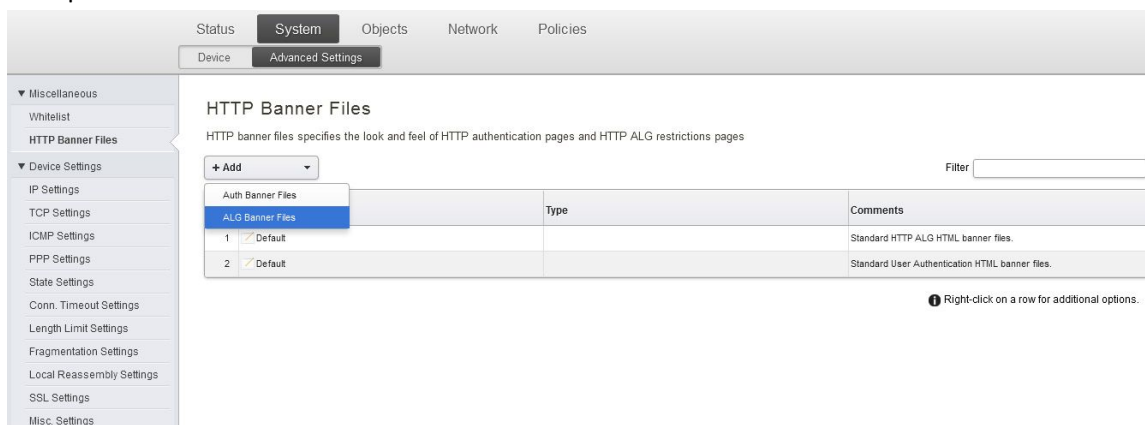
has been denied for the following reason:
Policy prevents this page to be accessed

Если он попытается получить доступ по протоколу https, то получит стандартное уведомление его браузера. В Firefox оно выглядит вот так.



Если необходимо, то html страницу, показываемую при запрещении доступа по http протоколу, можно отредактировать.

15. Для этого заходим в **System>Advanced Settings>Miscellaneous>HTTP Banner Files** и выбираем **Add>ALG Banner Files**



16. В открывшемся окне в поле **Name:** пишем **http_block** и нажимаем **OK**.

The screenshot shows the 'ALG Banner Files' configuration window. The 'Name' field is set to 'http_block'. The 'Comments' field is empty. The 'OK' button is highlighted.

17. В появившемся окне в поле **Page:** выбираем **URL Forbidden**, после чего редактируем html страницу (в примере мы её переведём на русский язык). Нажимаем **Save**, а потом **OK**.

The screenshot shows the 'URL Forbidden' HTML configuration window. The 'Page' dropdown is set to 'URLForbidden'. The HTML code is visible in the editor. The 'Save' button is highlighted.

18. После этого заходим в, созданный нами, ALG. **Objects>General>ALG>http_block**, в поле **HTML Banner** выбираем **http_block** и нажимаем **OK**.

The screenshot shows the D-Link web interface for configuring an ALG object. On the left is a navigation menu with options like ALG, Key Ring, Address Pool, IP Pools, NAT Pools, VPN Objects, LDAP, IKE Config Mode Pool, IKE ID Lists, IKE Algorithms, and IPsec Algorithms. The main area has tabs for General, File Integrity, Web Content Filtering, Anti-Virus, and URL Filter. The 'General' tab is active, showing the following settings:

- Name:** http_block
- Allowed Protocols:** HTTP
- Active Content Handling:**
 - ☐ Strip ActiveX objects (including Flash)
 - ☐ Strip Java applets
 - ☐ Strip Javascript/VBScript
 - ☐ Block Cookies
- SafeSearch:**
 - ☐ Force SafeSearch on Google™, Bing™ and Yahoo!™ search engines
- URL Verification:**
 - ☐ Verify that URLs do not contain invalid UTF8 encoding
- Fail Mode:** Deny
- HTML Banner:** Select the HTML banner object to use with this ALG. HTML Banner: http_block

A warning message states: "For HTTPS only Web Content Filtering and URL Filter are supported. Anti-Virus scanning, Active Content Handling and File Integrity settings will not be applied on HTTPS connections."

19. Сохраняем и активируем конфигурацию.

The screenshot shows the 'Save Configuration' dialog in the D-Link web interface. The top navigation bar includes 'Status', 'System', 'Objects', 'Network', and 'Policies'. Below this are sub-tabs for 'Run-time Information', 'Maintenance', and 'Tools'. The 'Status' tab is active, displaying the 'Save Configuration' section. The text reads: 'Save and activate changes made to the configuration file.' Below this is a section titled 'Save and Activate' with the question 'Are you sure you want to save the configuration?'. A warning message follows: 'An administrator needs to log in within 120 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.' At the bottom right are 'OK' and 'Cancel' buttons.

После чего при попытке доступа к запрещённой http странице получаем следующее сообщение.



Запрещено:

Доступ к странице: <http://facebook.com/>

запрещён по следующей причине:

Policy prevents this page to be accessed