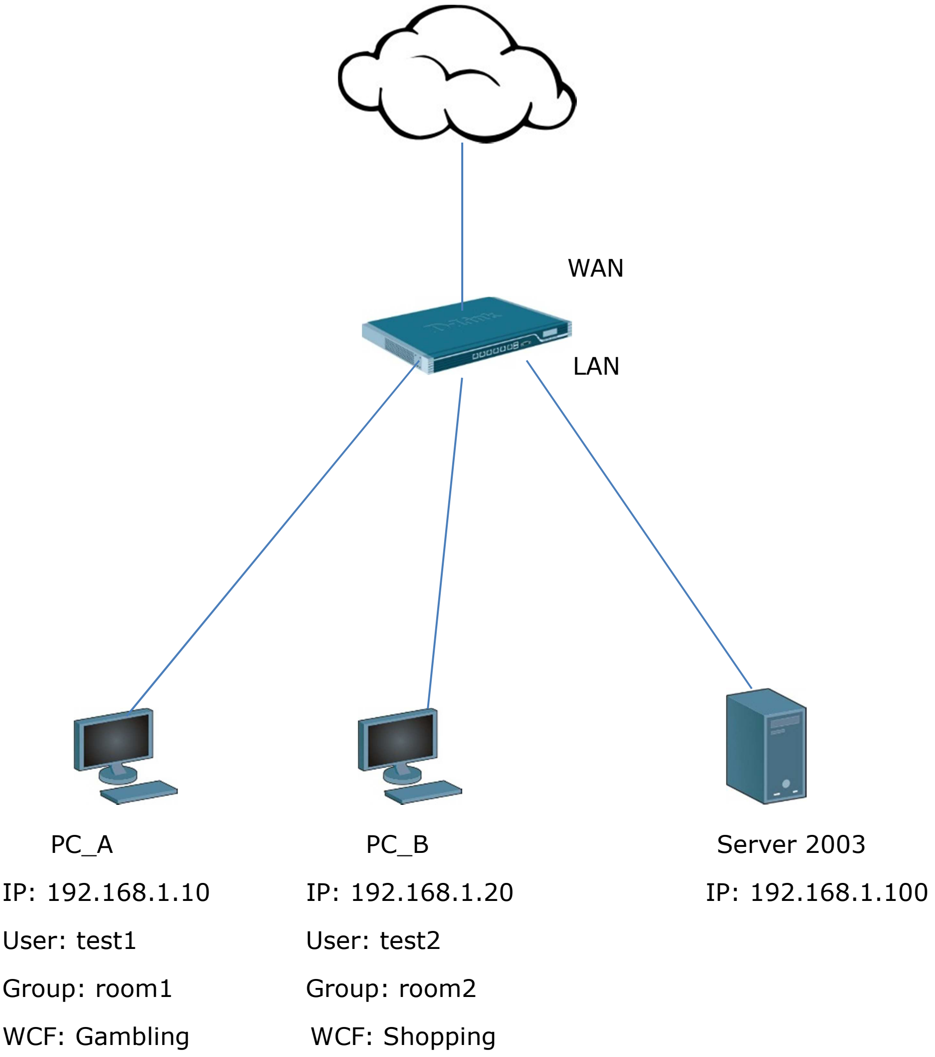
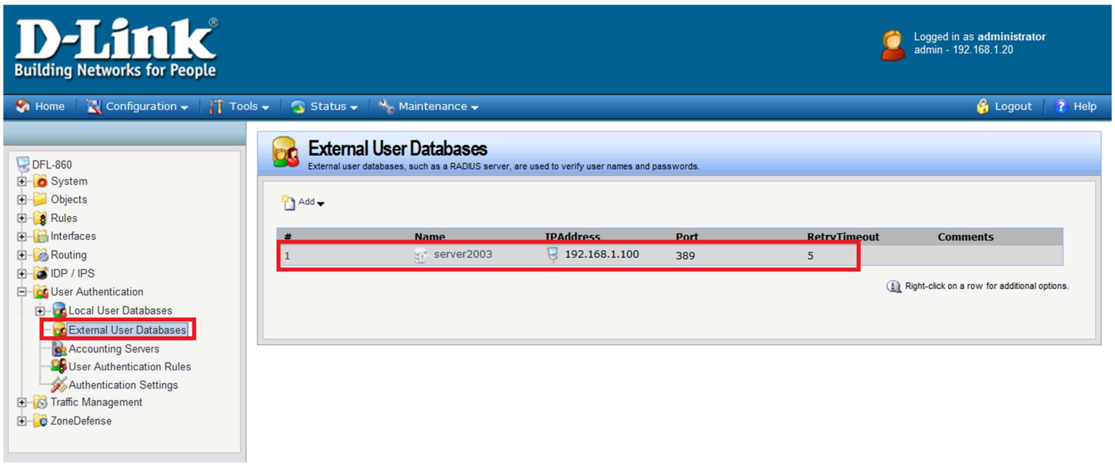
How to configure the DFL-series, to use the group and user created in AD windows 2003, for filters WCF in DFL-firewall.

Topology:



In this example, we have two groups "room1" and "room2". You have different WCF function, if you use different user account and password to login.

(1) Add a new "external user database".

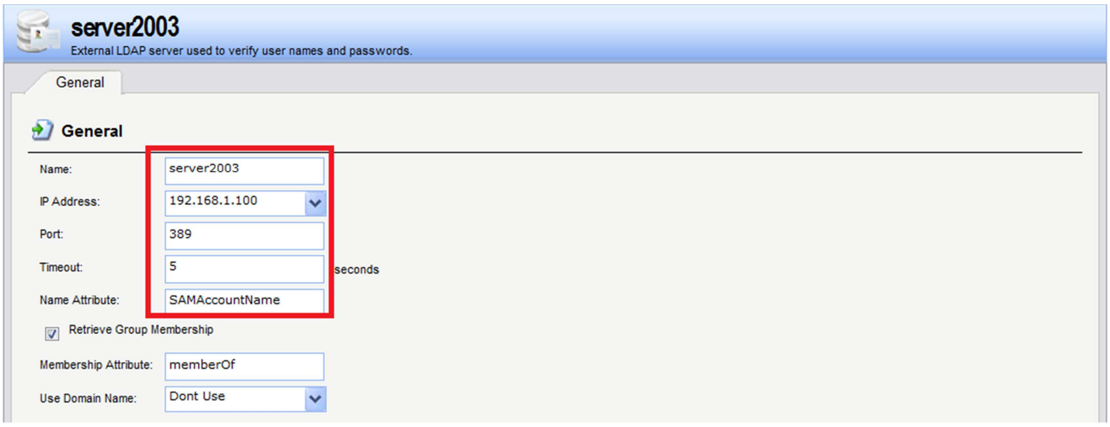


External User Databases

External user databases, such as a RADIUS server, are used to verify user names and passwords.

#	Name	IPAddress	Port	RetryTimeout	Comments
1	server2003	192.168.1.100	389	5	

Right-click on a row for additional options.



server2003

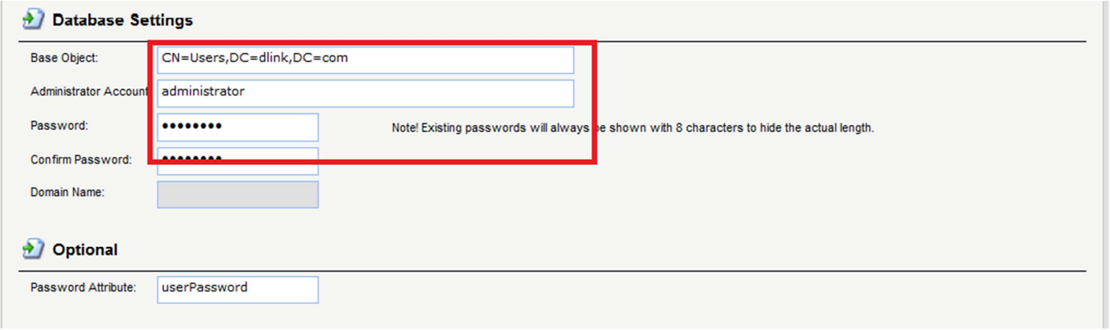
External LDAP server used to verify user names and passwords.

General

Name:	server2003
IP Address:	192.168.1.100
Port:	389
Timeout:	5 seconds
Name Attribute:	SAMAccountName

☑ Retrieve Group Membership

Membership Attribute:	memberOf
Use Domain Name:	Dont Use



Database Settings

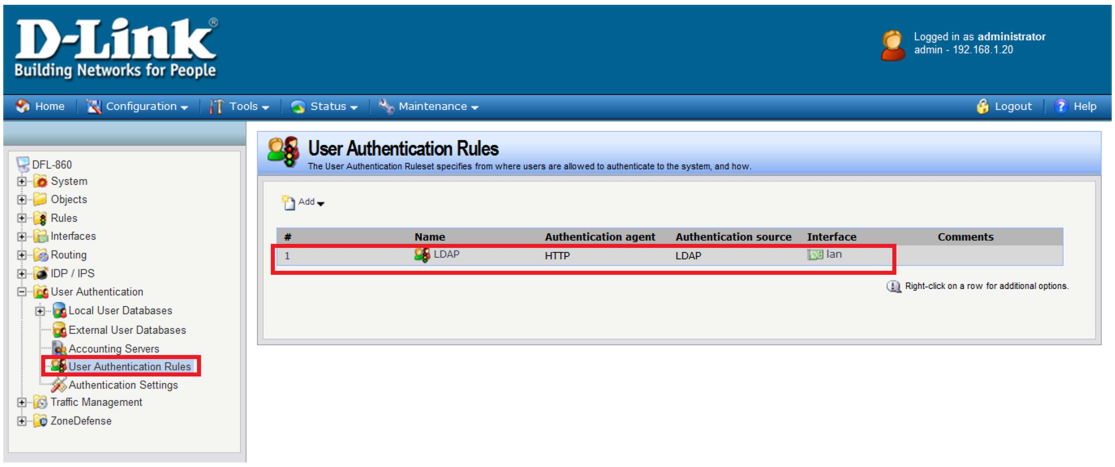
Base Object:	CN=Users,DC=dlink,DC=com
Administrator Account	administrator
Password:	••••••••
Confirm Password:	••••••••
Domain Name:	

Note! Existing passwords will always be shown with 8 characters to hide the actual length.

Optional

Password Attribute:	userPassword

(2) Add a new "user authentication riles".

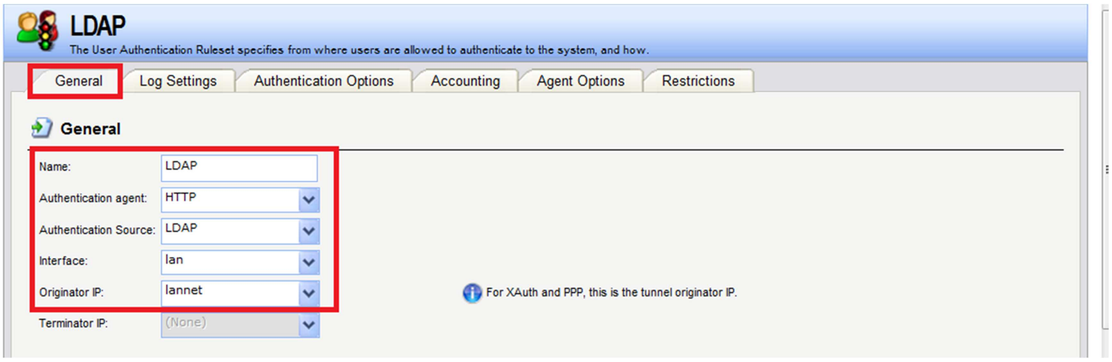


User Authentication Rules

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

#	Name	Authentication agent	Authentication source	Interface	Comments
1	LDAP	HTTP	LDAP	lan	

Right-click on a row for additional options.



LDAP

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

Name: LDAP

Authentication agent: HTTP

Authentication Source: LDAP

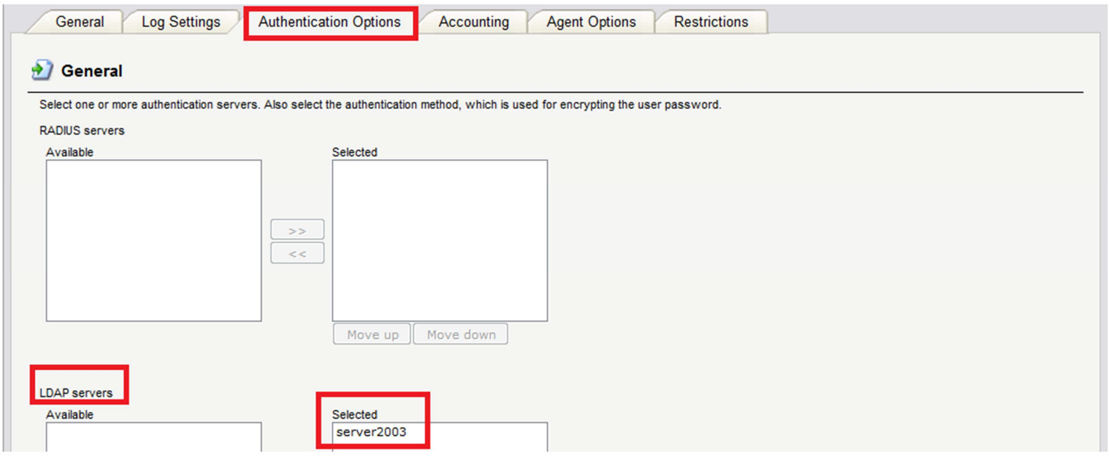
Interface: lan

Originator IP: lannet

For XAuth and PPP, this is the tunnel originator IP.

Terminator IP: (None)

(3) Choose "LDAP servers".



General

Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

RADIUS servers

Available

Selected

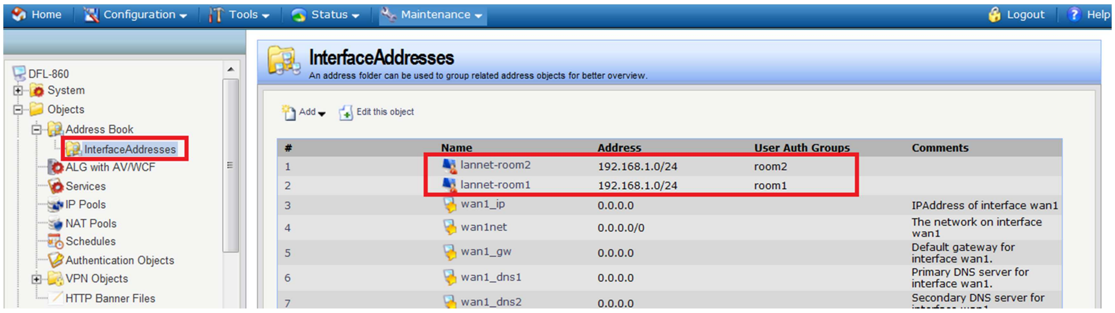
LDAP servers

Available

Selected

server2003

(4) Add two new authentication addresses.

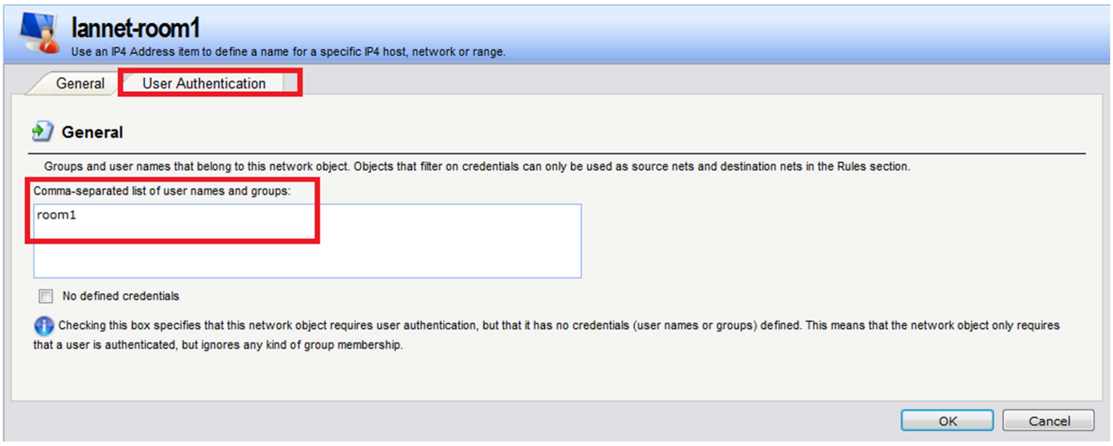


InterfaceAddresses

An address folder can be used to group related address objects for better overview.

#	Name	Address	User Auth Groups	Comments
1	lannet-room2	192.168.1.0/24	room2	
2	lannet-room1	192.168.1.0/24	room1	
3	wan1_ip	0.0.0.0		IPAddress of interface wan1
4	wan1net	0.0.0.0/0		The network on interface wan1
5	wan1_gw	0.0.0.0		Default gateway for interface wan1.
6	wan1_dns1	0.0.0.0		Primary DNS server for interface wan1.
7	wan1_dns2	0.0.0.0		Secondary DNS server for

(5) Authentication group names must be the same with LDAP server.



lannet-room1

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

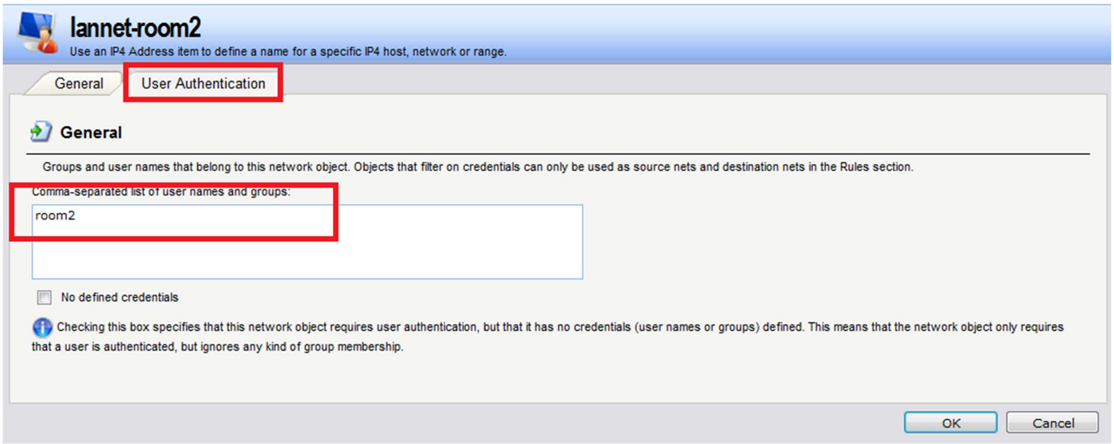
Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destination nets in the Rules section.

Comma-separated list of user names and groups:

room1

□ No defined credentials

Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only requires that a user is authenticated, but ignores any kind of group membership.



lannet-room2

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

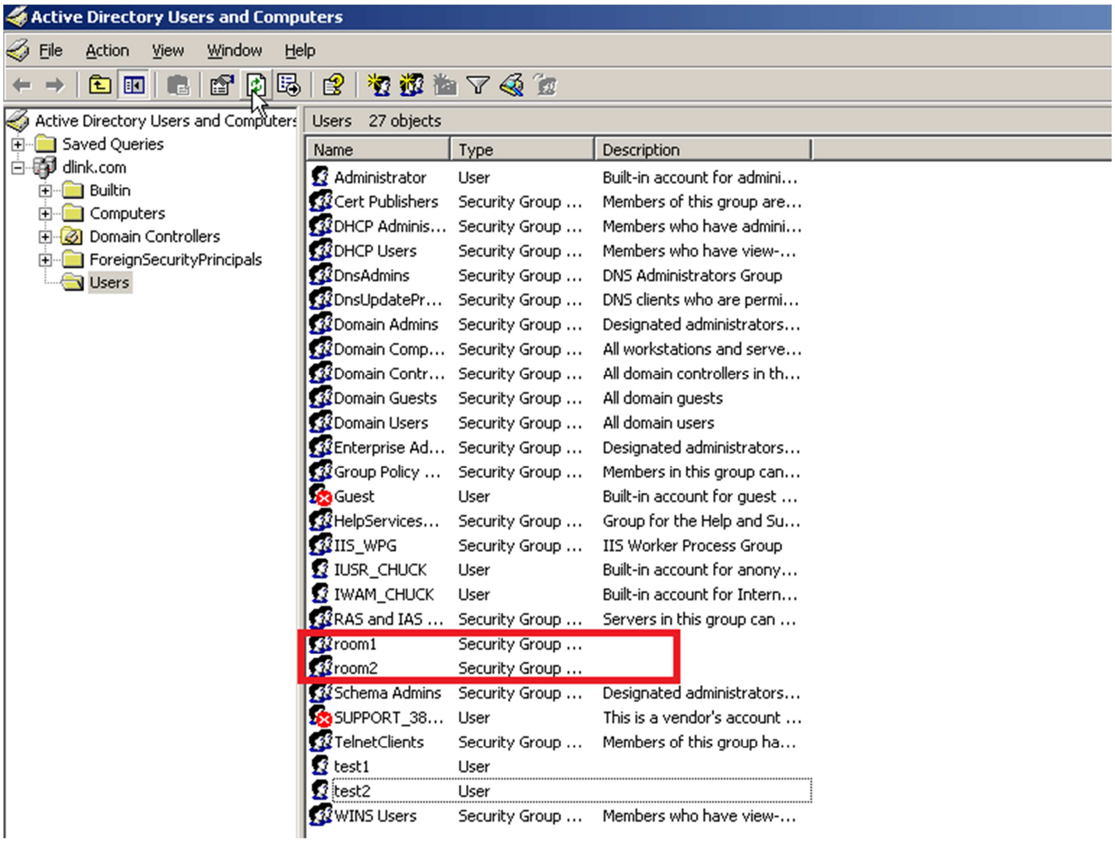
Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destination nets in the Rules section.

Comma-separated list of user names and groups:

room2

□ No defined credentials

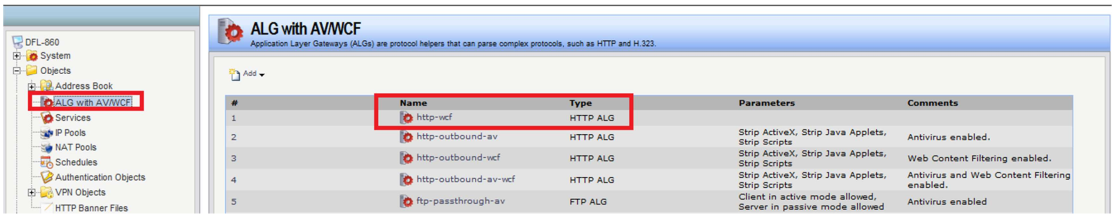
Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only requires that a user is authenticated, but ignores any kind of group membership.


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers
Saved Queries
dlink.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 27 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_CHUCK	User	Built-in account for anony...
IWAM_CHUCK	User	Built-in account for Intern...
RAS and IAS ...	Security Group ...	Servers in this group can ...
room1	Security Group ...	
room2	Security Group ...	
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...
test1	User	
test2	User	
WINS Users	Security Group ...	Members who have view-...

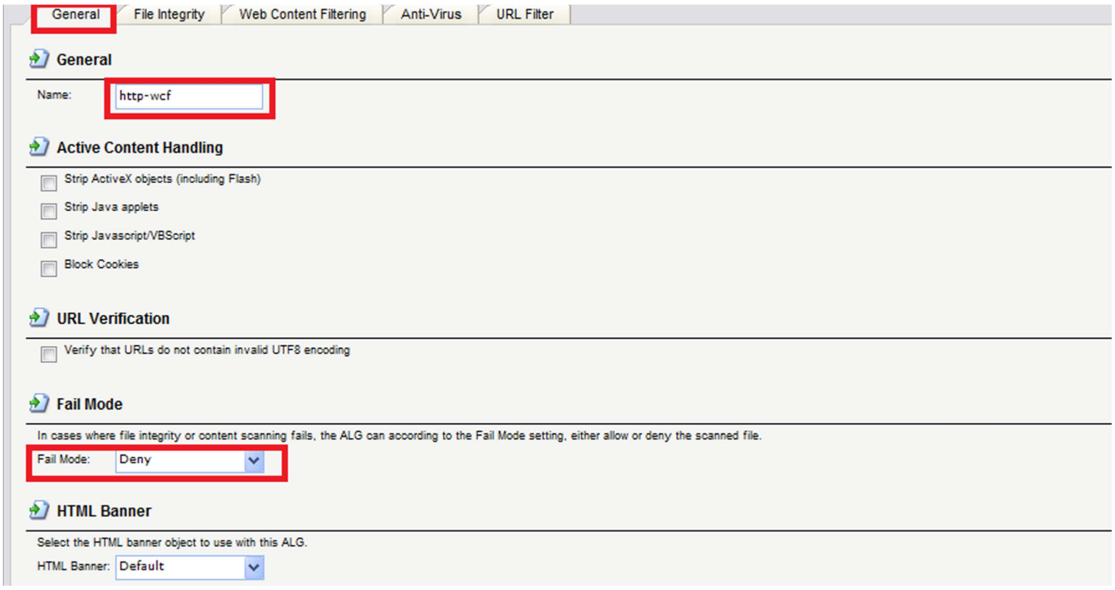
(6) Add a new "HTTP" ALG.



ALG with AV/WCF

Application Layer Gateways (ALGs) are protocol helpers that can parse complex protocols, such as HTTP and H.323.

#	Name	Type	Parameters	Comments
1	http-wcf	HTTP ALG		
2	http-outbound-av	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Antivirus enabled.
3	http-outbound-wcf	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Web Content Filtering enabled.
4	http-outbound-av-wcf	HTTP ALG	Strip ActiveX, Strip Java Applets, Strip Scripts	Antivirus and Web Content Filtering enabled.
5	ftp-passthrough-av	FTP ALG	Client in active mode allowed, Server in passive mode allowed	Antivirus enabled



General

Name: http-wcf

Active Content Handling

□ Strip ActiveX objects (including Flash)

□ Strip Java applets

□ Strip Javascript/VBScript

□ Block Cookies

URL Verification

□ Verify that URLs do not contain invalid UTF8 encoding

Fail Mode

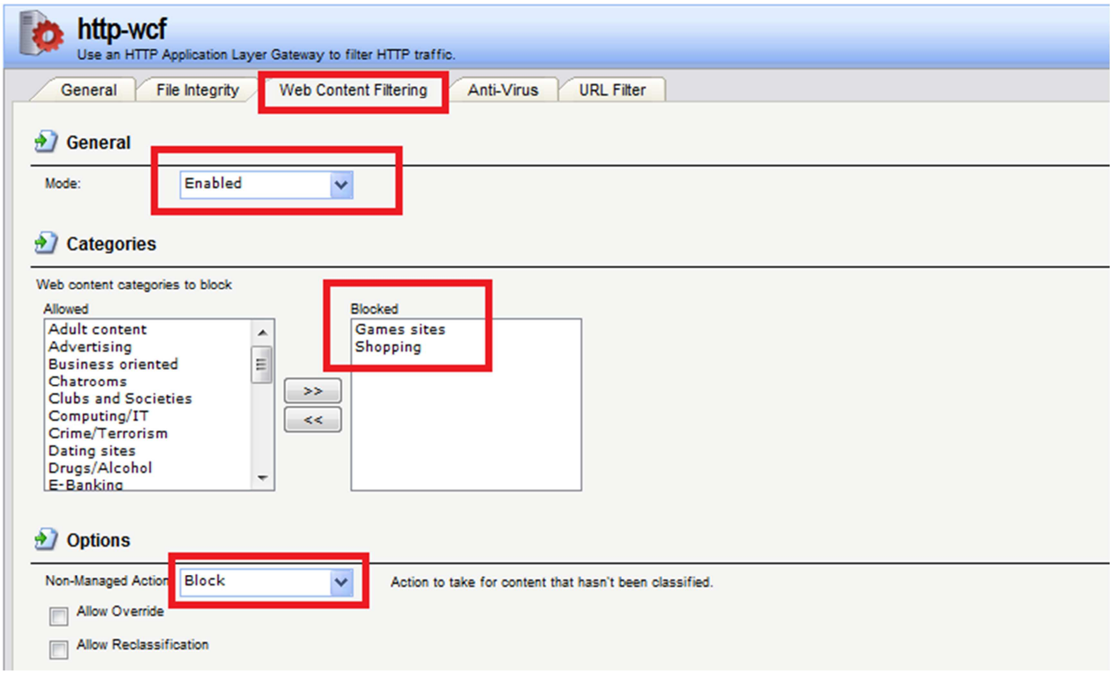
In cases where file integrity or content scanning fails, the ALG can according to the Fail Mode setting, either allow or deny the scanned file.

Fail Mode: Deny

HTML Banner

Select the HTML banner object to use with this ALG.

HTML Banner: Default



http-wcf

Use an HTTP Application Layer Gateway to filter HTTP traffic.

General

Mode: Enabled

Categories

Web content categories to block

Allowed:
- Adult content
- Advertising
- Business oriented
- Chatrooms
- Clubs and Societies
- Computing/IT
- Crime/Terrorism
- Dating sites
- Drugs/Alcohol
- E-Banking

Blocked:
- Games sites
- Shopping

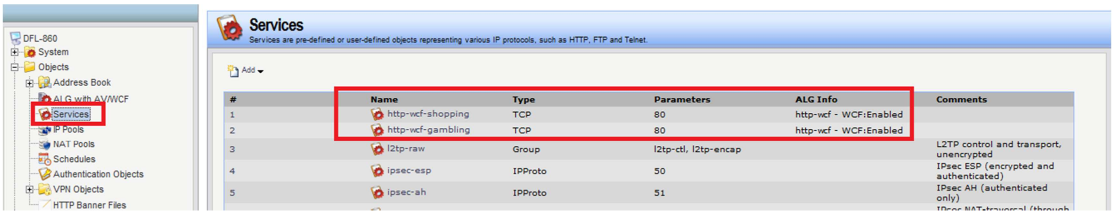
Options

Non-Managed Action: Block — Action to take for content that hasn't been classified.

□ Allow Override

□ Allow Reclassification

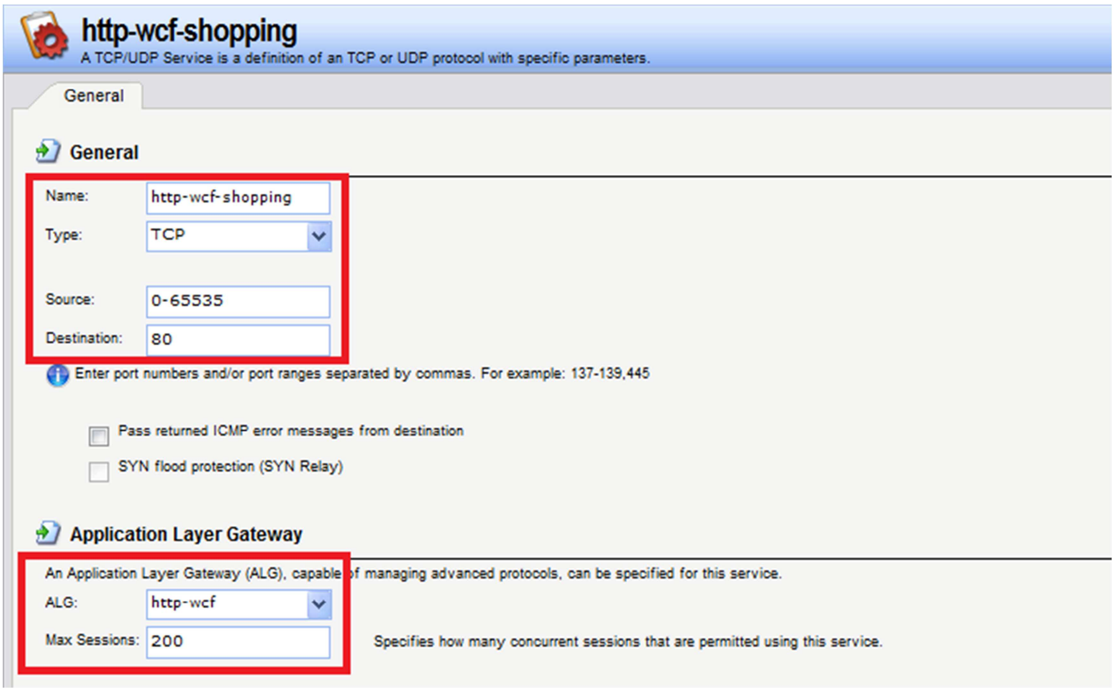
(7) Add two new services "HTTP-WCF-shopping" and "HTTP-WCF-gambling".



Services

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

#	Name	Type	Parameters	ALG Info	Comments
1	http-wcf-shopping	TCP	80	http-wcf - WCF:Enabled	
2	http-wcf-gambling	TCP	80	http-wcf - WCF:Enabled	
3	l2tp-raw	Group	l2tp-ctl, l2tp-encap		L2TP control and transport, unencrypted
4	ipsec-esp	IPProto	50		IPsec ESP (encrypted and authenticated)
5	ipsec-ah	IPProto	51		IPsec AH (authenticated only)



http-wcf-shopping

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

Name: http-wcf-shopping

Type: TCP

Source: 0-65535

Destination: 80

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

□ Pass returned ICMP error messages from destination

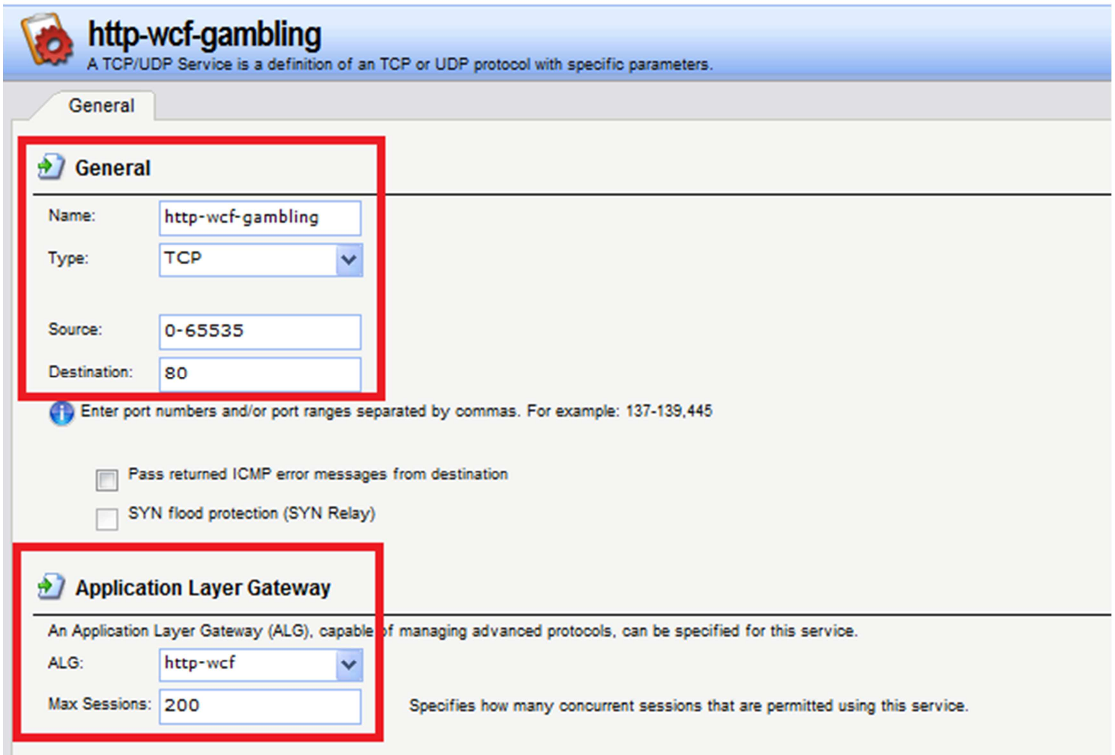
□ SYN flood protection (SYN Relay)

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: http-wcf

Max Sessions: 200 — Specifies how many concurrent sessions that are permitted using this service.



http-wcf-gambling

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

Name: http-wcf-gambling

Type: TCP

Source: 0-65535

Destination: 80

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

□ Pass returned ICMP error messages from destination

□ SYN flood protection (SYN Relay)

Application Layer Gateway

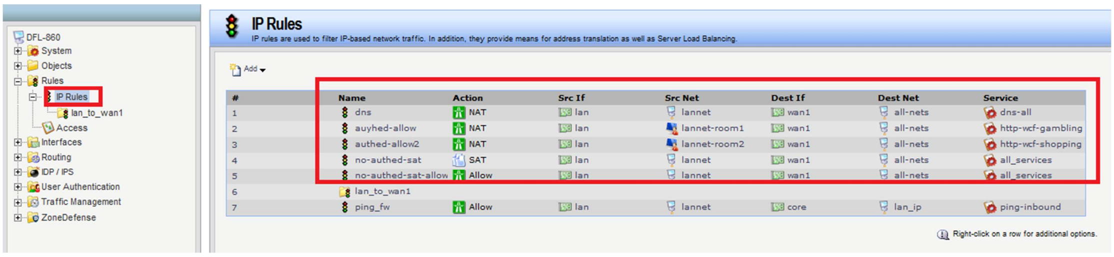
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: http-wcf

Max Sessions: 200

Specifies how many concurrent sessions that are permitted using this service.

(8) Add five IP rules. These are for authentications.



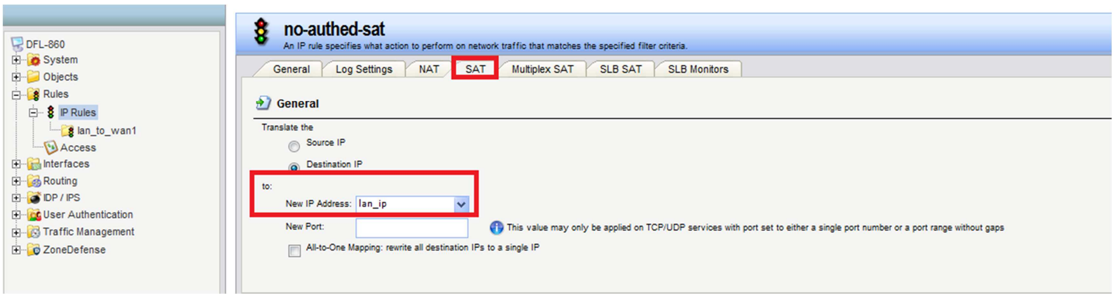
IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	dns	NAT	lan	lannet	wan1	all-nets	dns-all
2	auyhed-allow	NAT	lan	lannet-room1	wan1	all-nets	http-wcf-gambling
3	authed-allow2	NAT	lan	lannet-room2	wan1	all-nets	http-wcf-shopping
4	no-authed-sat	SAT	lan	lannet	wan1	all-nets	all_services
5	no-authed-sat-allow	Allow	lan	lannet	wan1	all-nets	all_services
6	lan_to_wan1						
7	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound

Right-click on a row for additional options.

(9) New IP address have to choose "LAN_IP".



no-authed-sat

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

General

Translate the

○ Source IP

● Destination IP

to:

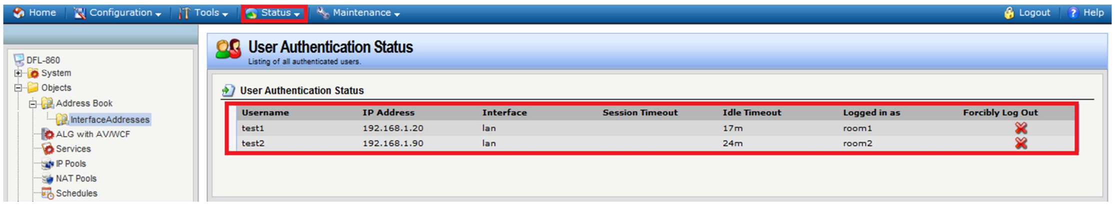
New IP Address: lan_ip

New Port:

This value may only be applied on TCP/UDP services with port set to either a single port number or a port range without gaps

□ All-to-One Mapping: rewrite all destination IPs to a single IP

(10) You can see the status, if you authentication successfully.



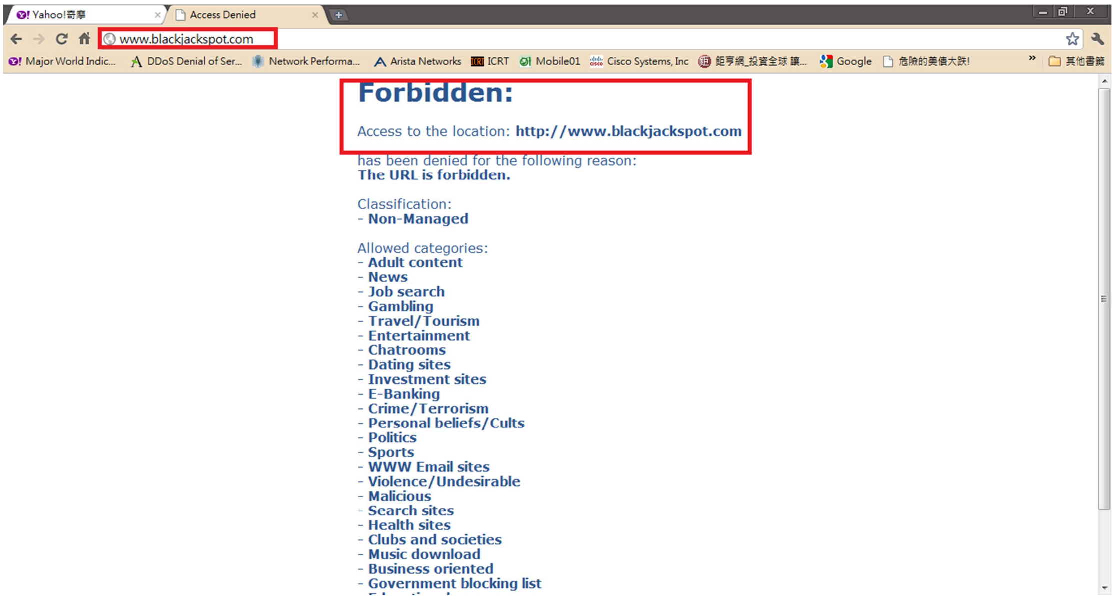
User Authentication Status

Listing of all authenticated users.

User Authentication Status

Username	IP Address	Interface	Session Timeout	Idle Timeout	Logged in as	Forcibly Log Out
test1	192.168.1.20	lan		17m	room1	✗
test2	192.168.1.90	lan		24m	room2	✗

(11) This is forbidden successfully.



Forbidden:

Access to the location: **http://www.blackjackspot.com**

has been denied for the following reason:
The URL is forbidden.

Classification:
- **Non-Managed**

Allowed categories:
- **Adult content**
- **News**
- **Job search**
- **Gambling**
- **Travel/Tourism**
- **Entertainment**
- **Chatrooms**
- **Dating sites**
- **Investment sites**
- **E-Banking**
- **Crime/Terrorism**
- **Personal beliefs/Cults**
- **Politics**
- **Sports**
- **WWW Email sites**
- **Violence/Undesirable**
- **Malicious**
- **Search sites**
- **Health sites**
- **Clubs and societies**
- **Music download**
- **Business oriented**
- **Government blocking list**

END