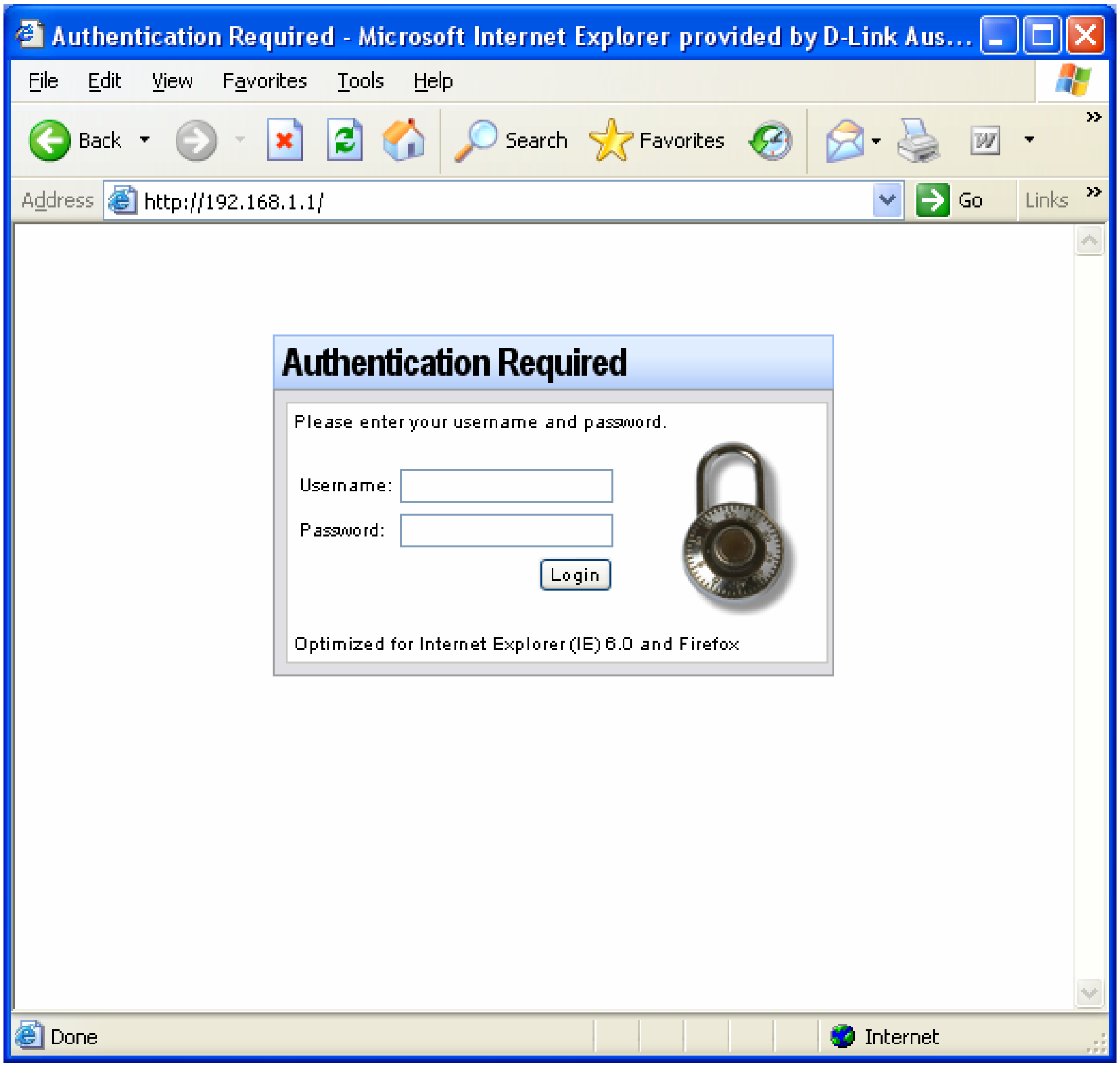
http://192.168.1.1
admin, admin


Authentication Required - Microsoft Internet Explorer provided by D-Link Aus...
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Address
Go
Links
Done
Internet

http://192.168.1.1/

Authentication Required

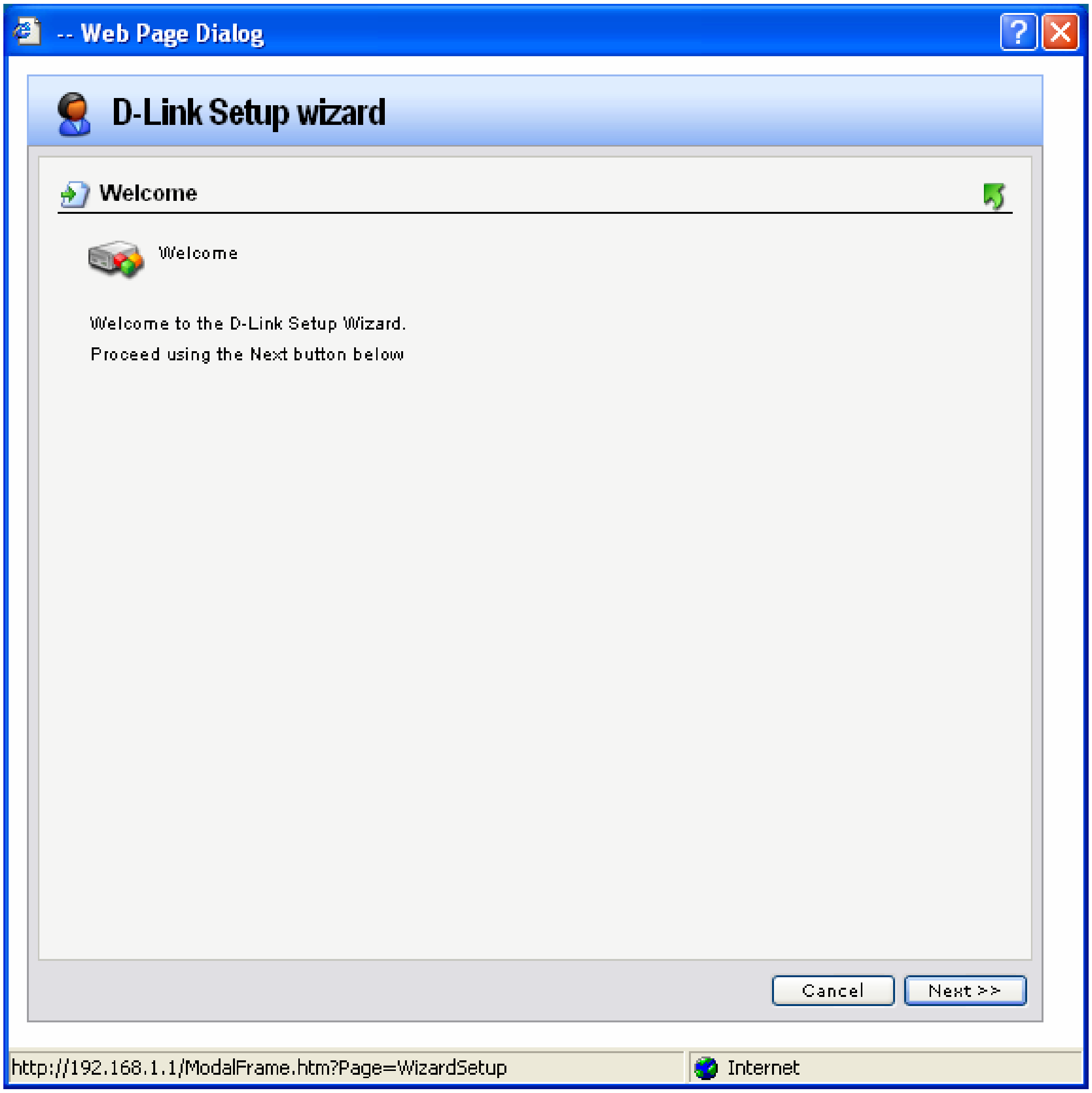
Please enter your username and password.

Username:

Password:

Login

Optimized for Internet Explorer (IE) 6.0 and Firefox



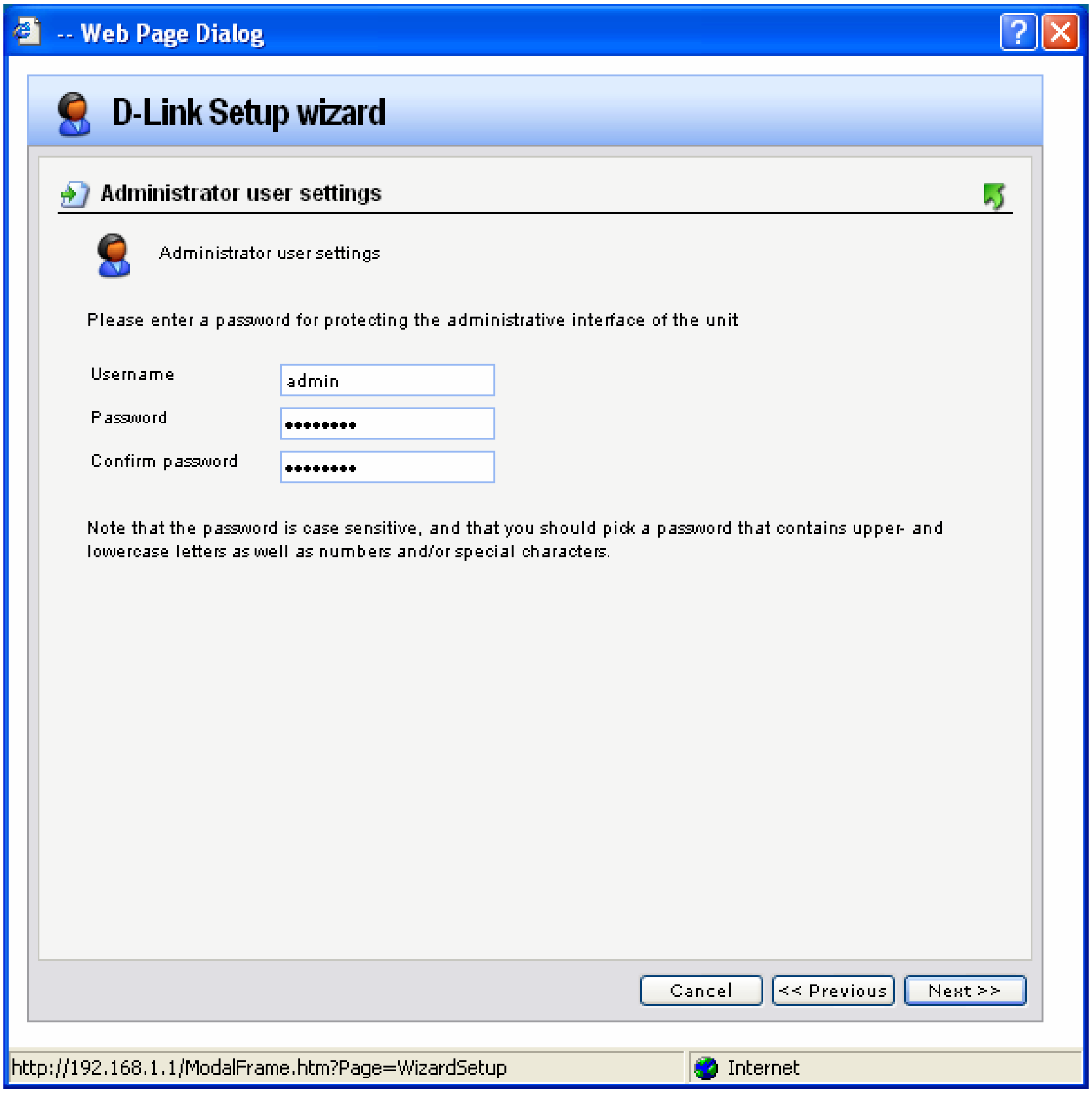
D-Link Setup wizard

Welcome

Welcome

Welcome to the D-Link Setup Wizard.

Proceed using the Next button below



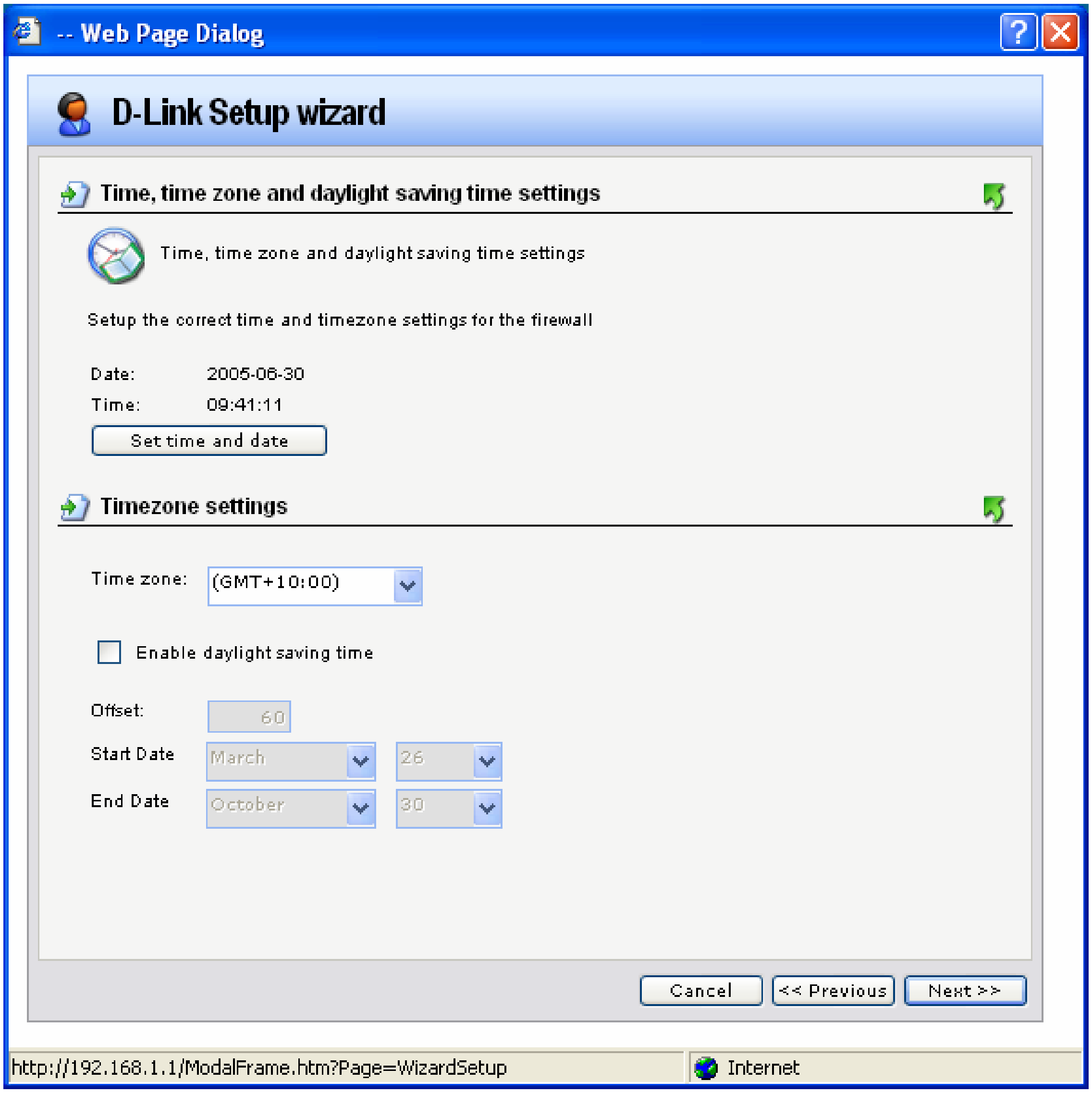
Administrator user settings

Administrator user settings

Please enter a password for protecting the administrative interface of the unit

Username	admin
Password	•••••••••
Confirm password	•••••••••

Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.



-- Web Page Dialog

D-Link Setup wizard

Time, time zone and daylight saving time settings

Time, time zone and daylight saving time settings

Setup the correct time and timezone settings for the firewall

Date: 2005-06-30

Time: 09:41:11

Timezone settings

Time zone: (GMT+10:00)

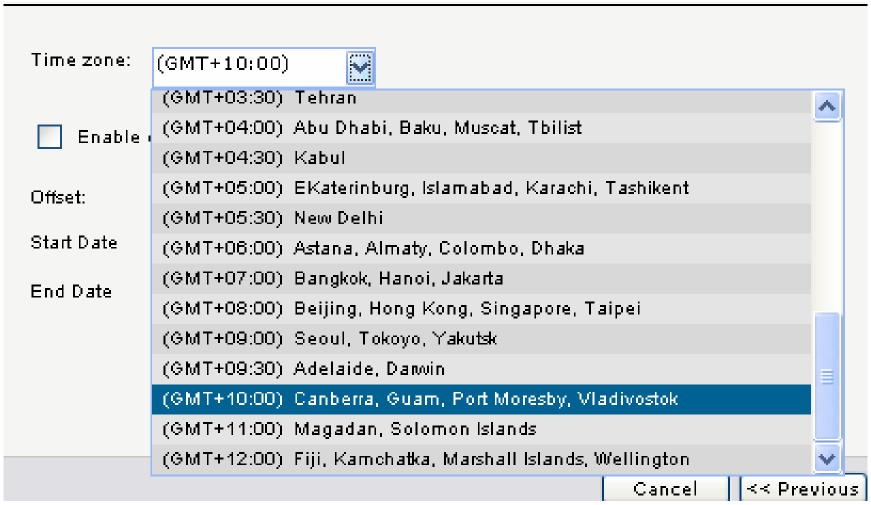
□ Enable daylight saving time

Offset: 60

Start Date March 26

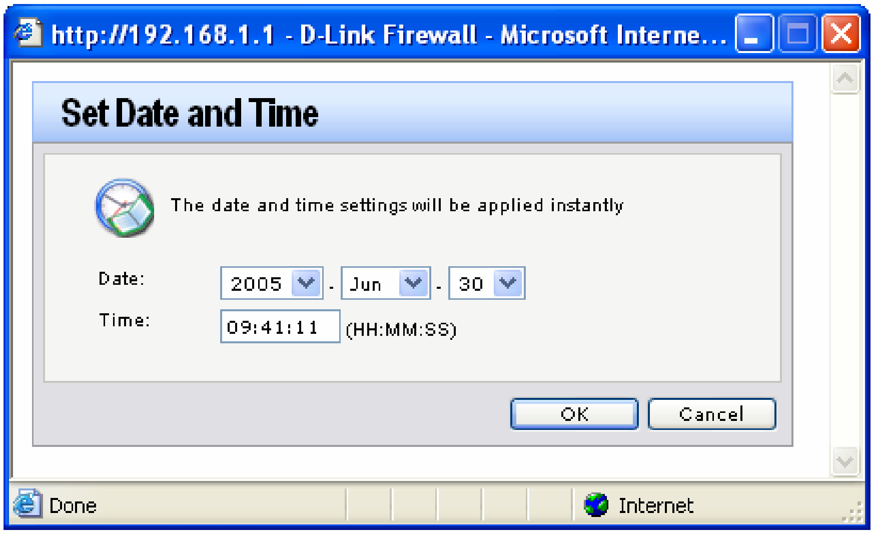
End Date October 30

http://192.168.1.1/ModalFrame.htm?Page=WizardSetup



Time zone: (GMT+10:00)

(GMT+03:30) Tehran
(GMT+04:00) Abu Dhabi, Baku, Muscat, Tbilist
(GMT+04:30) Kabul
(GMT+05:00) EKaterinburg, Islamabad, Karachi, Tashikent
(GMT+05:30) New Delhi
(GMT+06:00) Astana, Almaty, Colombo, Dhaka
(GMT+07:00) Bangkok, Hanoi, Jakarta
(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei
(GMT+09:00) Seoul, Tokoyo, Yakutsk
(GMT+09:30) Adelaide, Darwin
(GMT+10:00) Canberra, Guam, Port Moresby, Vladivostok
(GMT+11:00) Magadan, Solomon Islands
(GMT+12:00) Fiji, Kamchatka, Marshall Islands, Wellington

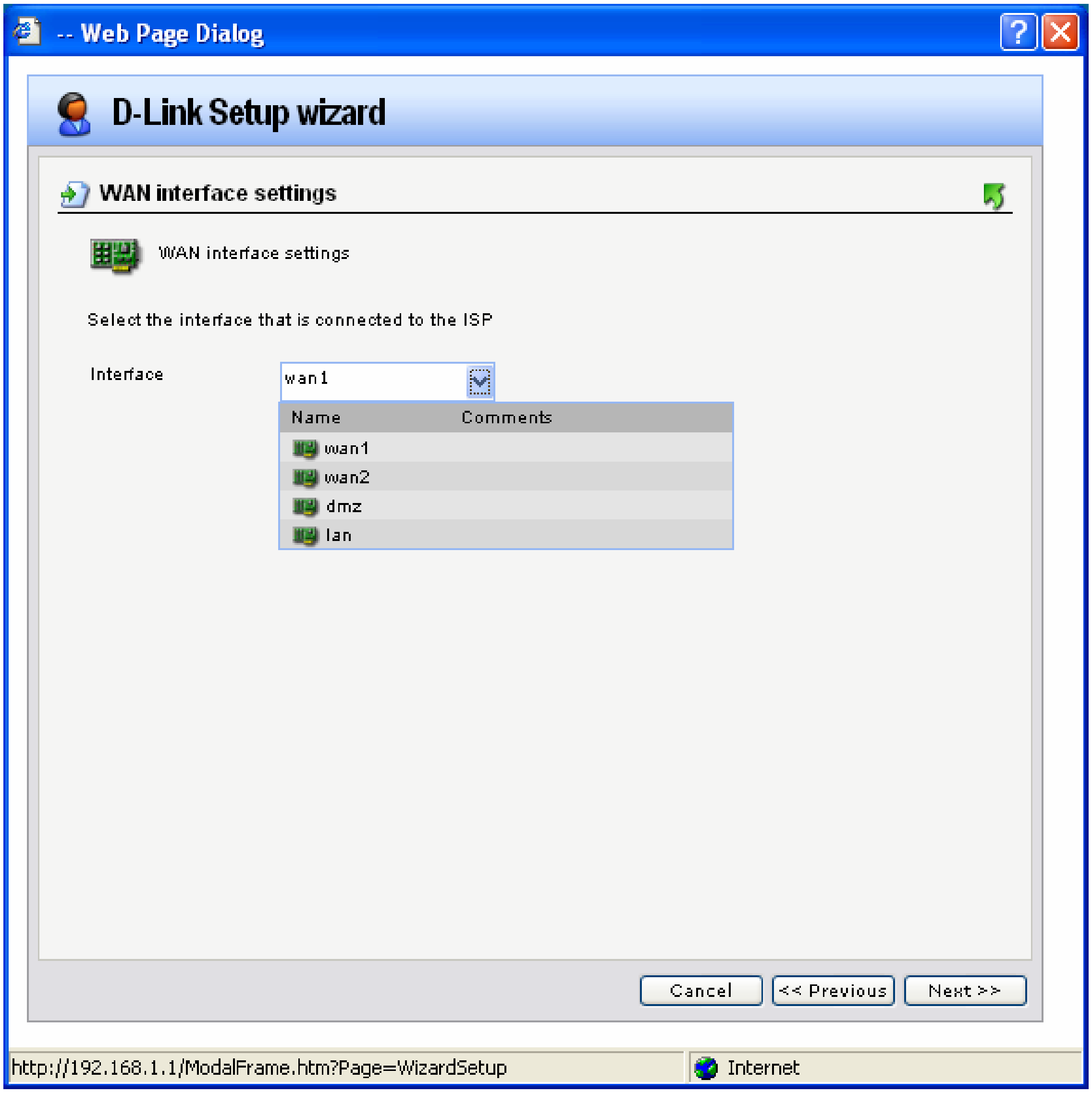


Set Date and Time

The date and time settings will be applied instantly

Date: 2005 - Jun - 30

Time: 09:41:11 (HH:MM:SS)



D-Link Setup wizard

WAN interface settings

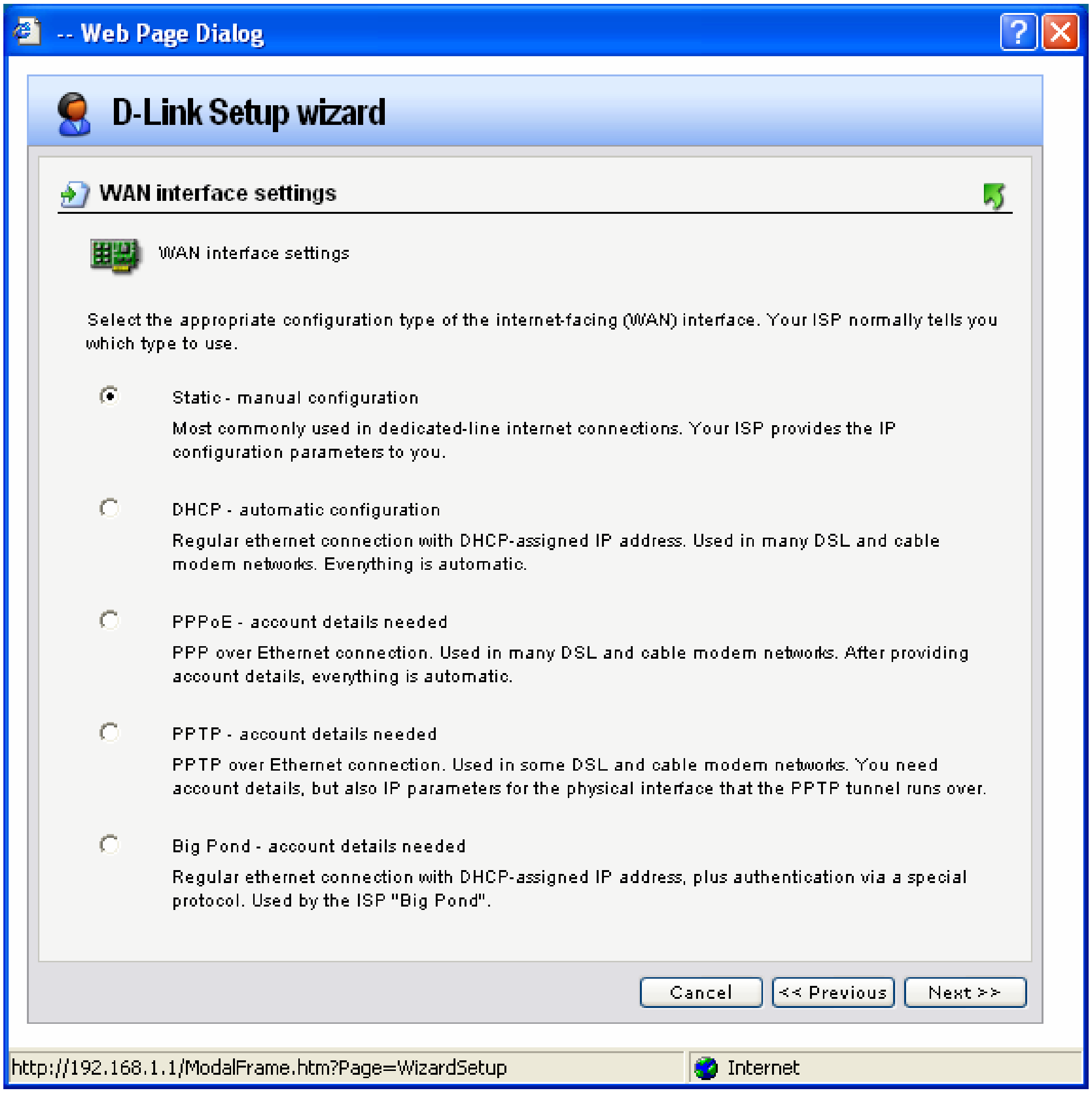
WAN interface settings

Select the interface that is connected to the ISP

Interface wan1

Name	Comments
wan1	
wan2	
dmz	
lan	

http://192.168.1.1/ModalFrame.htm?Page=WizardSetup



WAN interface settings

WAN interface settings

Select the appropriate configuration type of the internet-facing (WAN) interface. Your ISP normally tells you which type to use.

● Static - manual configuration

Most commonly used in dedicated-line internet connections. Your ISP provides the IP configuration parameters to you.

○ DHCP - automatic configuration

Regular ethernet connection with DHCP-assigned IP address. Used in many DSL and cable modem networks. Everything is automatic.

○ PPPoE - account details needed

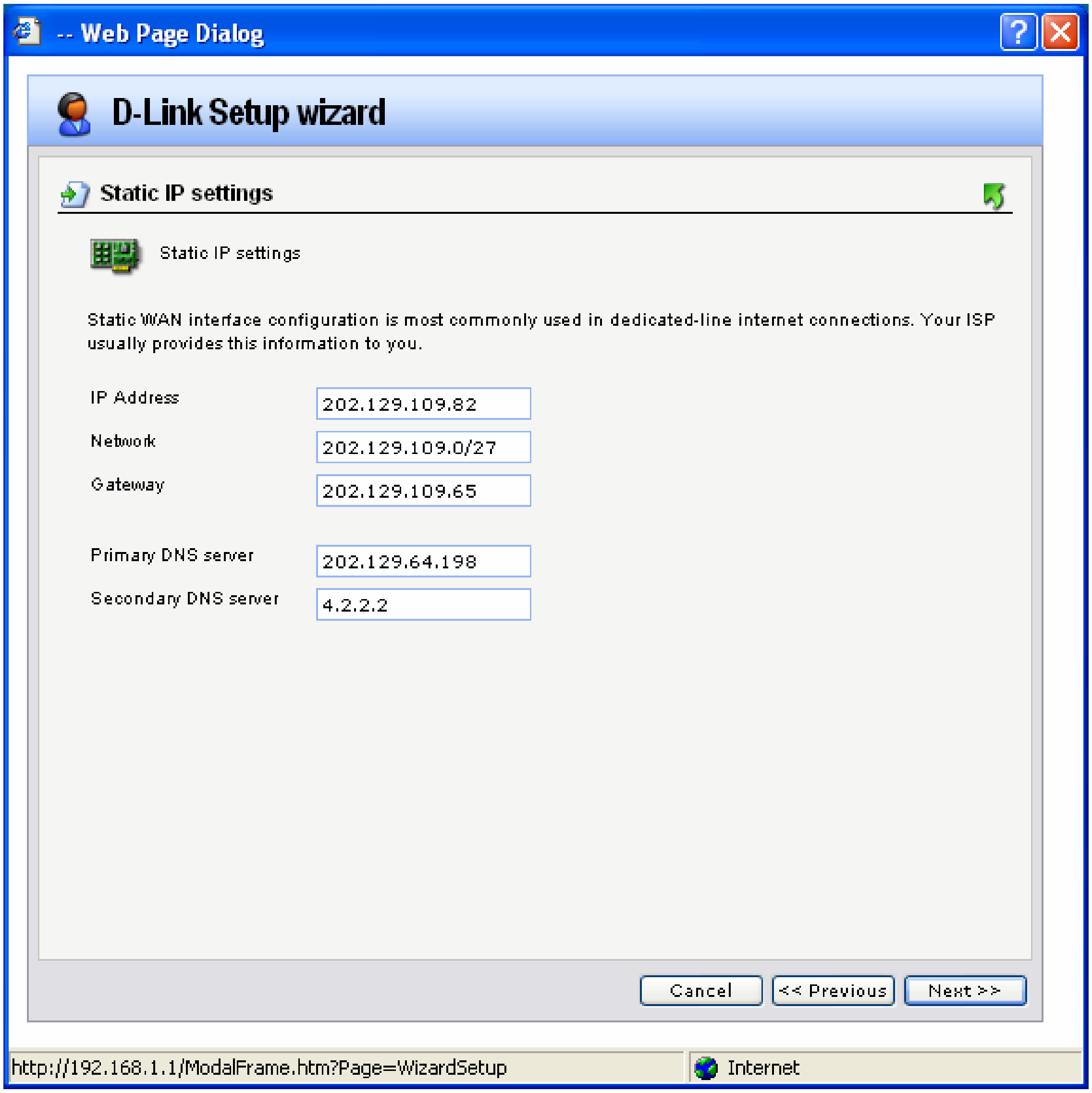
PPP over Ethernet connection. Used in many DSL and cable modem networks. After providing account details, everything is automatic.

○ PPTP - account details needed

PPTP over Ethernet connection. Used in some DSL and cable modem networks. You need account details, but also IP parameters for the physical interface that the PPTP tunnel runs over.

○ Big Pond - account details needed

Regular ethernet connection with DHCP-assigned IP address, plus authentication via a special protocol. Used by the ISP "Big Pond".



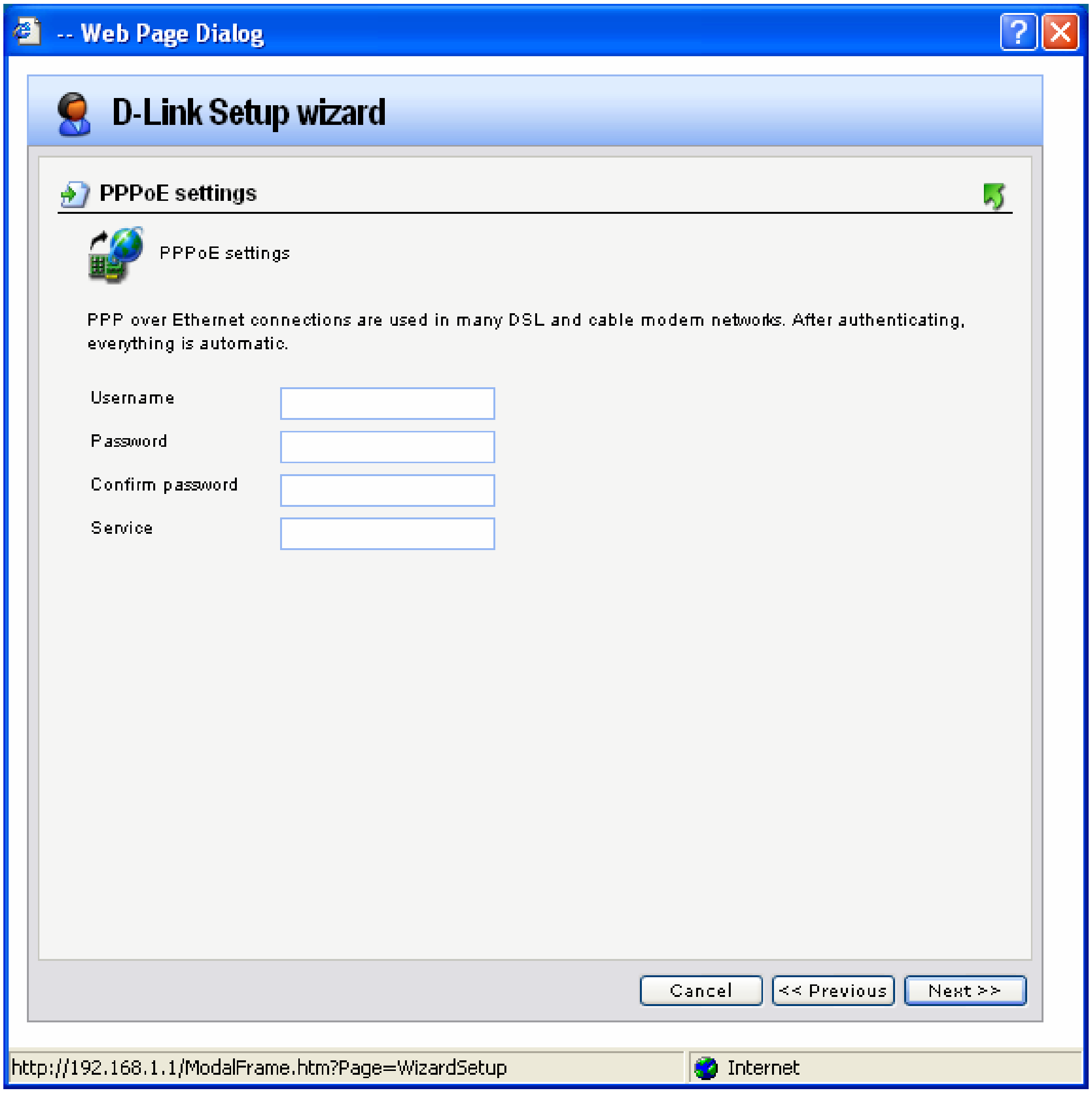
D-Link Setup wizard

Static IP settings

Static IP settings

Static WAN interface configuration is most commonly used in dedicated-line internet connections. Your ISP usually provides this information to you.

IP Address	202.129.109.82
Network	202.129.109.0/27
Gateway	202.129.109.65
Primary DNS server	202.129.64.198
Secondary DNS server	4.2.2.2



-- Web Page Dialog

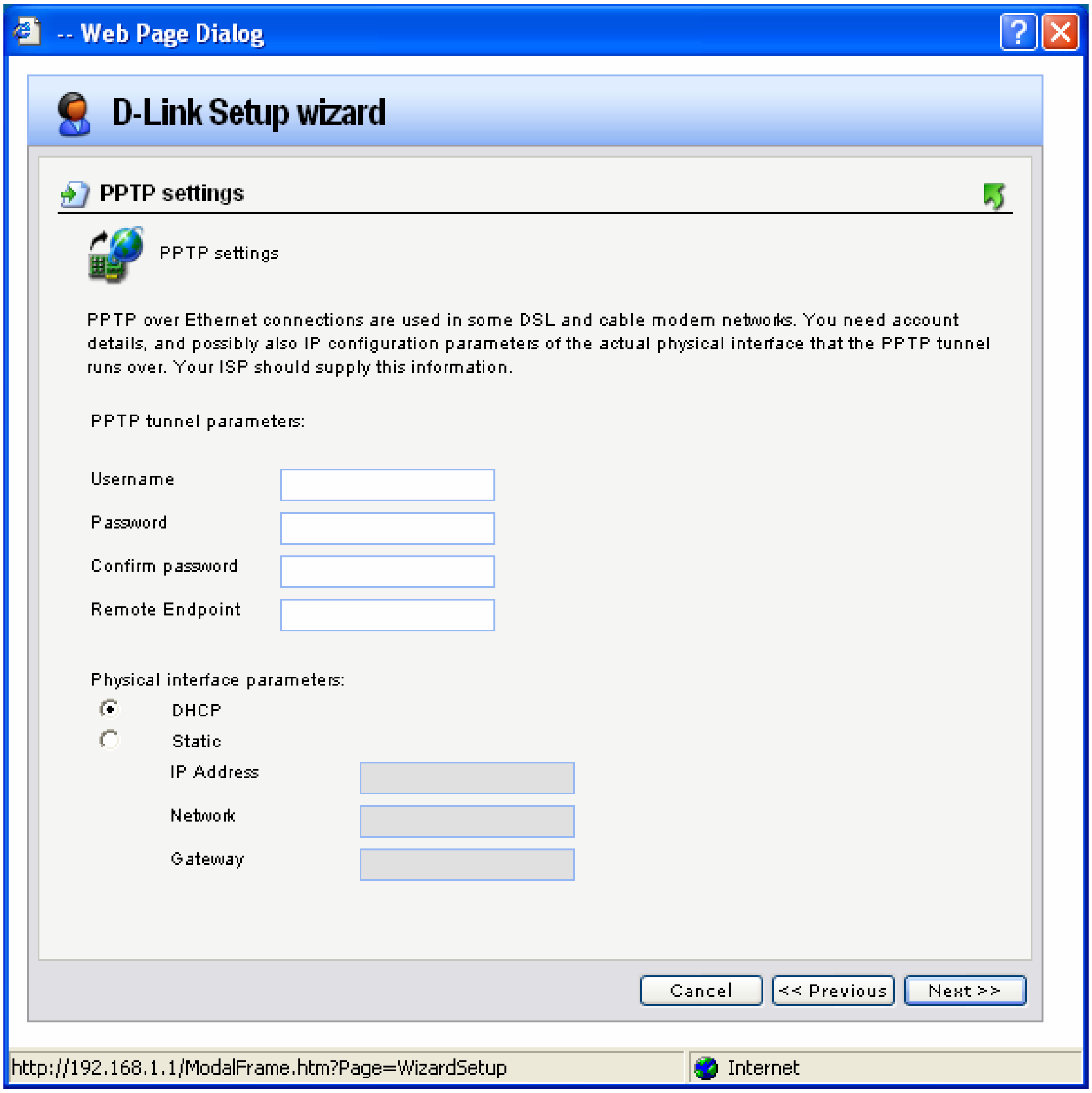
D-Link Setup wizard

PPPoE settings

PPPoE settings

PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.

Username	
Password	
Confirm password	
Service	



PPTP settings

PPTP settings

PPTP over Ethernet connections are used in some DSL and cable modem networks. You need account details, and possibly also IP configuration parameters of the actual physical interface that the PPTP tunnel runs over. Your ISP should supply this information.

PPTP tunnel parameters:

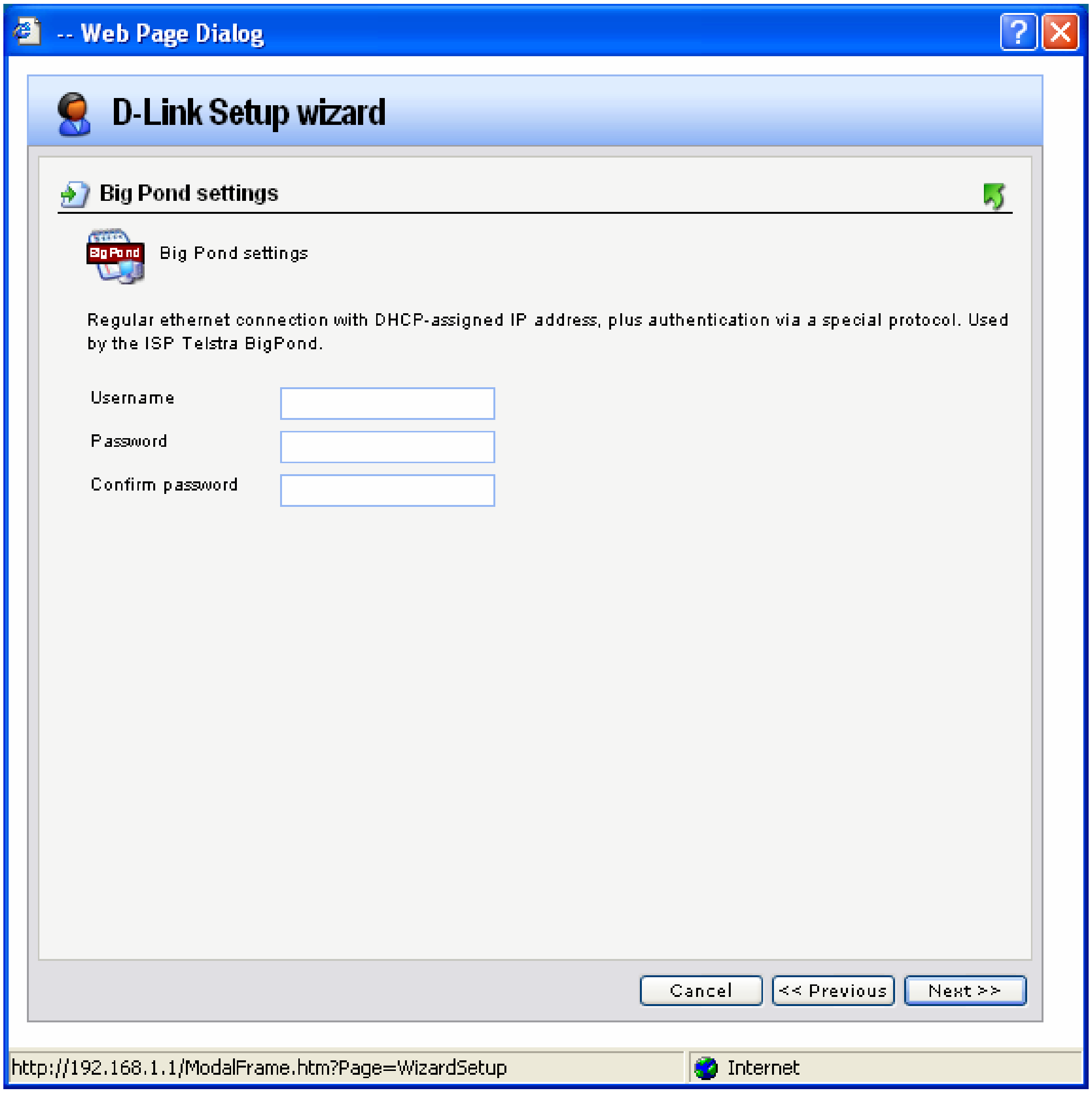
Username	
Password	
Confirm password	
Remote Endpoint	

Physical interface parameters:

● DHCP

○ Static

IP Address	
Network	
Gateway	

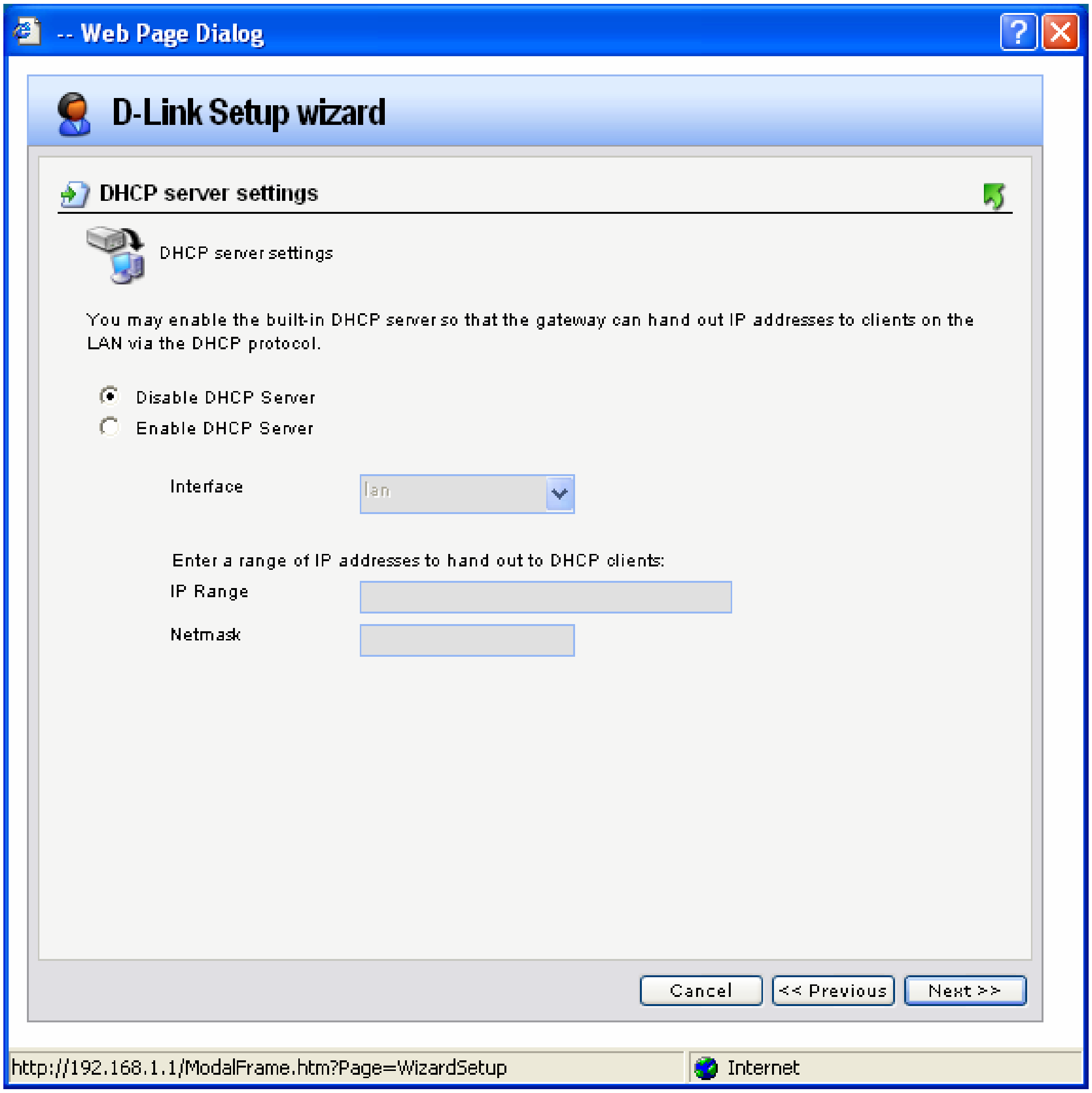


Big Pond settings

Big Pond settings

Regular ethernet connection with DHCP-assigned IP address, plus authentication via a special protocol. Used by the ISP Telstra BigPond.

Username	
Password	
Confirm password	



D-Link Setup wizard

DHCP server settings

DHCP server settings

You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.

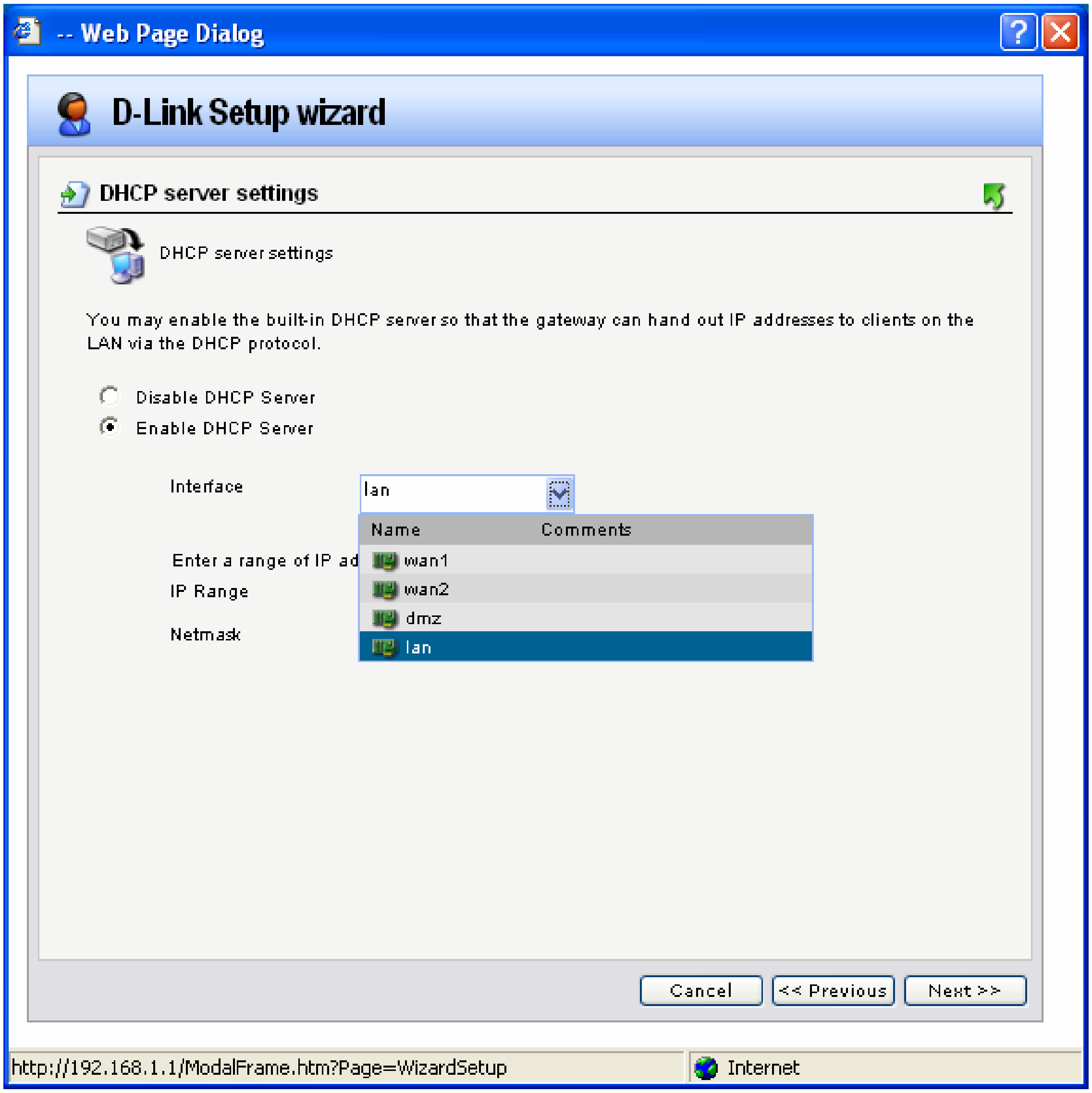
● Disable DHCP Server
○ Enable DHCP Server

Interface: lan

Enter a range of IP addresses to hand out to DHCP clients:

IP Range

Netmask



D-Link Setup wizard

DHCP server settings

DHCP server settings

You may enable the built-in DHCP server so that the gateway can hand out IP addresses to clients on the LAN via the DHCP protocol.

○ Disable DHCP Server

● Enable DHCP Server

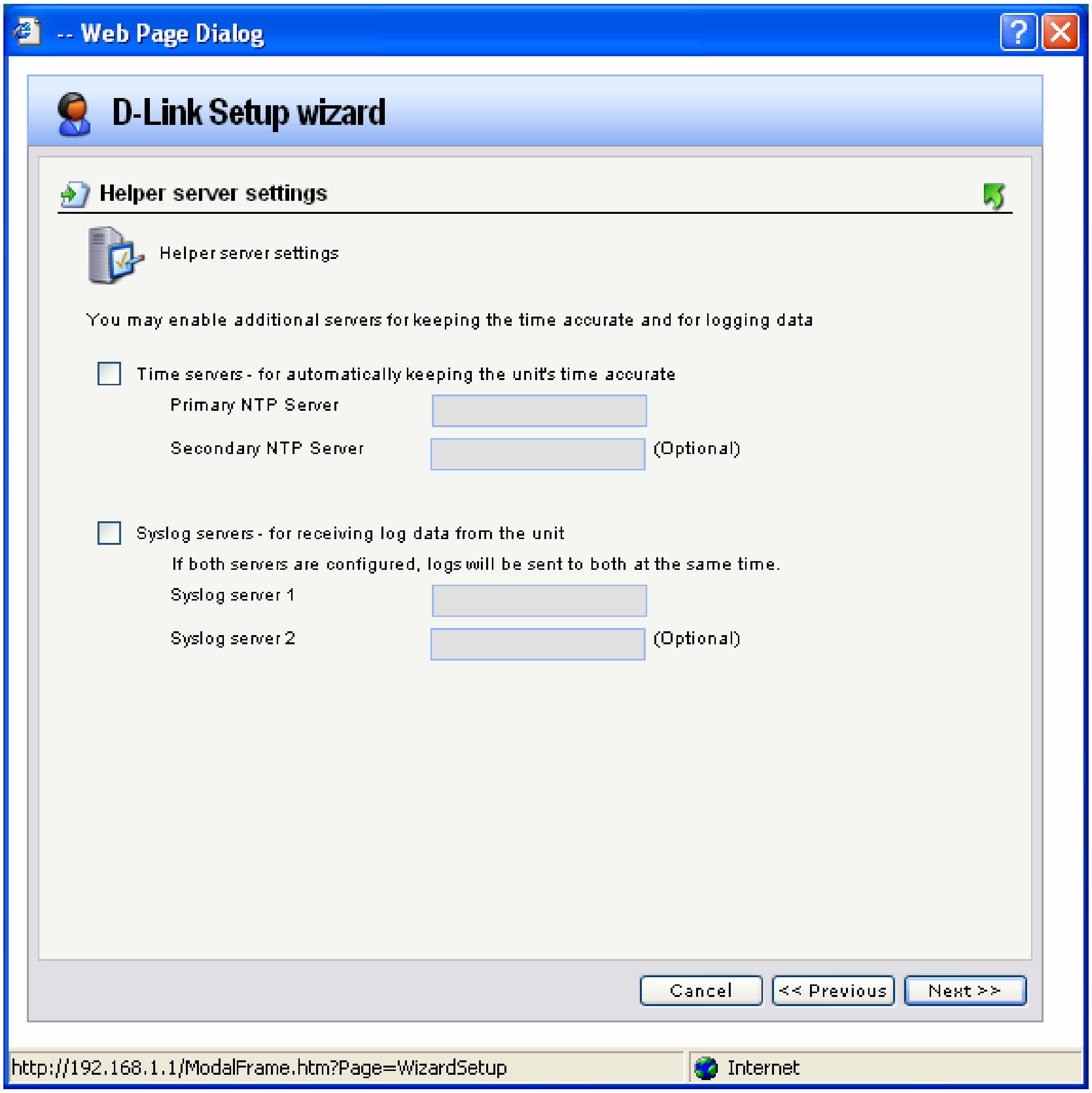
Interface: lan

Name	Comments
wan1	
wan2	
dmz	
lan	

Enter a range of IP ad

IP Range

Netmask



D-Link Setup wizard

Helper server settings

Helper server settings

You may enable additional servers for keeping the time accurate and for logging data

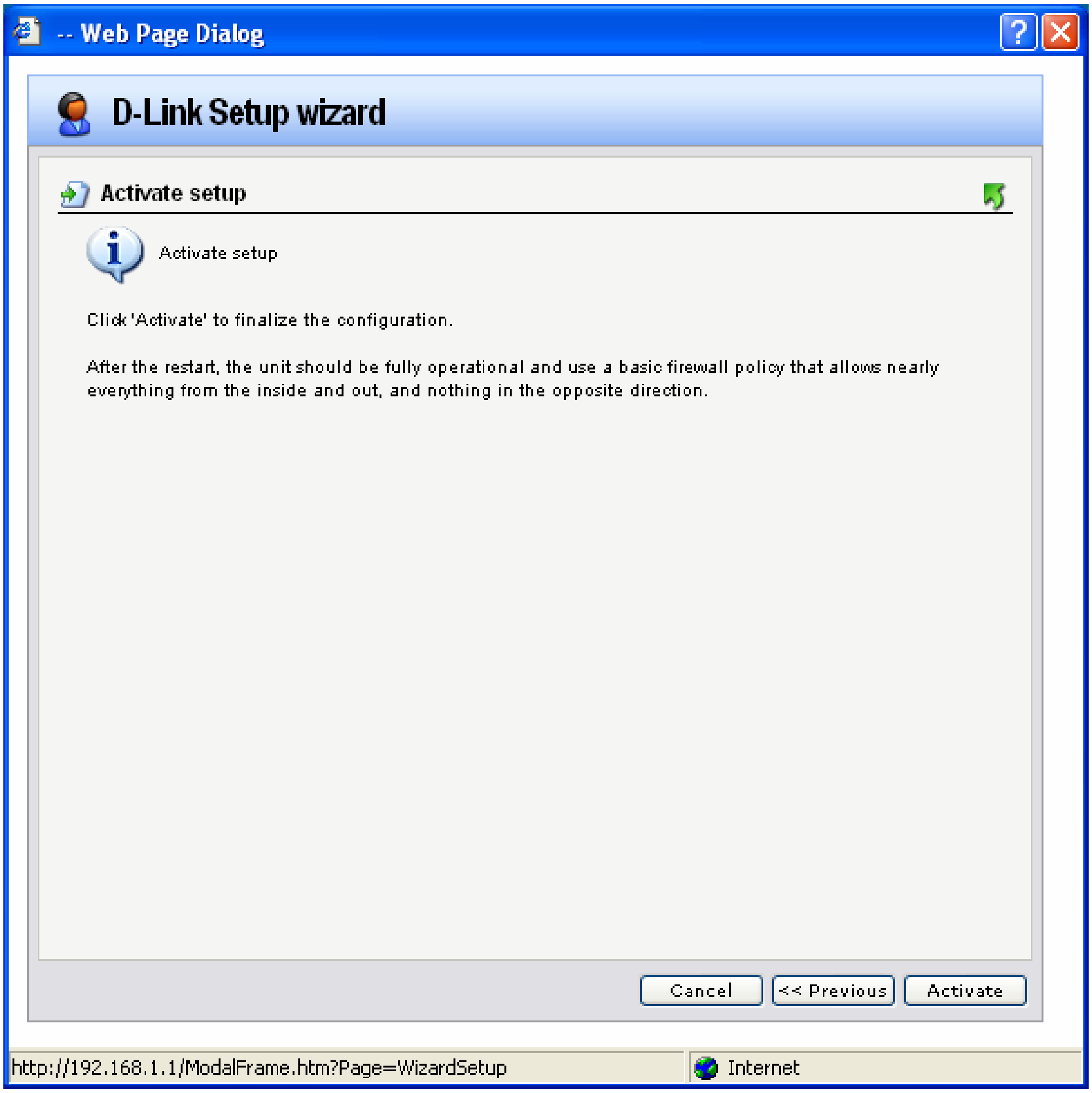
□ Time servers - for automatically keeping the unit's time accurate

Primary NTP Server		
Secondary NTP Server		(Optional)

□ Syslog servers - for receiving log data from the unit

If both servers are configured, logs will be sent to both at the same time.

Syslog server 1		
Syslog server 2		(Optional)

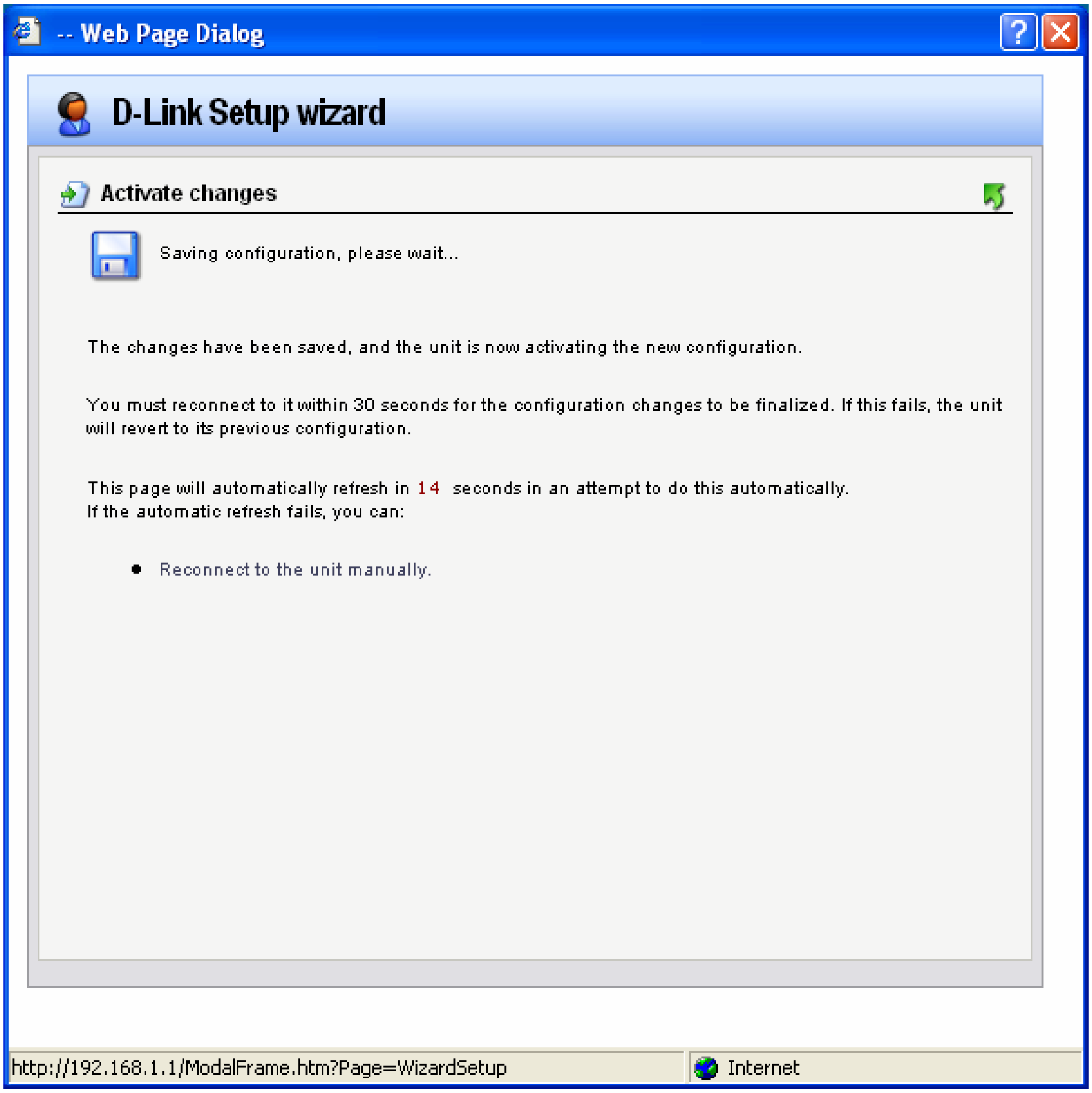


Activate setup

Activate setup

Click 'Activate' to finalize the configuration.

After the restart, the unit should be fully operational and use a basic firewall policy that allows nearly everything from the inside and out, and nothing in the opposite direction.



D-Link Setup wizard

Activate changes

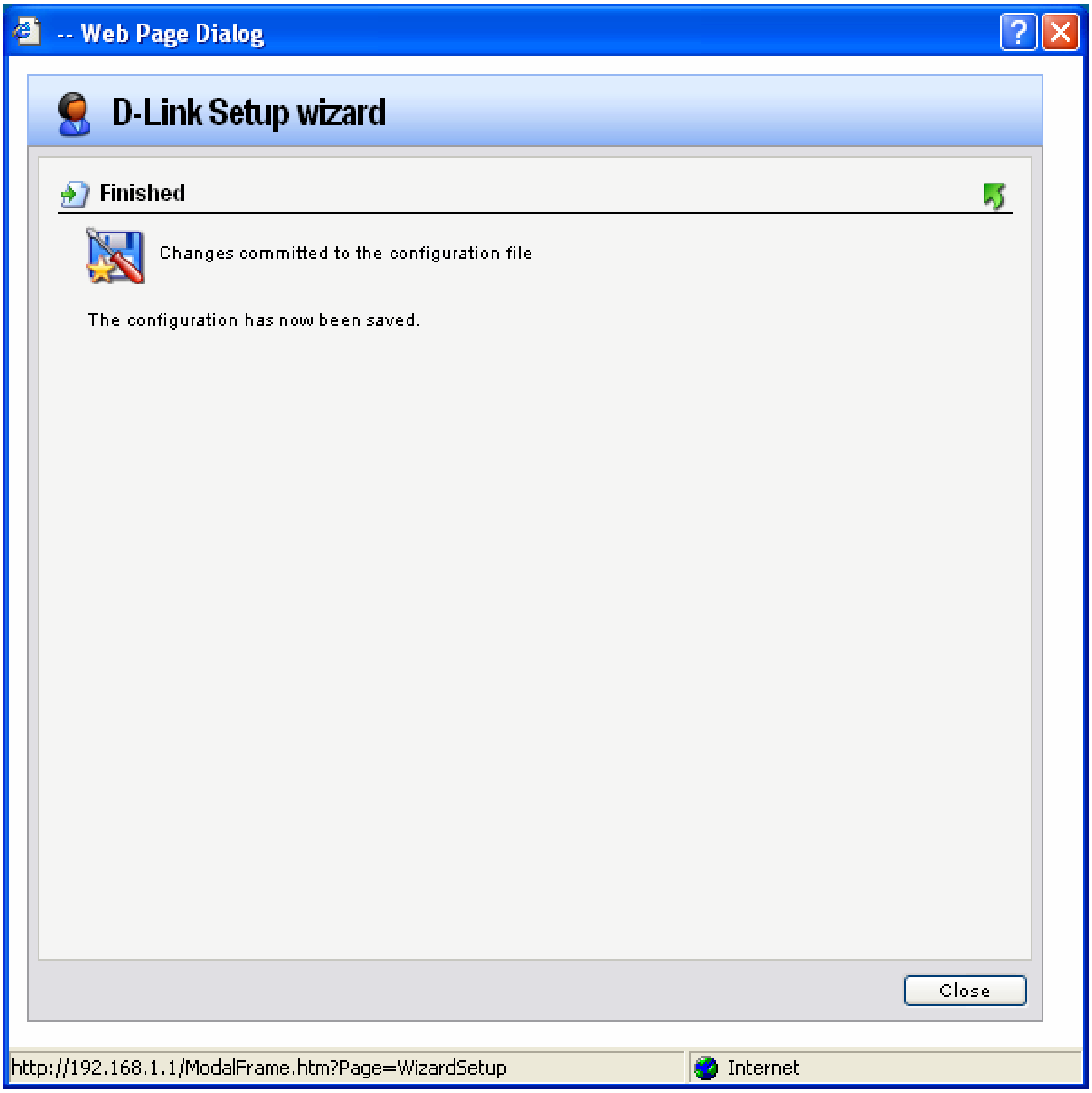
Saving configuration, please wait...

The changes have been saved, and the unit is now activating the new configuration.

You must reconnect to it within 30 seconds for the configuration changes to be finalized. If this fails, the unit will revert to its previous configuration.

This page will automatically refresh in 14 seconds in an attempt to do this automatically.
If the automatic refresh fails, you can:

- Reconnect to the unit manually.

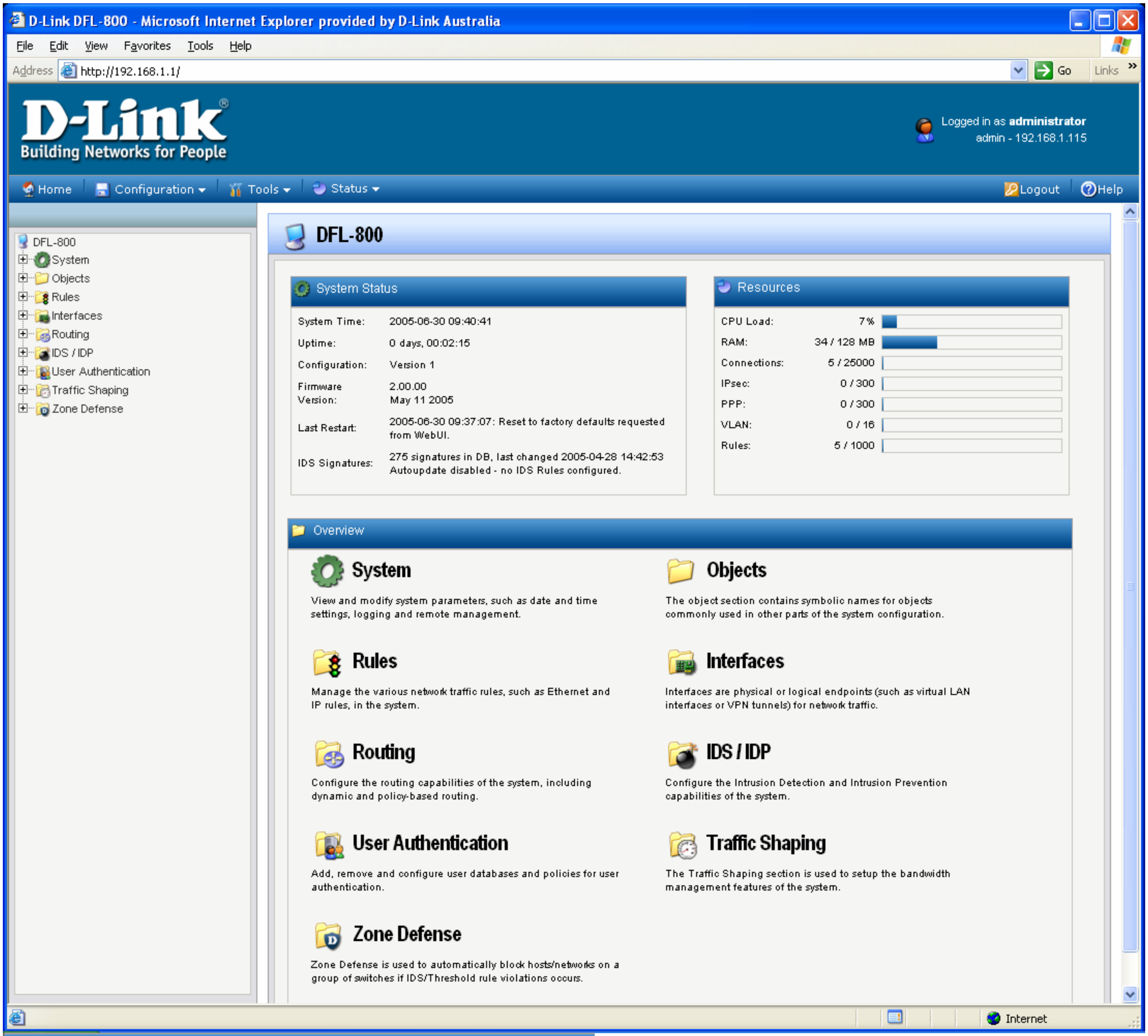


D-Link Setup wizard

Finished

Changes committed to the configuration file

The configuration has now been saved.


D-Link DFL-800 - Microsoft Internet Explorer provided by D-Link Australia
File Edit View Favorites Tools Help
Address http://192.168.1.1/
Go Links
D-Link Building Networks for People
Logged in as administrator
admin - 192.168.1.115
Home Configuration Tools Status
Logout Help
DFL-800
System
Objects
Rules
Interfaces
Routing
IDS / IDP
User Authentication
Traffic Shaping
Zone Defense
Internet

DFL-800

System Status

System Time:	2005-06-30 09:40:41
Uptime:	0 days, 00:02:15
Configuration:	Version 1
Firmware Version:	2.00.00 May 11 2005
Last Restart:	2005-06-30 09:37:07: Reset to factory defaults requested from WebUI.
IDS Signatures:	275 signatures in DB, last changed 2005-04-28 14:42:53 Autoupdate disabled - no IDS Rules configured.

Resources

CPU Load:	7%
RAM:	34 / 128 MB
Connections:	5 / 25000
IPsec:	0 / 300
PPP:	0 / 300
VLAN:	0 / 16
Rules:	5 / 1000

Overview

System

View and modify system parameters, such as date and time settings, logging and remote management.

Objects

The object section contains symbolic names for objects commonly used in other parts of the system configuration.

Rules

Manage the various network traffic rules, such as Ethernet and IP rules, in the system.

Interfaces

Interfaces are physical or logical endpoints (such as virtual LAN interfaces or VPN tunnels) for network traffic.

Routing

Configure the routing capabilities of the system, including dynamic and policy-based routing.

IDS / IDP

Configure the Intrusion Detection and Intrusion Prevention capabilities of the system.

User Authentication

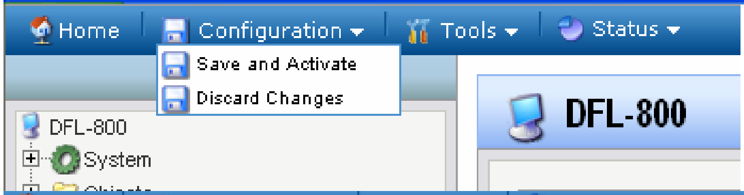
Add, remove and configure user databases and policies for user authentication.

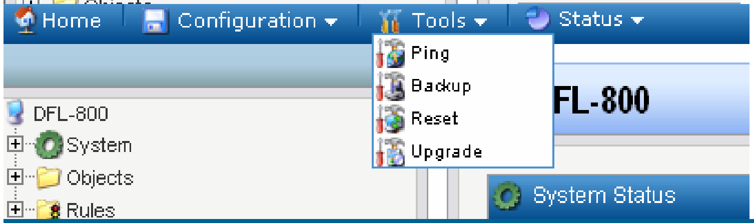
Traffic Shaping

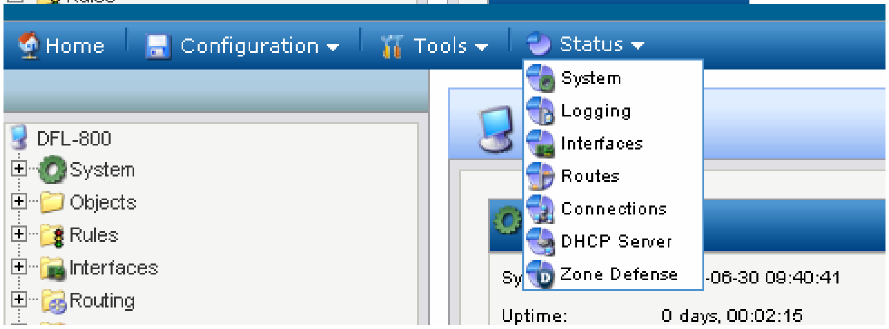
The Traffic Shaping section is used to setup the bandwidth management features of the system.

Zone Defense

Zone Defense is used to automatically block hosts/networks on a group of switches if IDS/Threshold rule violations occurs.

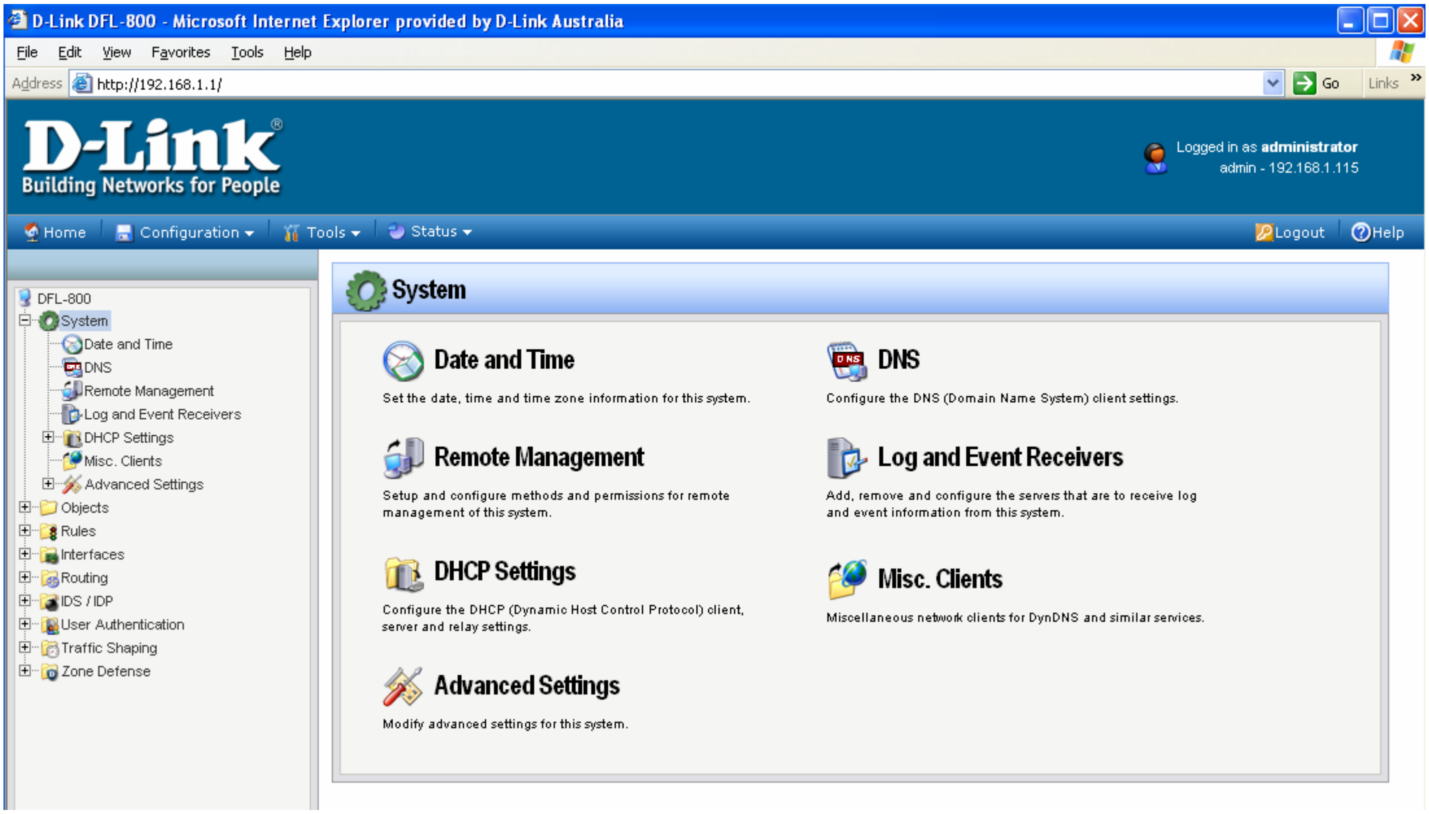






Sy -06-30 09:40:41

Uptime: 0 days, 00:02:15



System

Date and Time

Set the date, time and time zone information for this system.

DNS

Configure the DNS (Domain Name System) client settings.

Remote Management

Setup and configure methods and permissions for remote management of this system.

Log and Event Receivers

Add, remove and configure the servers that are to receive log and event information from this system.

DHCP Settings

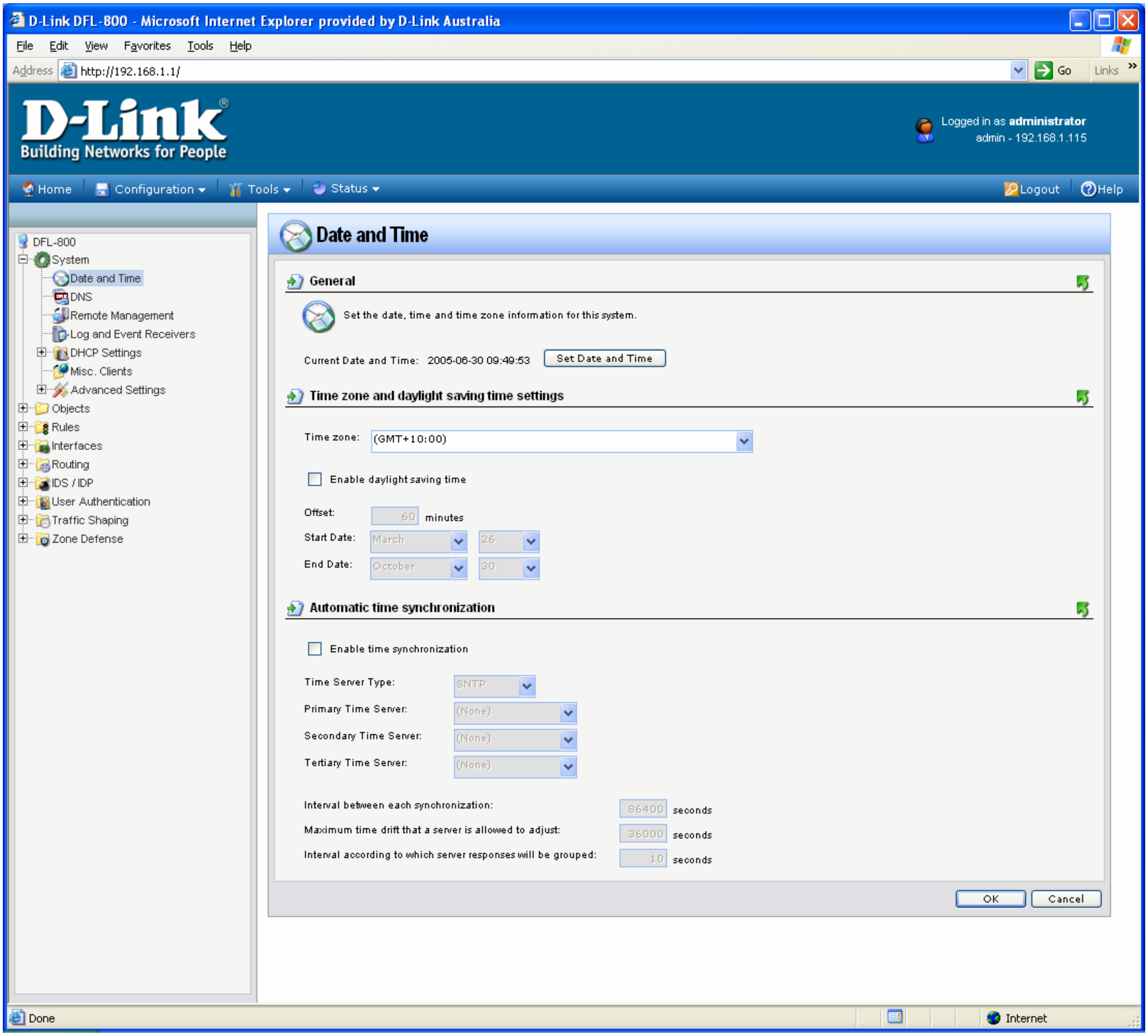
Configure the DHCP (Dynamic Host Control Protocol) client, server and relay settings.

Misc. Clients

Miscellaneous network clients for DynDNS and similar services.

Advanced Settings

Modify advanced settings for this system.



Date and Time

General

Set the date, time and time zone information for this system.

Current Date and Time: 2005-06-30 09:49:53 [Set Date and Time]

Time zone and daylight saving time settings

Time zone: (GMT+10:00)

□ Enable daylight saving time

Offset: 60 minutes

Start Date: March 26

End Date: October 30

Automatic time synchronization

□ Enable time synchronization

Time Server Type: SNTP

Primary Time Server: (None)

Secondary Time Server: (None)

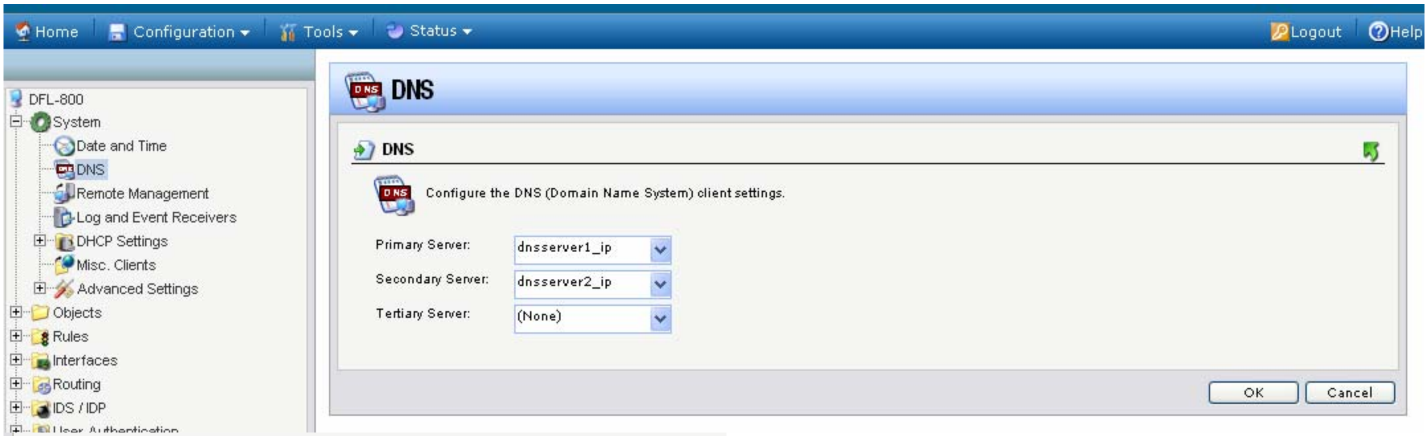
Tertiary Time Server: (None)

Interval between each synchronization: 86400 seconds

Maximum time drift that a server is allowed to adjust: 36000 seconds

Interval according to which server responses will be grouped: 10 seconds

[OK] [Cancel]



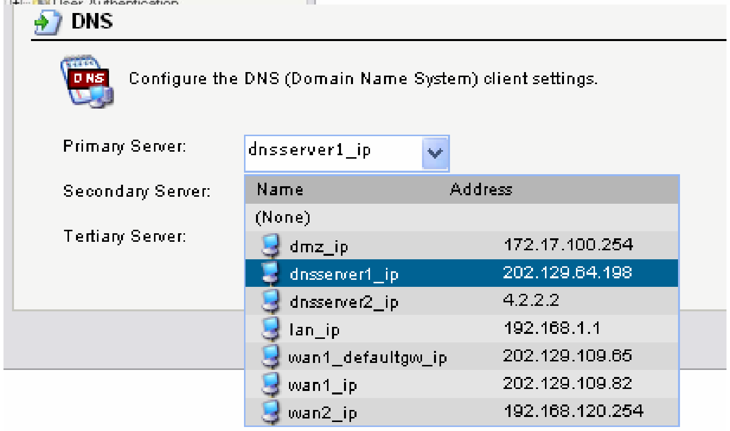
DNS

Configure the DNS (Domain Name System) client settings.

Primary Server: dnsserver1_ip

Secondary Server: dnsserver2_ip

Tertiary Server: (None)


DNS

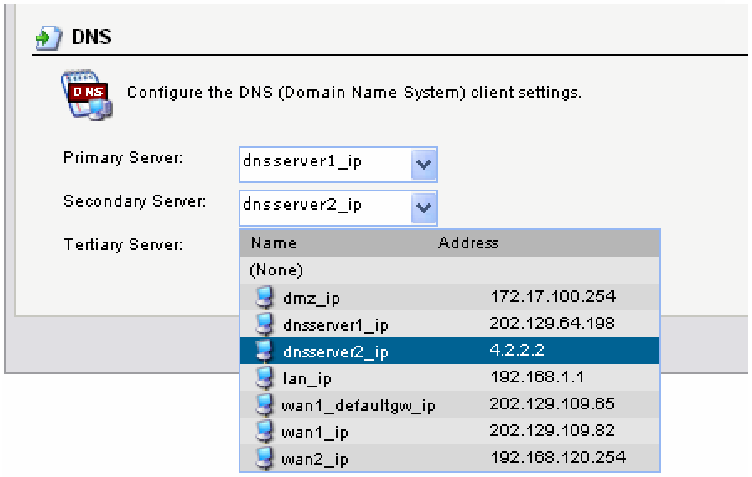
Configure the DNS (Domain Name System) client settings.

Primary Server: dnsserver1_ip

Secondary Server:

Tertiary Server:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254


DNS

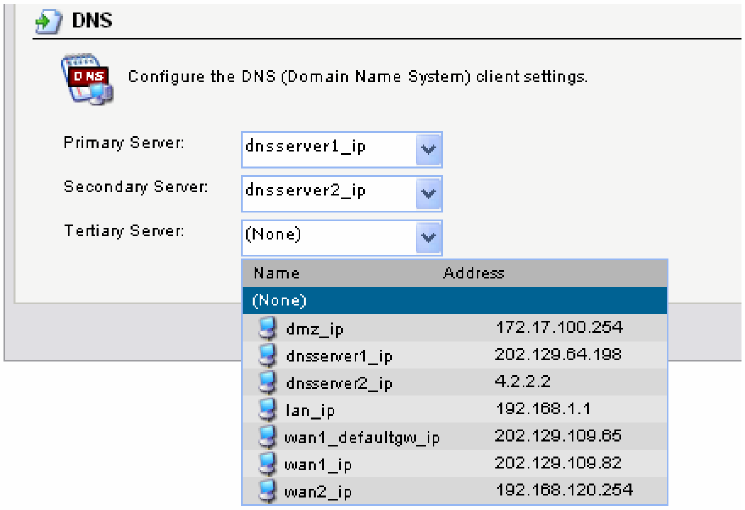
Configure the DNS (Domain Name System) client settings.

Primary Server: dnsserver1_ip

Secondary Server: dnsserver2_ip

Tertiary Server:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254


DNS

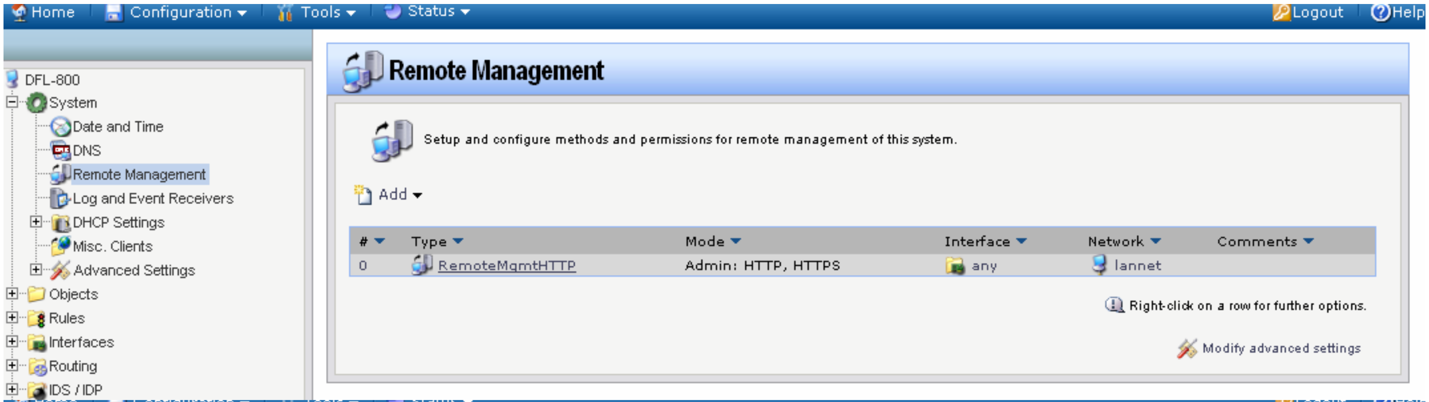
Configure the DNS (Domain Name System) client settings.

Primary Server: dnsserver1_ip

Secondary Server: dnsserver2_ip

Tertiary Server: (None)

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254



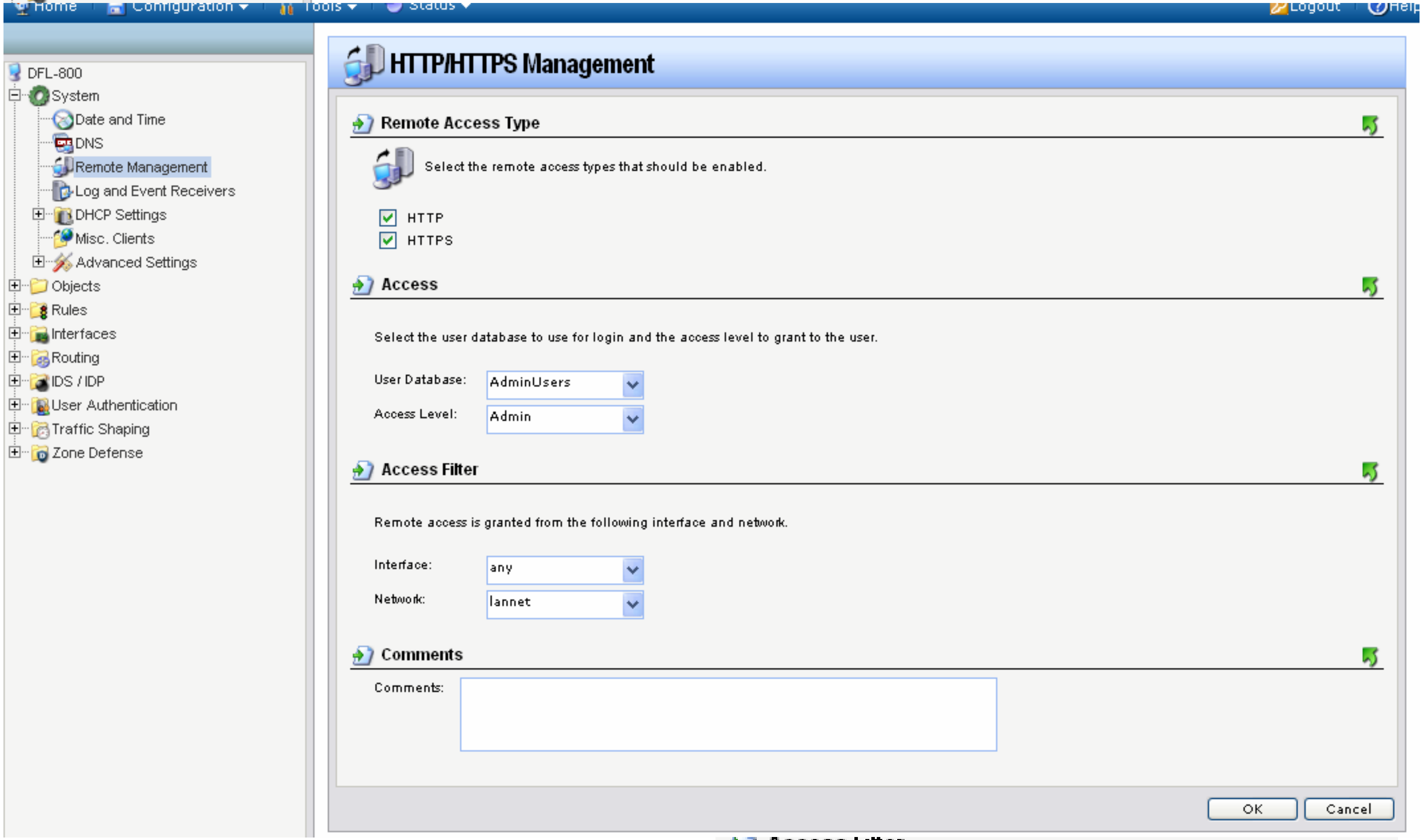
Remote Management

Setup and configure methods and permissions for remote management of this system.

#	Type	Mode	Interface	Network	Comments
0	RemoteMgmtHTTP	Admin: HTTP, HTTPS	any	lannet	

Right-click on a row for further options.

Modify advanced settings



HTTP/HTTPS Management

Remote Access Type

Select the remote access types that should be enabled.

☑ HTTP
☑ HTTPS

Access

Select the user database to use for login and the access level to grant to the user.

User Database: AdminUsers

Access Level: Admin

Access Filter

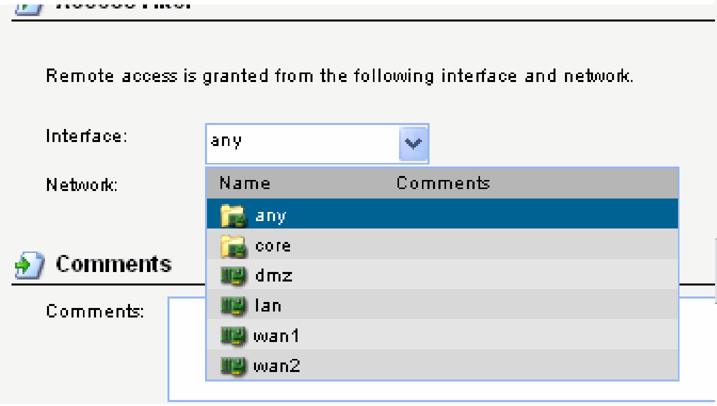
Remote access is granted from the following interface and network.

Interface: any

Network: lannet

Comments

Comments:



Access Filter

Remote access is granted from the following interface and network.

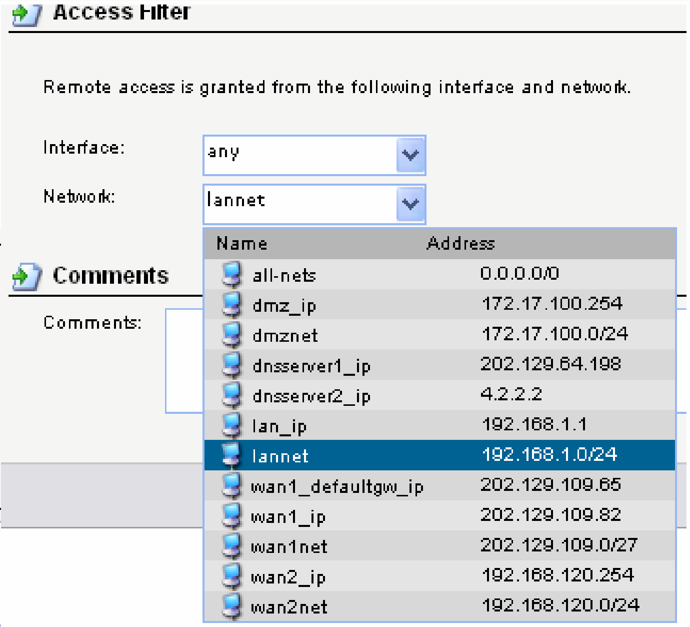
Interface: any

Network:

Name	Comments
any	
core	
dmz	
lan	
wan1	
wan2	

Comments

Comments:



Access Filter

Remote access is granted from the following interface and network.

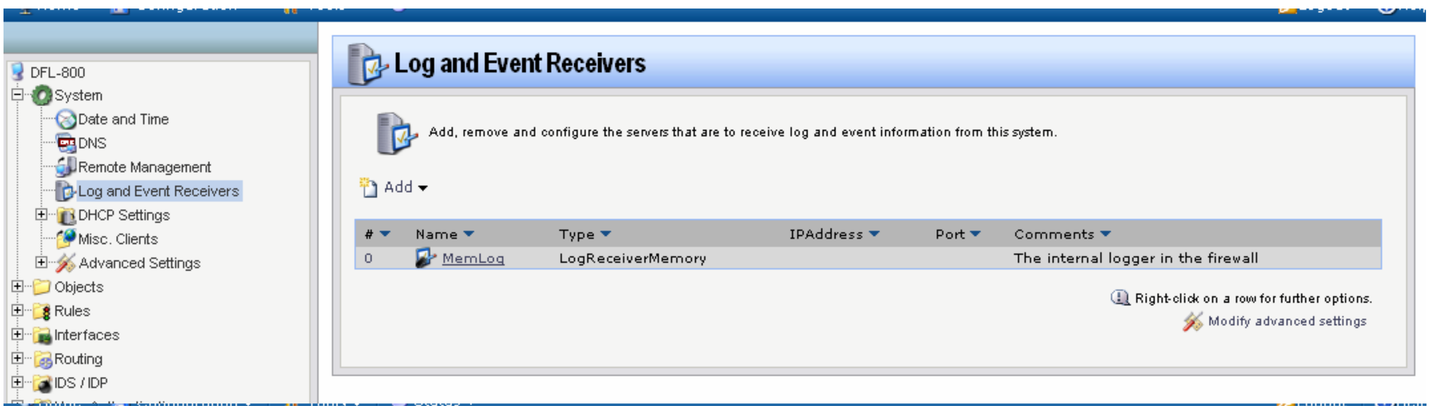
Interface: any

Network: lannet

Name	Address
all-nets	0.0.0.0/0
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
lannet	192.168.1.0/24
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan1net	202.129.109.0/27
wan2_ip	192.168.120.254
wan2net	192.168.120.0/24

Comments

Comments:

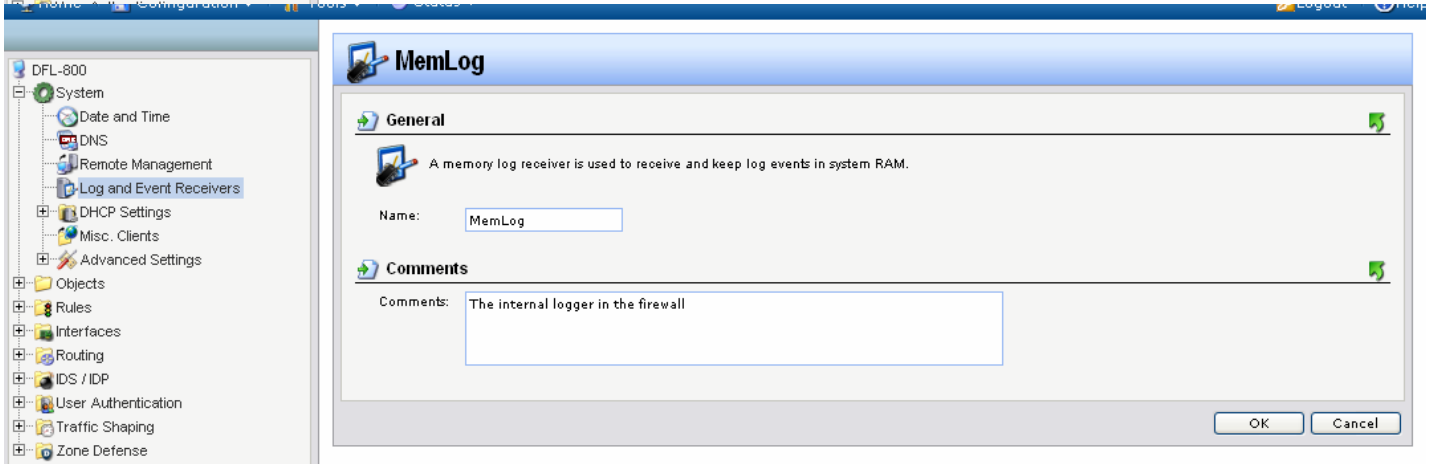


Log and Event Receivers

Add, remove and configure the servers that are to receive log and event information from this system.

#	Name	Type	IPAddress	Port	Comments
0	MemLog	LogReceiverMemory			The internal logger in the firewall

Right-click on a row for further options.



MemLog

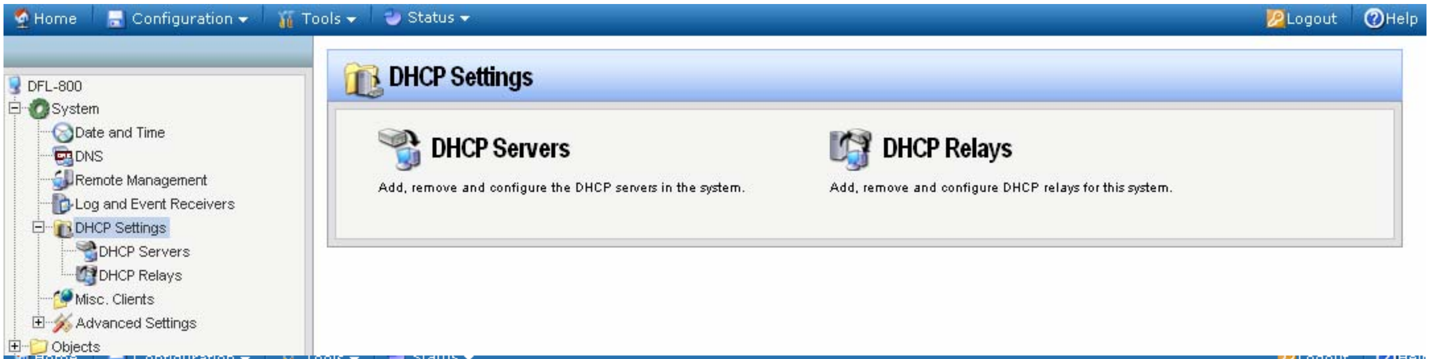
General

A memory log receiver is used to receive and keep log events in system RAM.

Name: MemLog

Comments

Comments: The internal logger in the firewall



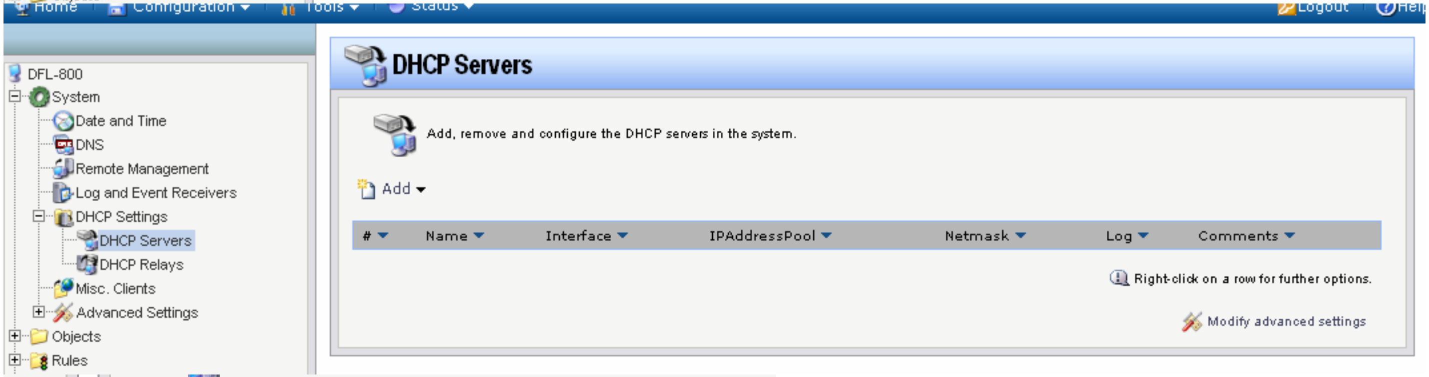
DHCP Settings

DHCP Servers

Add, remove and configure the DHCP servers in the system.

DHCP Relays

Add, remove and configure DHCP relays for this system.



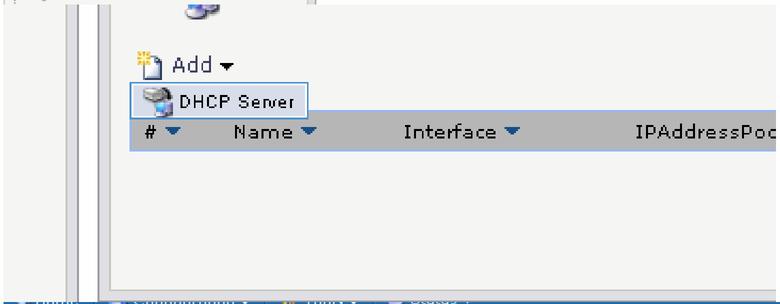
DHCP Servers

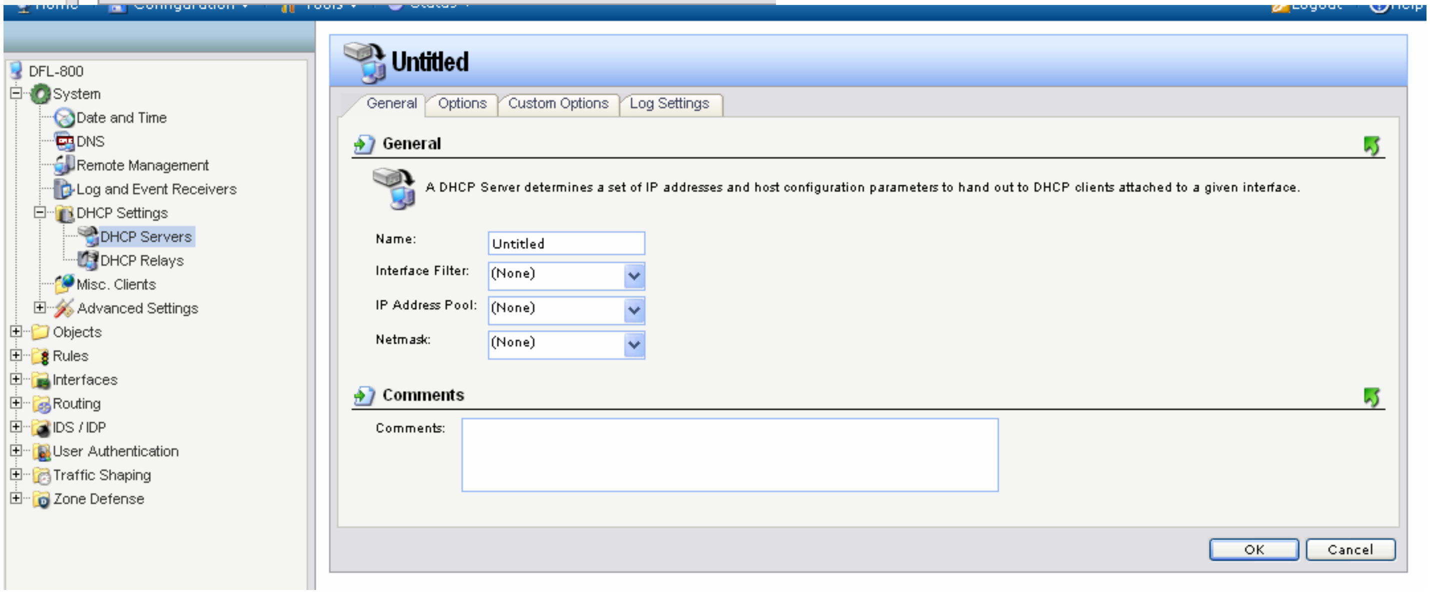
Add, remove and configure the DHCP servers in the system.

#	Name	Interface	IPAddressPool	Netmask	Log	Comments

Right-click on a row for further options.

Modify advanced settings





Untitled

General

A DHCP Server determines a set of IP addresses and host configuration parameters to hand out to DHCP clients attached to a given interface.

Name: Untitled

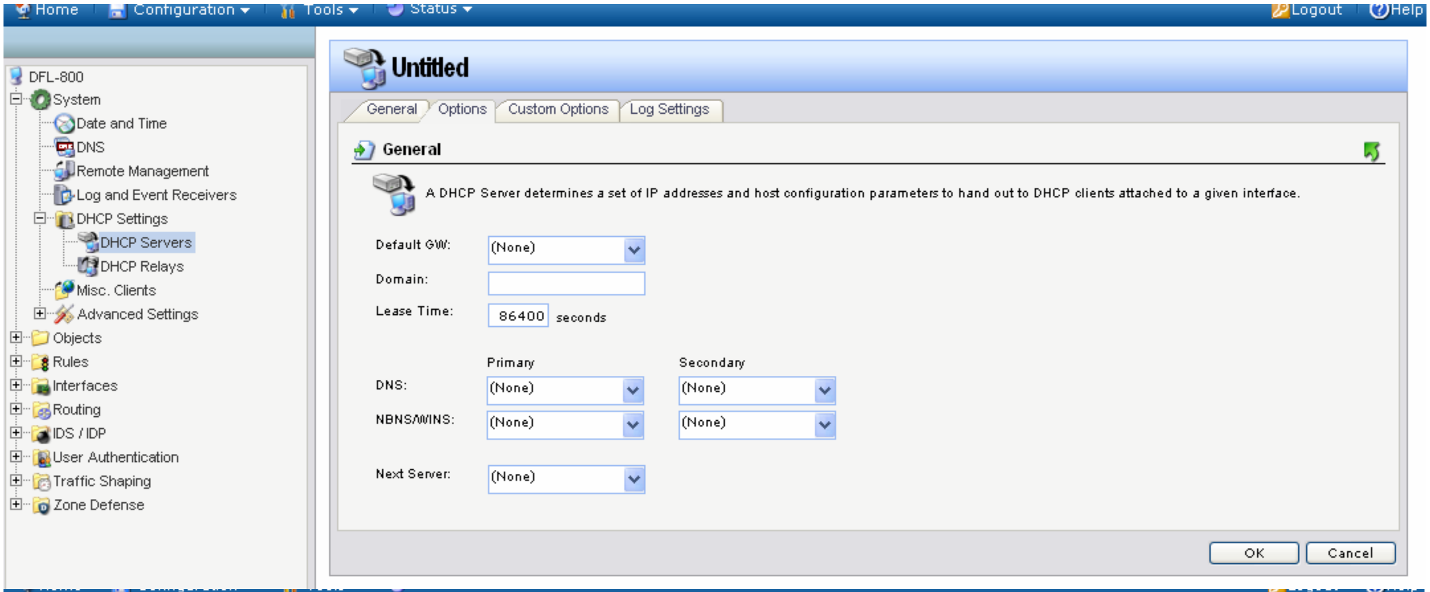
Interface Filter: (None)

IP Address Pool: (None)

Netmask: (None)

Comments

Comments:



General

A DHCP Server determines a set of IP addresses and host configuration parameters to hand out to DHCP clients attached to a given interface.

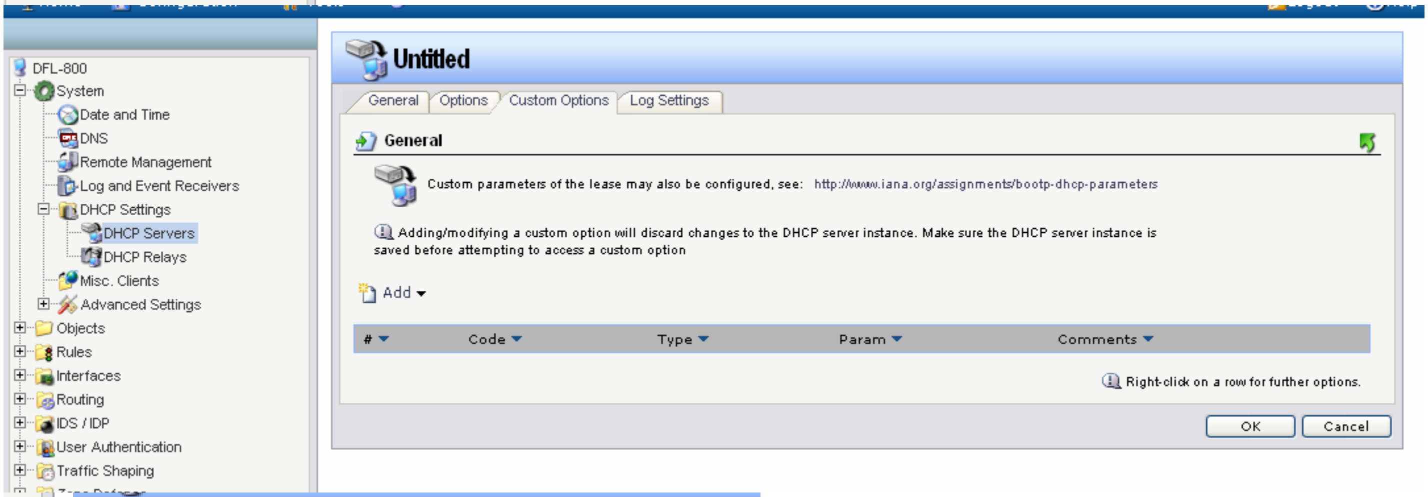
Default GW: (None)

Domain:

Lease Time: 86400 seconds

	Primary	Secondary
DNS:	(None)	(None)
NBNS/WINS:	(None)	(None)

Next Server: (None)



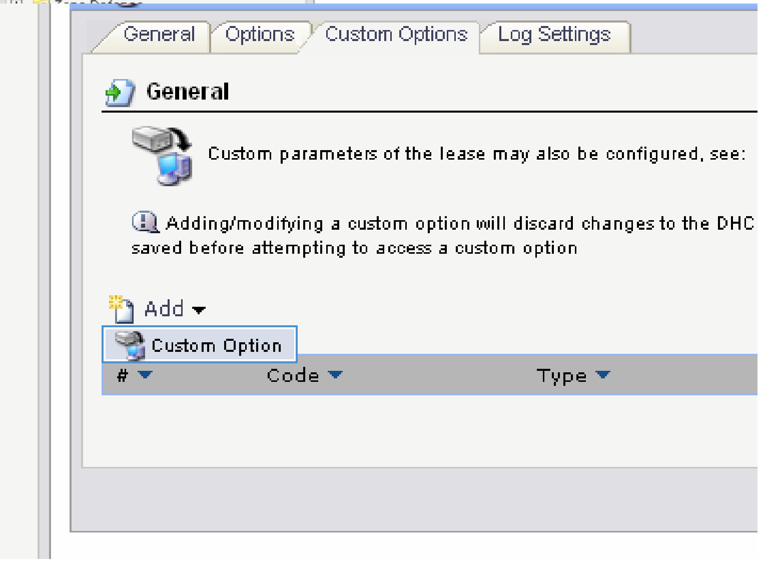
General

Custom parameters of the lease may also be configured, see: http://www.iana.org/assignments/bootp-dhcp-parameters

Adding/modifying a custom option will discard changes to the DHCP server instance. Make sure the DHCP server instance is saved before attempting to access a custom option

#	Code	Type	Param	Comments

Right-click on a row for further options.

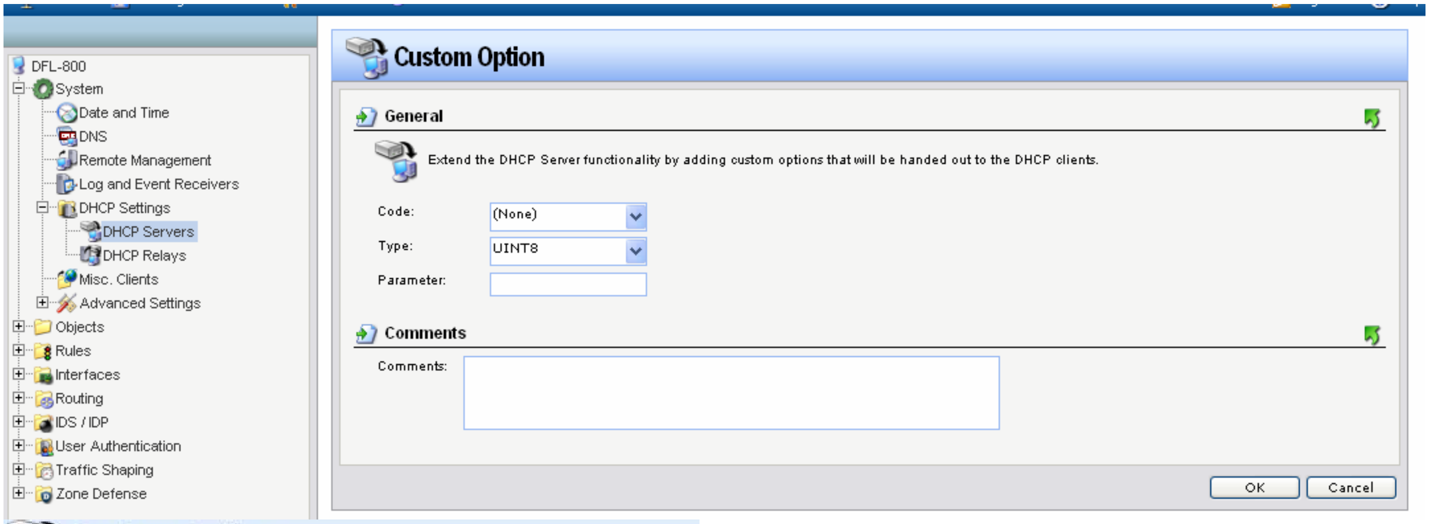


General

Custom parameters of the lease may also be configured, see:

Adding/modifying a custom option will discard changes to the DHC saved before attempting to access a custom option

#	Code	Type



Custom Option

General

Extend the DHCP Server functionality by adding custom options that will be handed out to the DHCP clients.

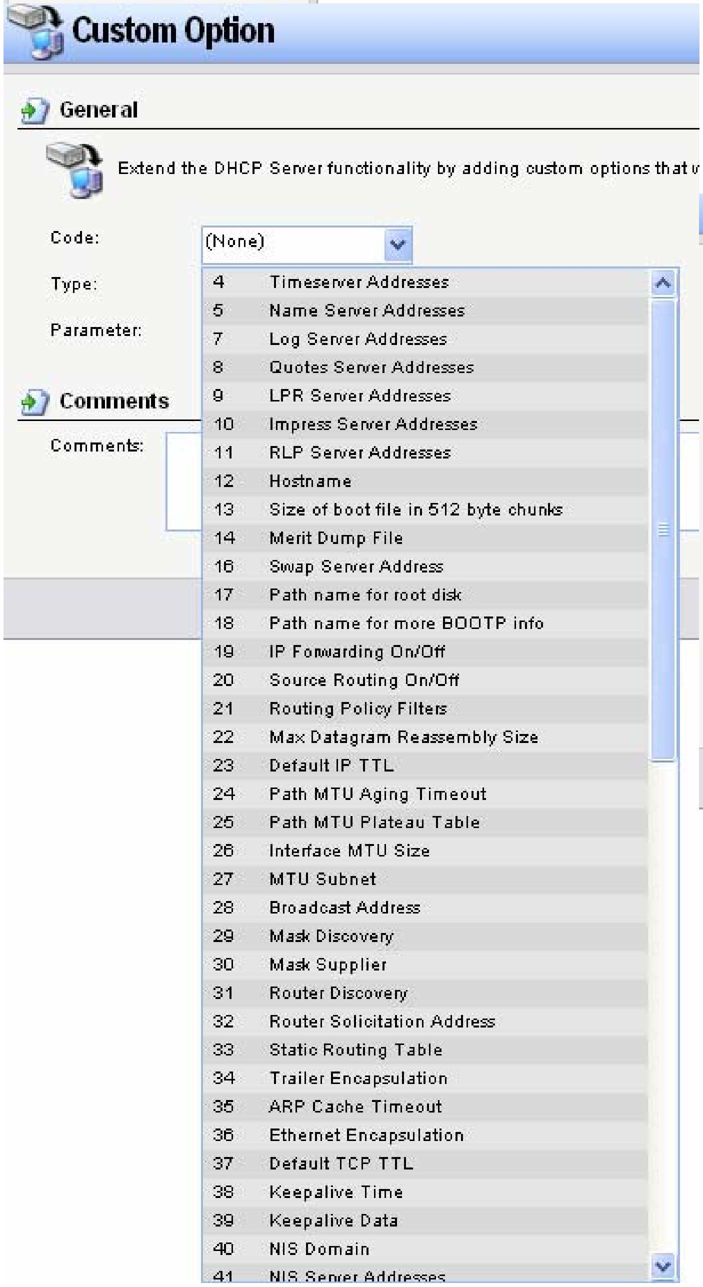
Code: (None)

Type: UINT8

Parameter:

Comments

Comments:



Custom Option

General

Extend the DHCP Server functionality by adding custom options that w

Code: (None)

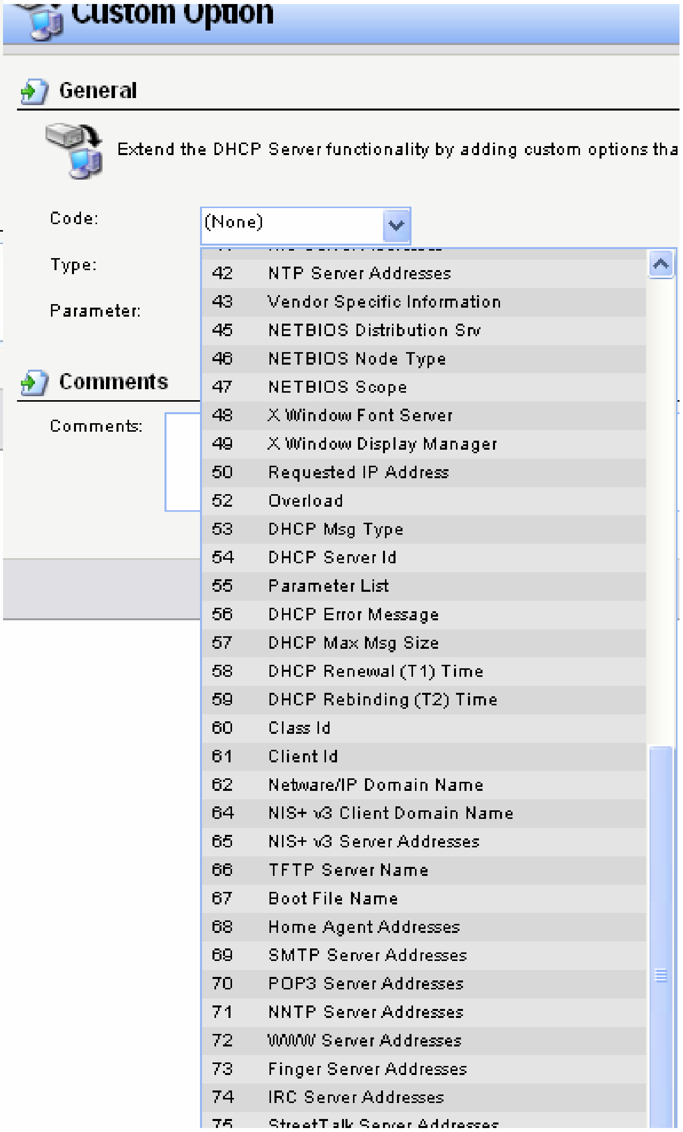
Type:

Parameter:

Comments

Comments:

4	Timeserver Addresses
5	Name Server Addresses
7	Log Server Addresses
8	Quotes Server Addresses
9	LPR Server Addresses
10	Impress Server Addresses
11	RLP Server Addresses
12	Hostname
13	Size of boot file in 512 byte chunks
14	Merit Dump File
16	Swap Server Address
17	Path name for root disk
18	Path name for more BOOTP info
19	IP Forwarding On/Off
20	Source Routing On/Off
21	Routing Policy Filters
22	Max Datagram Reassembly Size
23	Default IP TTL
24	Path MTU Aging Timeout
25	Path MTU Plateau Table
26	Interface MTU Size
27	MTU Subnet
28	Broadcast Address
29	Mask Discovery
30	Mask Supplier
31	Router Discovery
32	Router Solicitation Address
33	Static Routing Table
34	Trailer Encapsulation
35	ARP Cache Timeout
36	Ethernet Encapsulation
37	Default TCP TTL
38	Keepalive Time
39	Keepalive Data
40	NIS Domain
41	NIS Server Addresses



Custom Option

General

Extend the DHCP Server functionality by adding custom options tha

Code: (None)

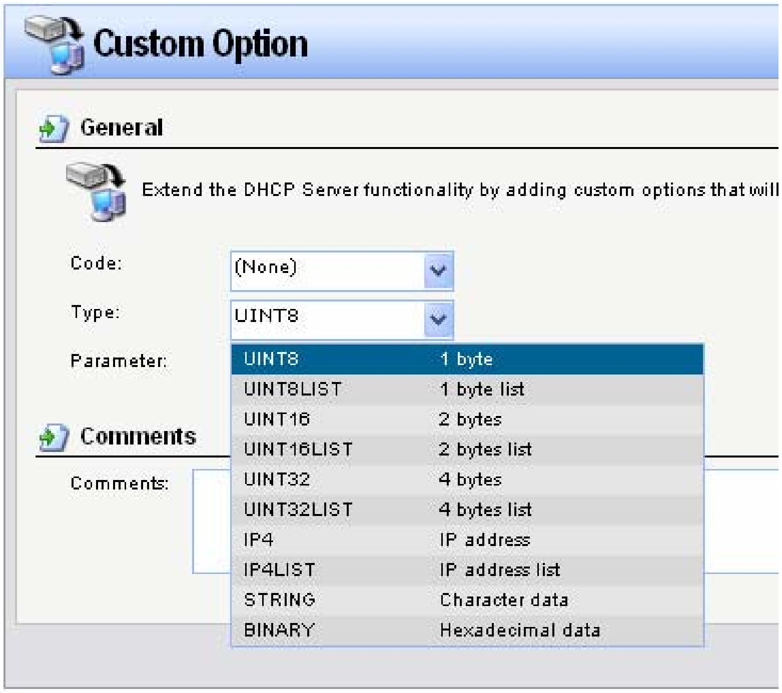
Type:

Parameter:

Comments

Comments:

42	NTP Server Addresses
43	Vendor Specific Information
45	NETBIOS Distribution Srv
46	NETBIOS Node Type
47	NETBIOS Scope
48	X Window Font Server
49	X Window Display Manager
50	Requested IP Address
52	Overload
53	DHCP Msg Type
54	DHCP Server Id
55	Parameter List
56	DHCP Error Message
57	DHCP Max Msg Size
58	DHCP Renewal (T1) Time
59	DHCP Rebinding (T2) Time
60	Class Id
61	Client Id
62	Netware/IP Domain Name
64	NIS+ v3 Client Domain Name
65	NIS+ v3 Server Addresses
66	TFTP Server Name
67	Boot File Name
68	Home Agent Addresses
69	SMTP Server Addresses
70	POP3 Server Addresses
71	NNTP Server Addresses
72	WWW Server Addresses
73	Finger Server Addresses
74	IRC Server Addresses
75	StreetTalk Server Addresses



Custom Option

General

Extend the DHCP Server functionality by adding custom options that will

Code: (None)

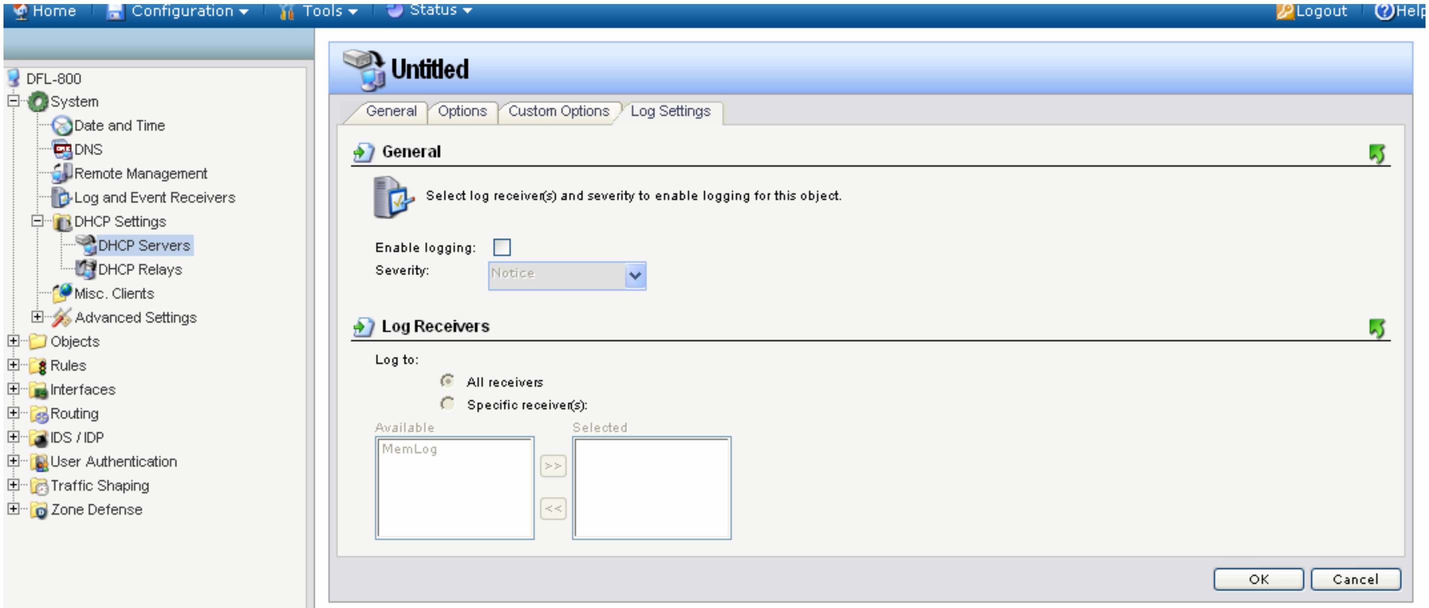
Type: UINT8

Parameter:

UINT8	1 byte
UINT8LIST	1 byte list
UINT16	2 bytes
UINT16LIST	2 bytes list
UINT32	4 bytes
UINT32LIST	4 bytes list
IP4	IP address
IP4LIST	IP address list
STRING	Character data
BINARY	Hexadecimal data

Comments

Comments:



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

Log Receivers

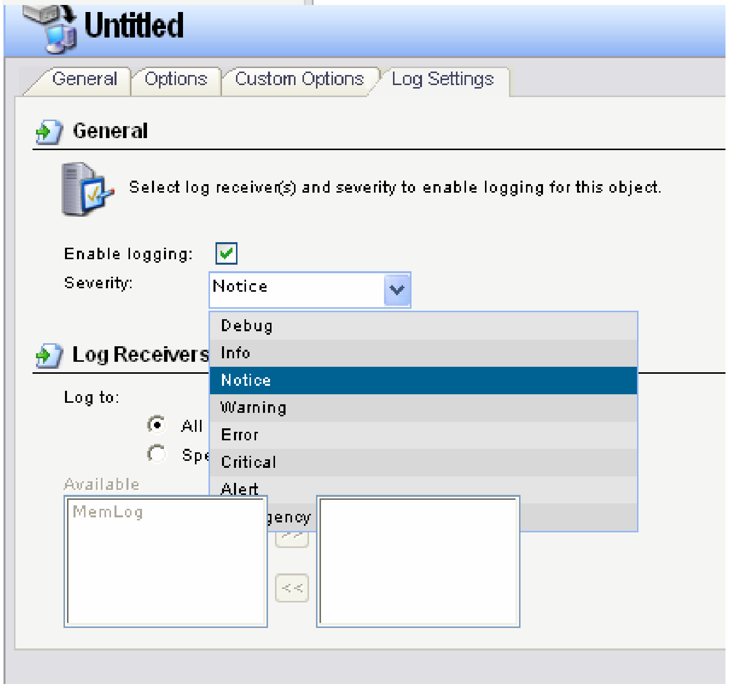
Log to:

● All receivers

○ Specific receiver(s):

Available: MemLog

Selected:



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: ☑

Severity: Notice

- Debug
- Info
- Notice
- Warning
- Error
- Critical
- Alert
- gency

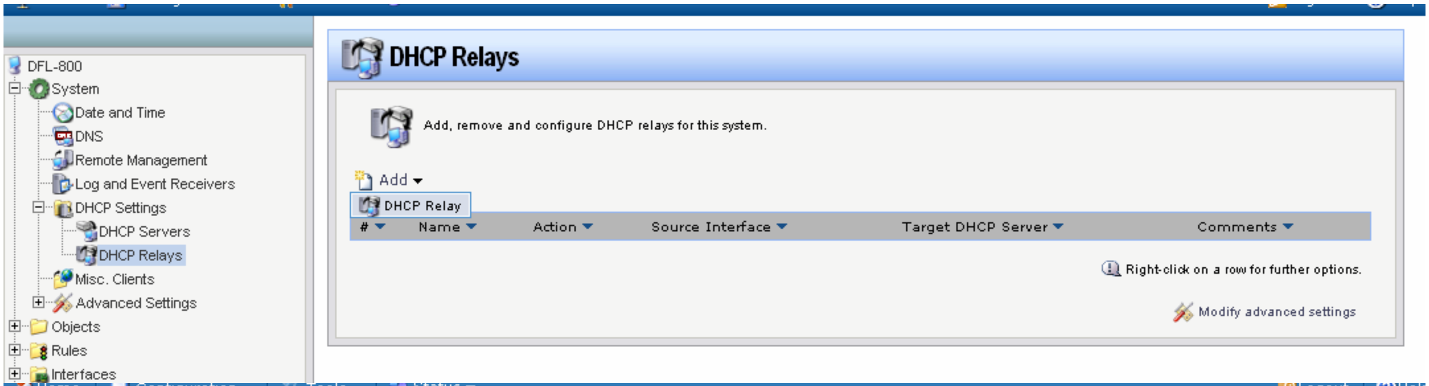
Log Receivers

Log to:

● All

○ Spe

Available: MemLog

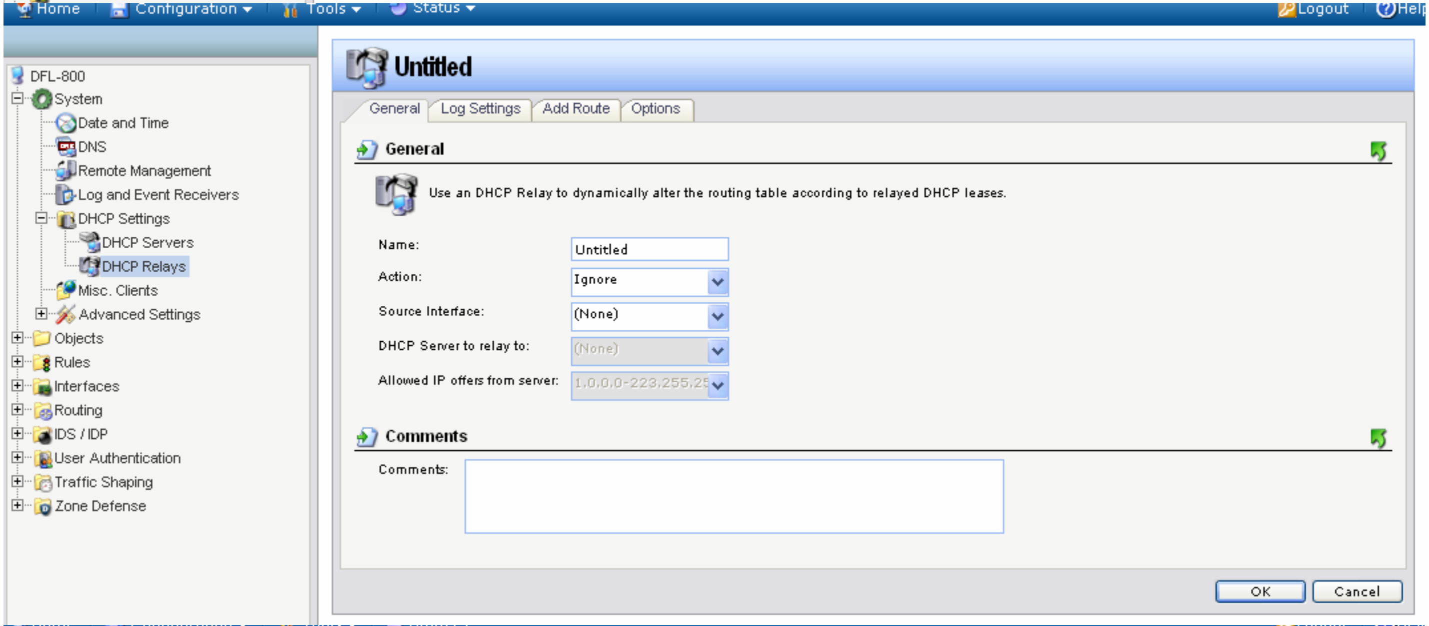


DHCP Relays

Add, remove and configure DHCP relays for this system.

#	Name	Action	Source Interface	Target DHCP Server	Comments

Right-click on a row for further options.



Untitled

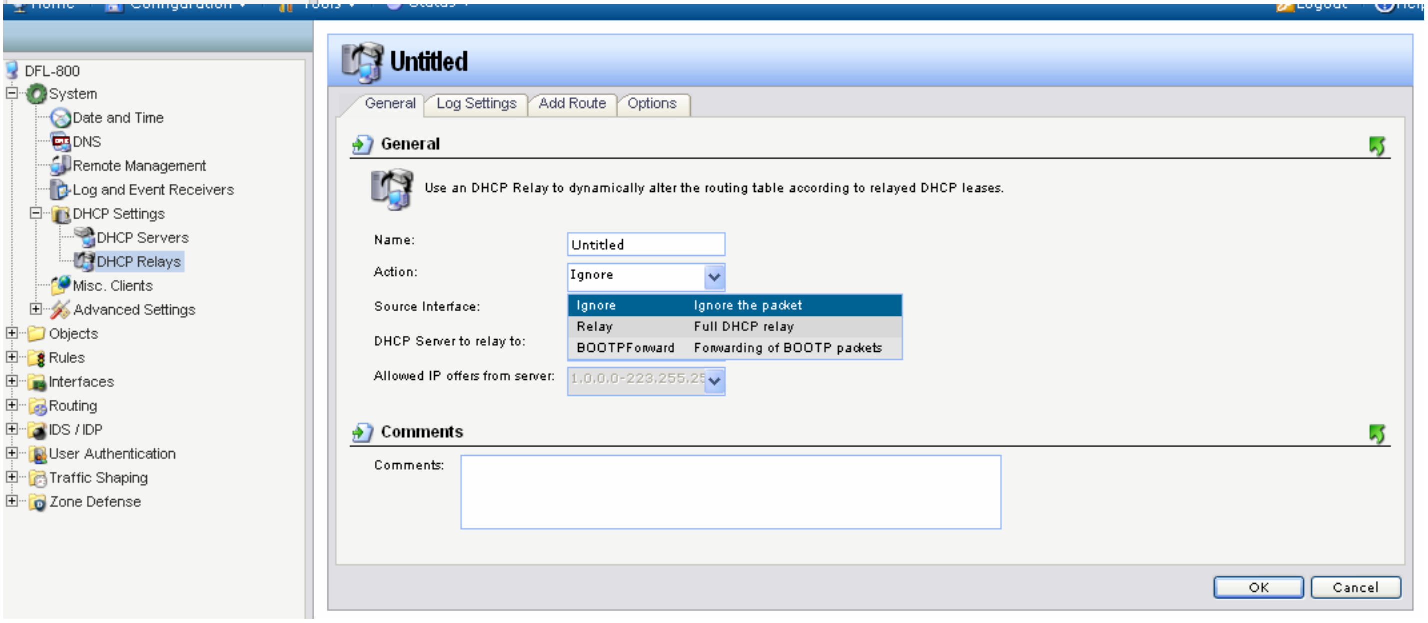
General

Use an DHCP Relay to dynamically alter the routing table according to relayed DHCP leases.

Name:	Untitled
Action:	Ignore
Source Interface:	(None)
DHCP Server to relay to:	(None)
Allowed IP offers from server:	1.0.0.0-223.255.25

Comments

Comments:



Untitled

General

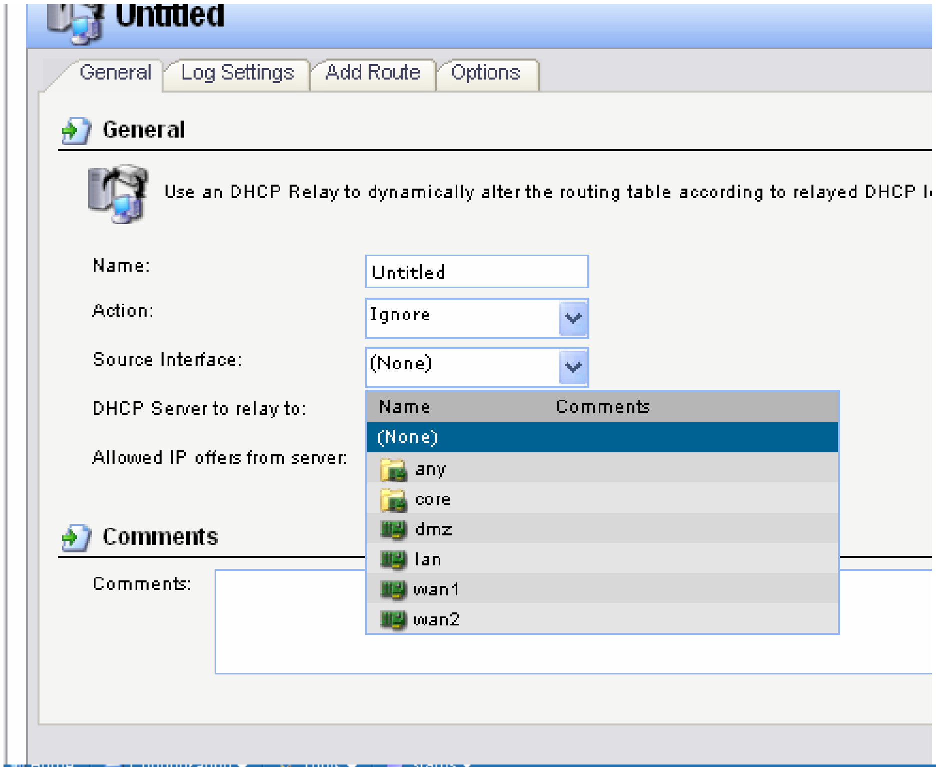
Use an DHCP Relay to dynamically alter the routing table according to relayed DHCP leases.

Name:	Untitled
Action:	Ignore
Source Interface:	
DHCP Server to relay to:	
Allowed IP offers from server:	1.0.0.0-223.255.25

Ignore	Ignore the packet
Relay	Full DHCP relay
BOOTPForward	Forwarding of BOOTP packets

Comments

Comments:



Untitled

General

Use an DHCP Relay to dynamically alter the routing table according to relayed DHCP l

Name: Untitled

Action: Ignore

Source Interface: (None)

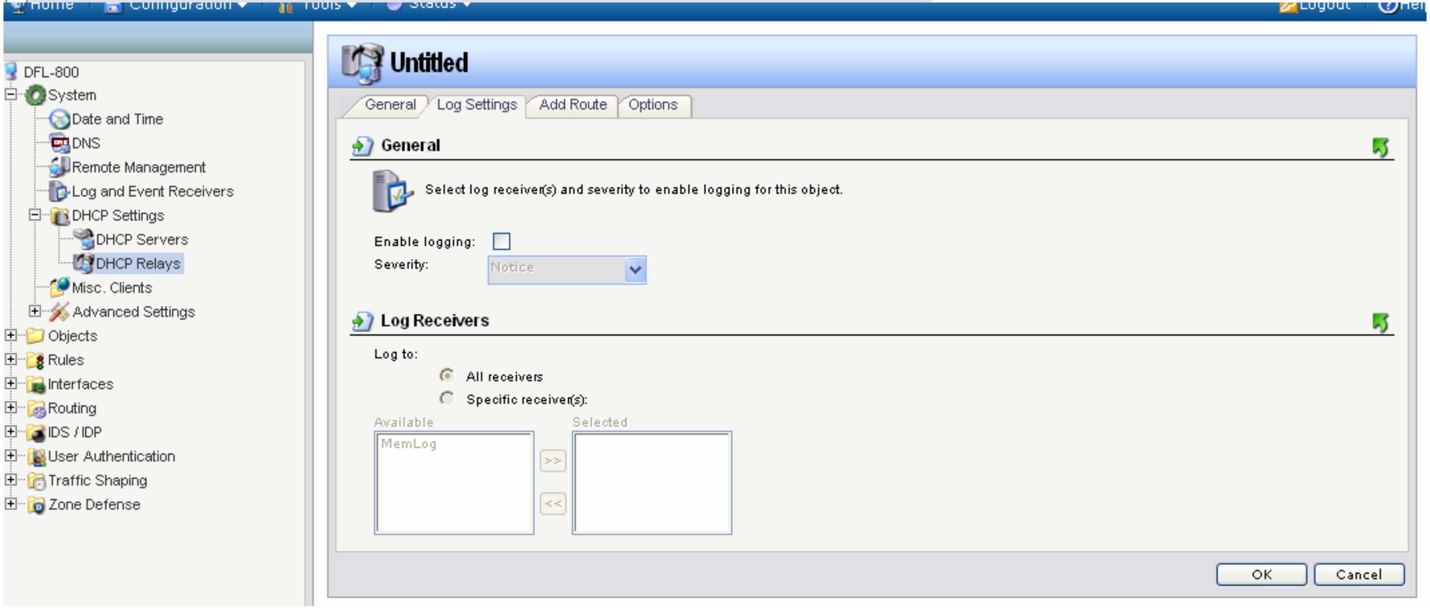
DHCP Server to relay to:

Allowed IP offers from server:

Name	Comments
(None)	
any	
core	
dmz	
lan	
wan1	
wan2	

Comments

Comments:



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

Log Receivers

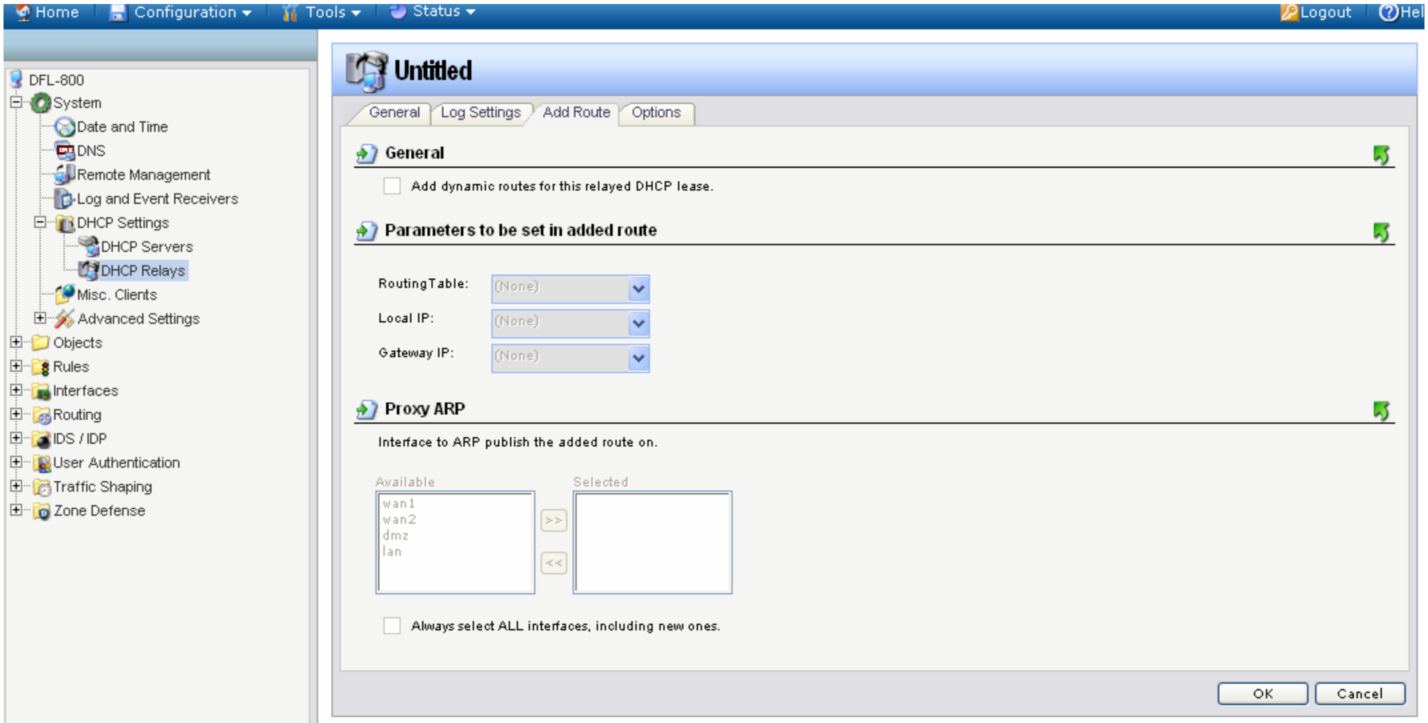
Log to:

● All receivers

○ Specific receiver(s):

Available: MemLog

Selected:



General

□ Add dynamic routes for this relayed DHCP lease.

Parameters to be set in added route

RoutingTable: (None)

Local IP: (None)

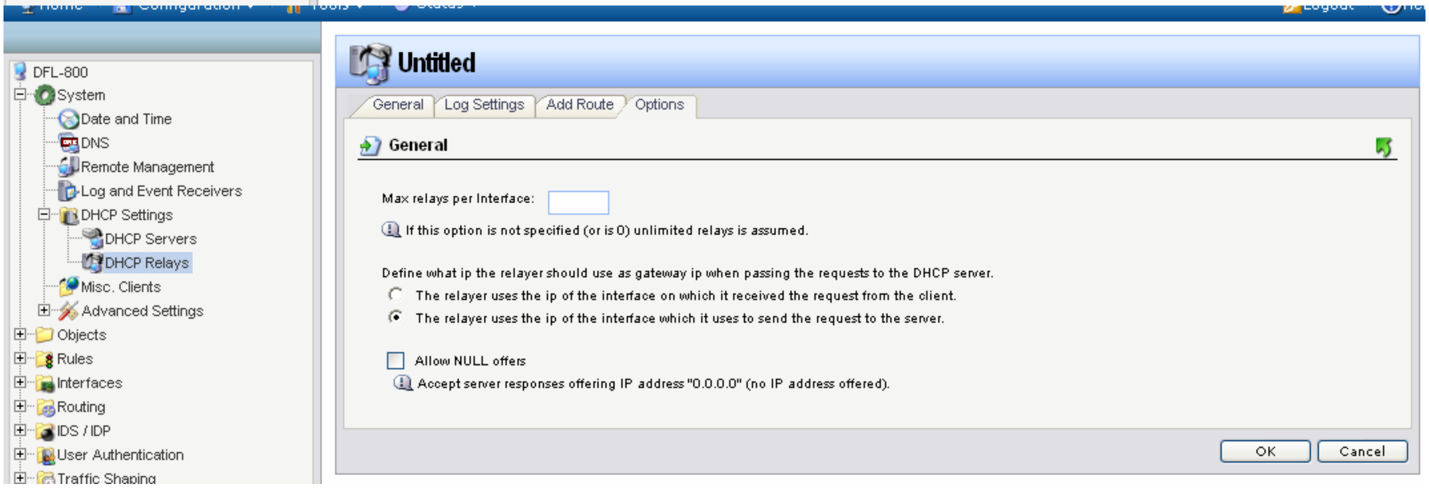
Gateway IP: (None)

Proxy ARP

Interface to ARP publish the added route on.

Available	Selected
wan1 wan2 dmz lan	

□ Always select ALL interfaces, including new ones.



General

Max relays per Interface:

If this option is not specified (or is 0) unlimited relays is assumed.

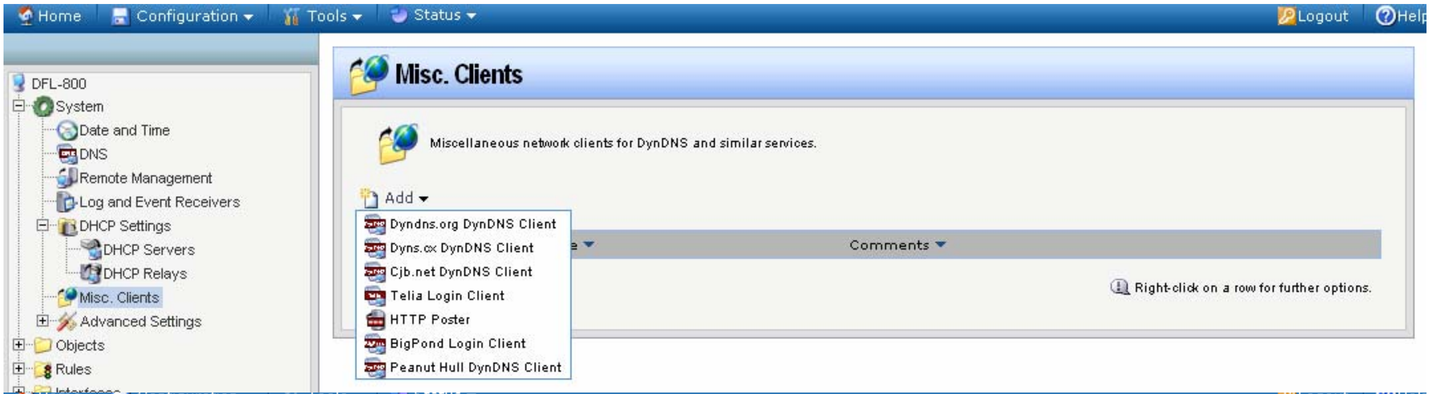
Define what ip the relayer should use as gateway ip when passing the requests to the DHCP server.

○ The relayer uses the ip of the interface on which it received the request from the client.

● The relayer uses the ip of the interface which it uses to send the request to the server.

□ Allow NULL offers

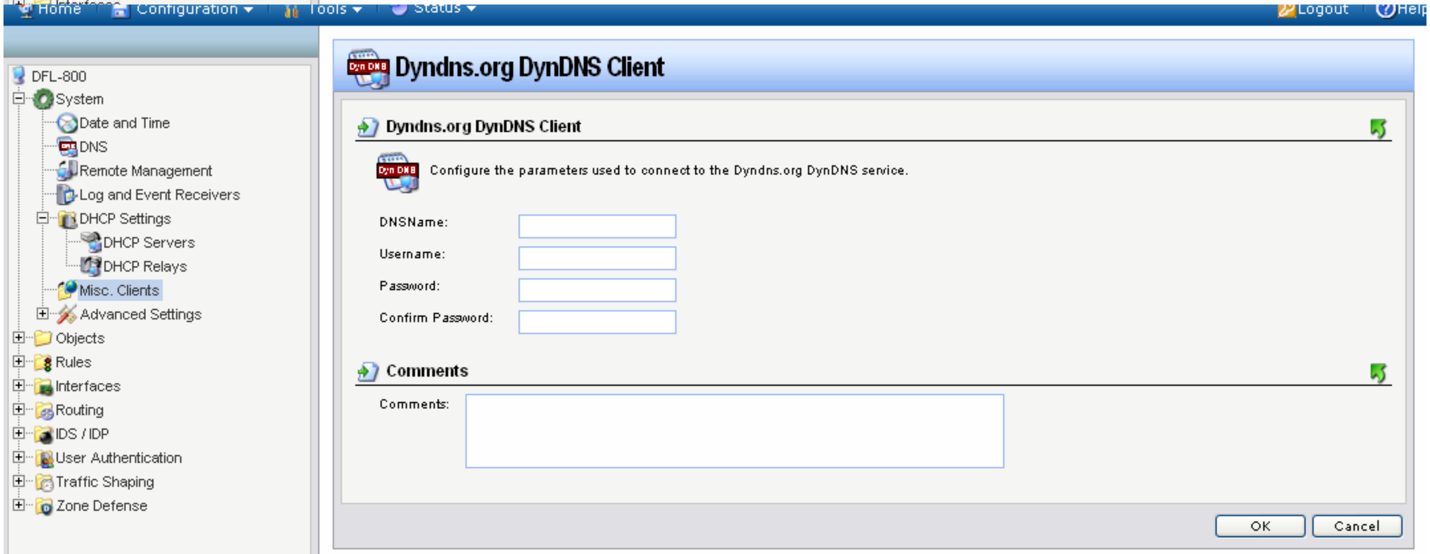
Accept server responses offering IP address "0.0.0.0" (no IP address offered).



Misc. Clients

Miscellaneous network clients for DynDNS and similar services.

Right-click on a row for further options.



Dyndns.org DynDNS Client

Dyndns.org DynDNS Client

Configure the parameters used to connect to the Dyndns.org DynDNS service.

DNSName:

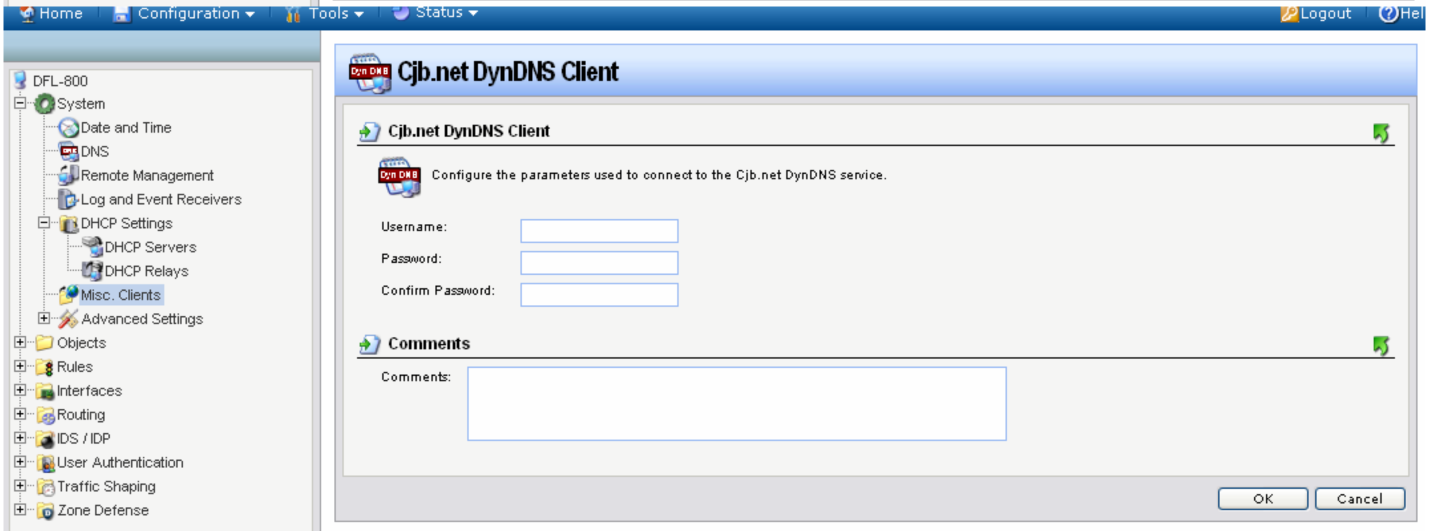
Username:

Password:

Confirm Password:

Comments

Comments:



Cjb.net DynDNS Client

Cjb.net DynDNS Client

Configure the parameters used to connect to the Cjb.net DynDNS service.

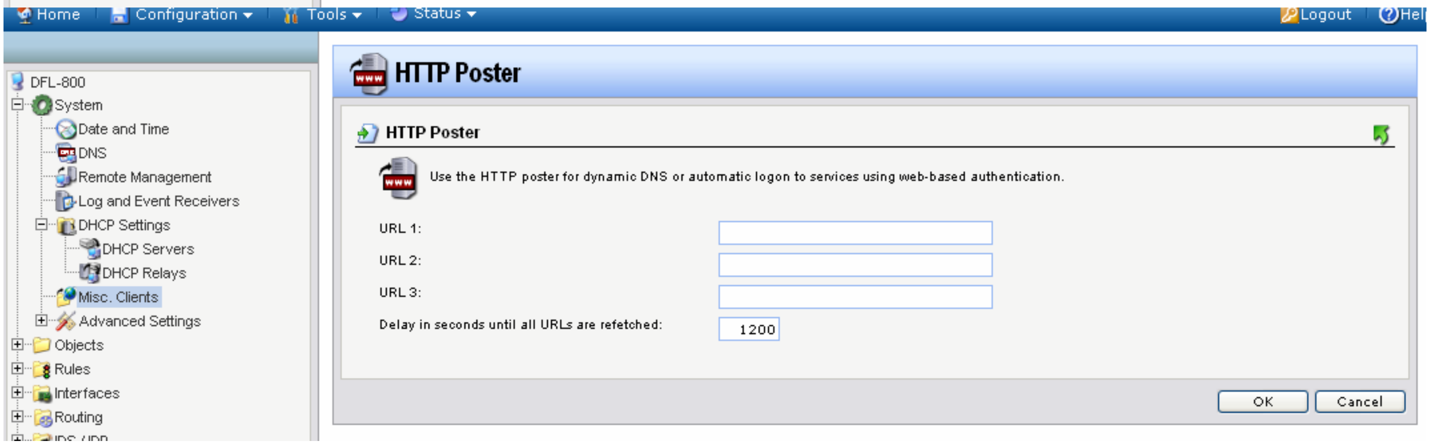
Username:

Password:

Confirm Password:

Comments

Comments:



HTTP Poster

HTTP Poster

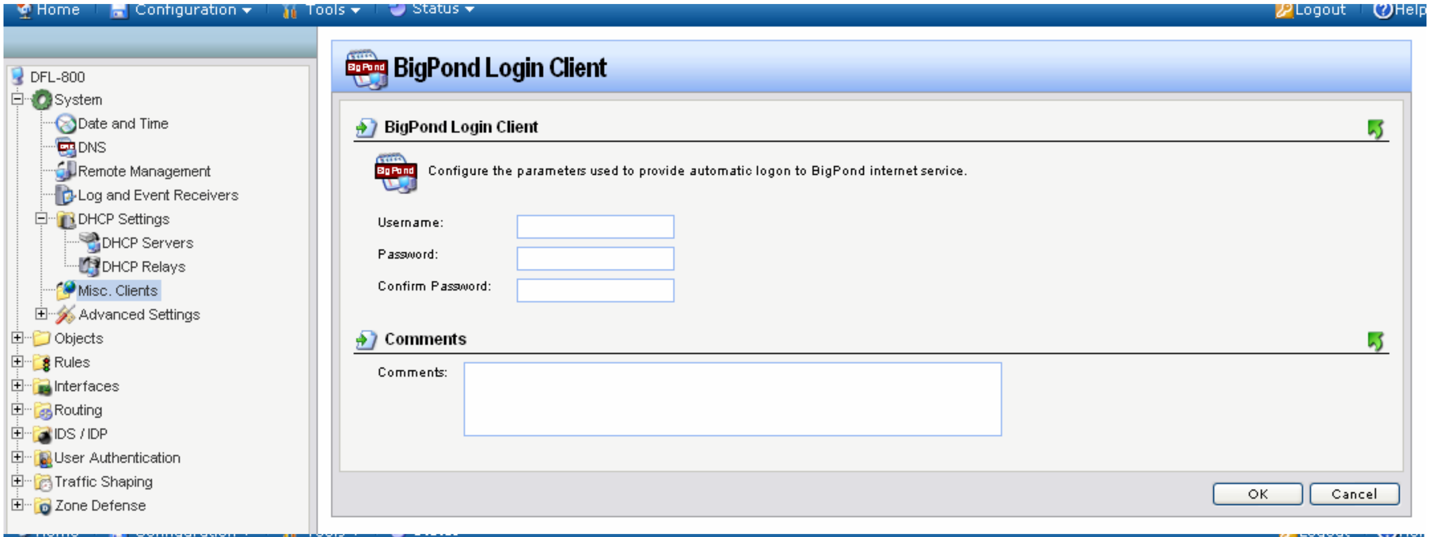
Use the HTTP poster for dynamic DNS or automatic logon to services using web-based authentication.

URL 1:

URL 2:

URL 3:

Delay in seconds until all URLs are refetched: 1200



BigPond Login Client

BigPond Login Client

Configure the parameters used to provide automatic logon to BigPond internet service.

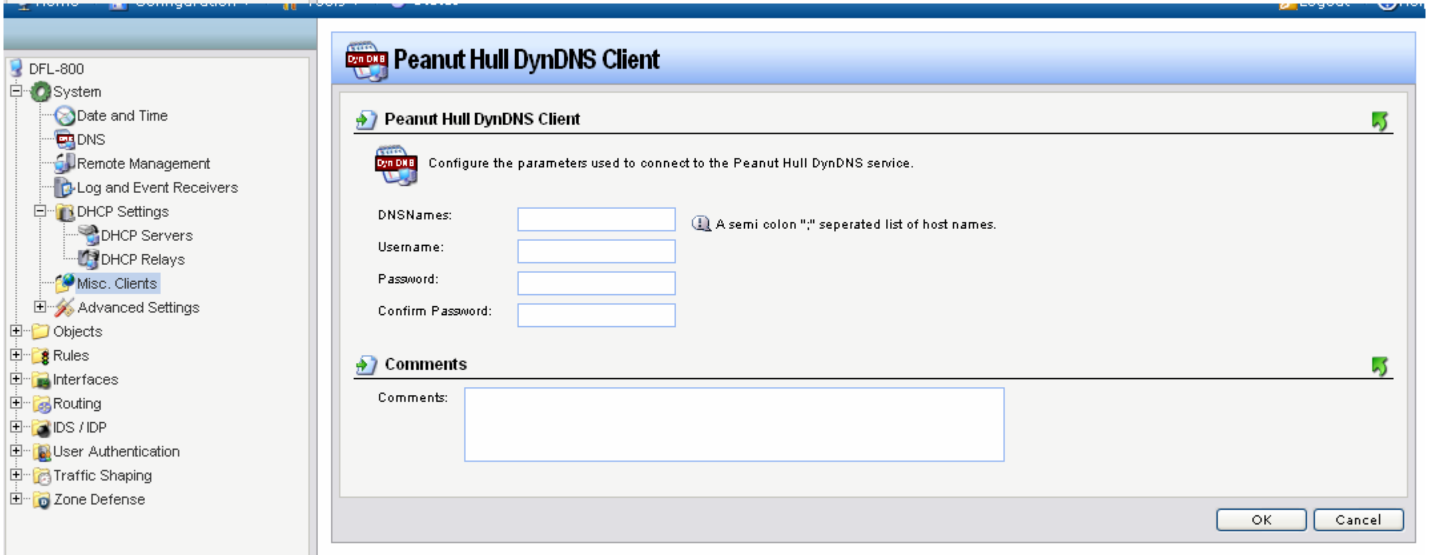
Username:

Password:

Confirm Password:

Comments

Comments:



Peanut Hull DynDNS Client

Peanut Hull DynDNS Client

Configure the parameters used to connect to the Peanut Hull DynDNS service.

DNSNames: A semi colon ";" seperated list of host names.

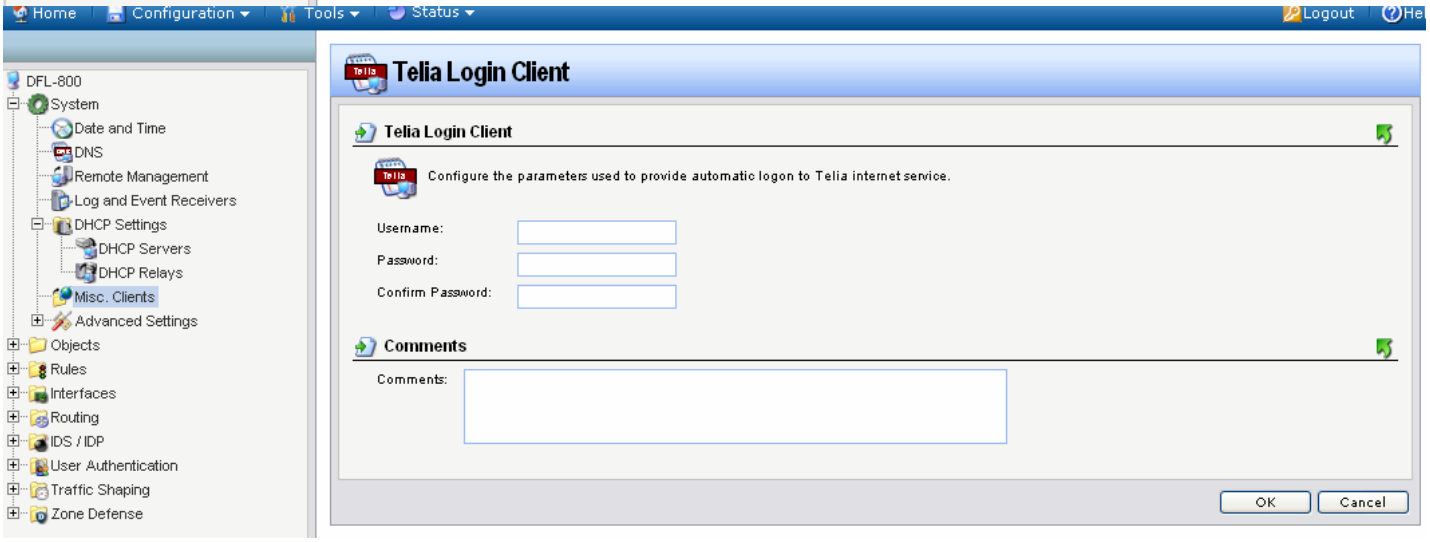
Username:

Password:

Confirm Password:

Comments

Comments:



Telia Login Client

Telia Login Client

Configure the parameters used to provide automatic logon to Telia internet service.

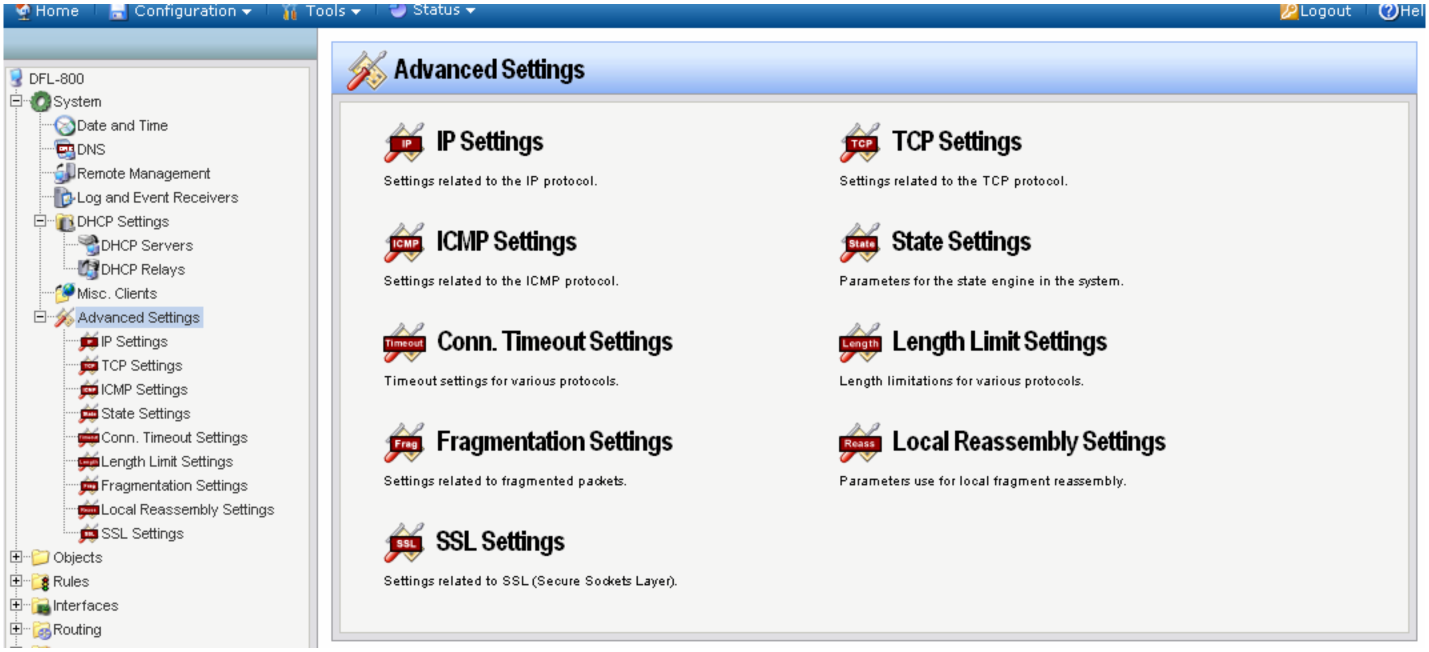
Username:

Password:

Confirm Password:

Comments

Comments:



Advanced Settings

IP Settings

Settings related to the IP protocol.

TCP Settings

Settings related to the TCP protocol.

ICMP Settings

Settings related to the ICMP protocol.

State Settings

Parameters for the state engine in the system.

Conn. Timeout Settings

Timeout settings for various protocols.

Length Limit Settings

Length limitations for various protocols.

Fragmentation Settings

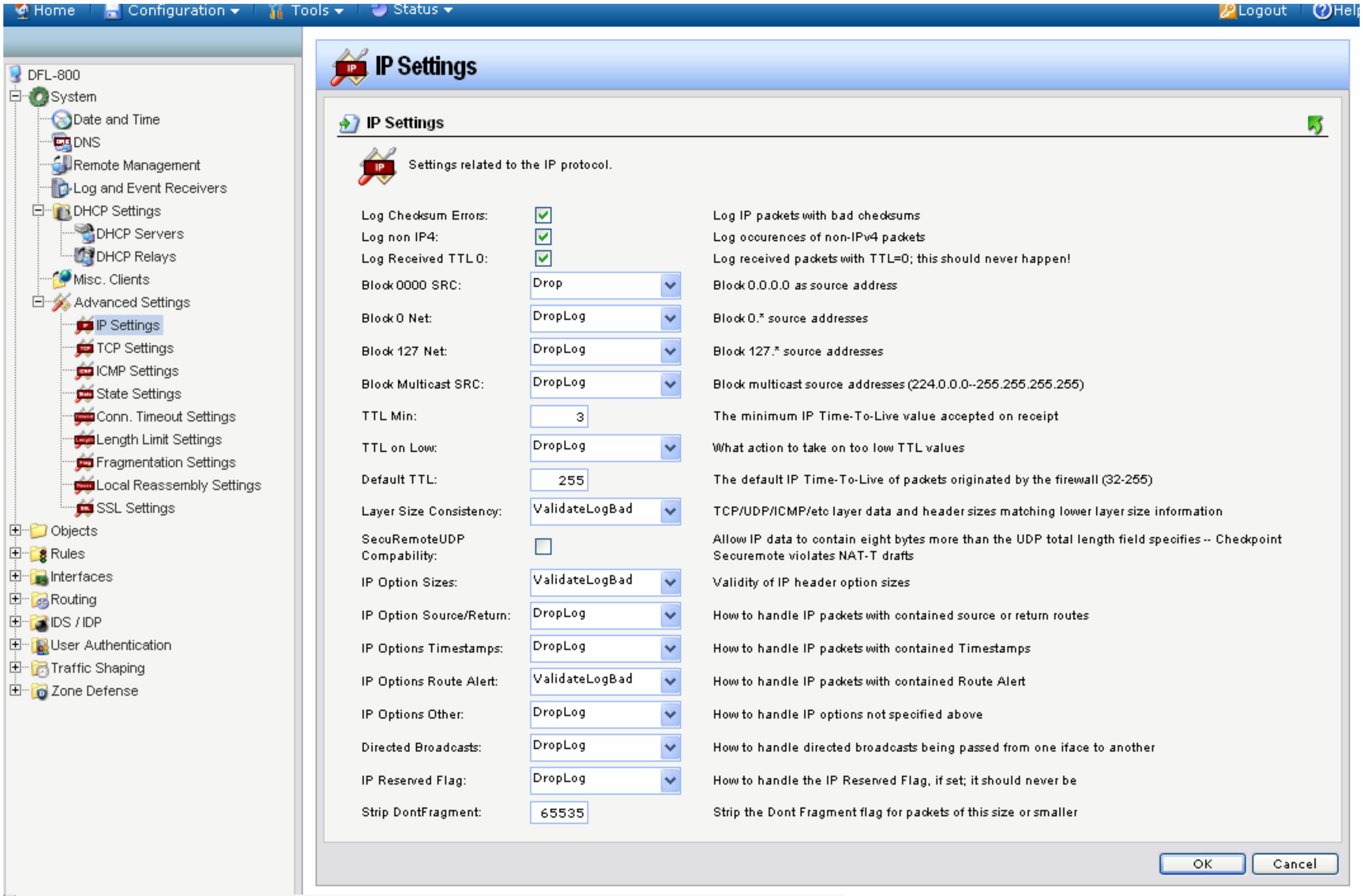
Settings related to fragmented packets.

Local Reassembly Settings

Parameters use for local fragment reassembly.

SSL Settings

Settings related to SSL (Secure Sockets Layer).

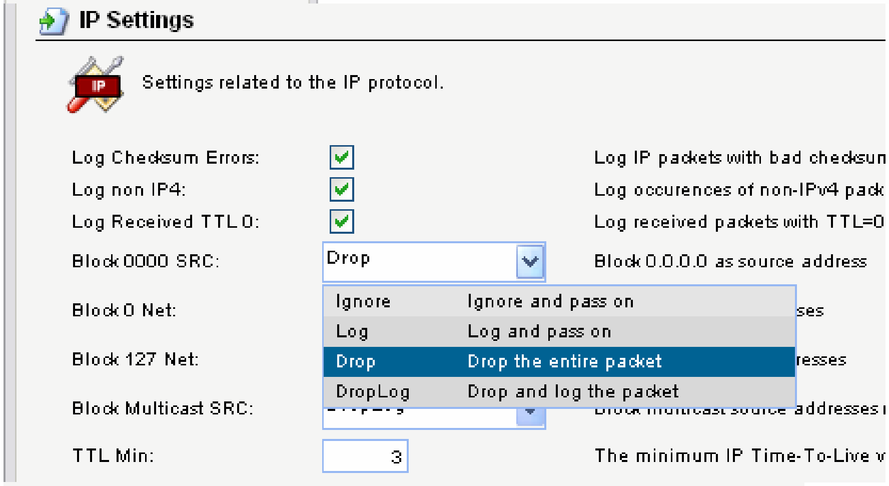


IP Settings

IP Settings

Settings related to the IP protocol.

Log Checksum Errors:	☑	Log IP packets with bad checksums
Log non IP4:	☑	Log occurences of non-IPv4 packets
Log Received TTL 0:	☑	Log received packets with TTL=0; this should never happen!
Block 0000 SRC:	Drop	Block 0.0.0.0 as source address
Block 0 Net:	DropLog	Block 0.* source addresses
Block 127 Net:	DropLog	Block 127.* source addresses
Block Multicast SRC:	DropLog	Block multicast source addresses (224.0.0.0-255.255.255.255)
TTL Min:	3	The minimum IP Time-To-Live value accepted on receipt
TTL on Low:	DropLog	What action to take on too low TTL values
Default TTL:	255	The default IP Time-To-Live of packets originated by the firewall (32-255)
Layer Size Consistency:	ValidateLogBad	TCP/UDP/ICMP/etc layer data and header sizes matching lower layer size information
SecuRemoteUDP Compability:	□	Allow IP data to contain eight bytes more than the UDP total length field specifies -- Checkpoint Securemote violates NAT-T drafts
IP Option Sizes:	ValidateLogBad	Validity of IP header option sizes
IP Option Source/Return:	DropLog	How to handle IP packets with contained source or return routes
IP Options Timestamps:	DropLog	How to handle IP packets with contained Timestamps
IP Options Route Alert:	ValidateLogBad	How to handle IP packets with contained Route Alert
IP Options Other:	DropLog	How to handle IP options not specified above
Directed Broadcasts:	DropLog	How to handle directed broadcasts being passed from one iface to another
IP Reserved Flag:	DropLog	How to handle the IP Reserved Flag, if set; it should never be
Strip DontFragment:	65535	Strip the Dont Fragment flag for packets of this size or smaller

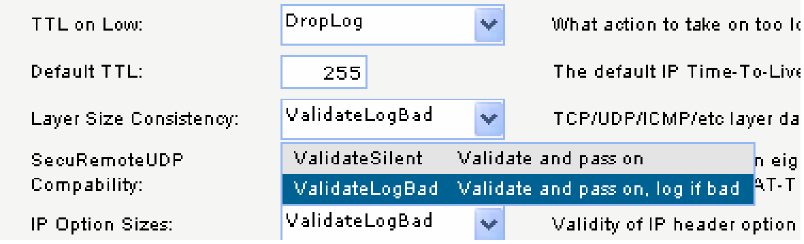


IP Settings

Settings related to the IP protocol.

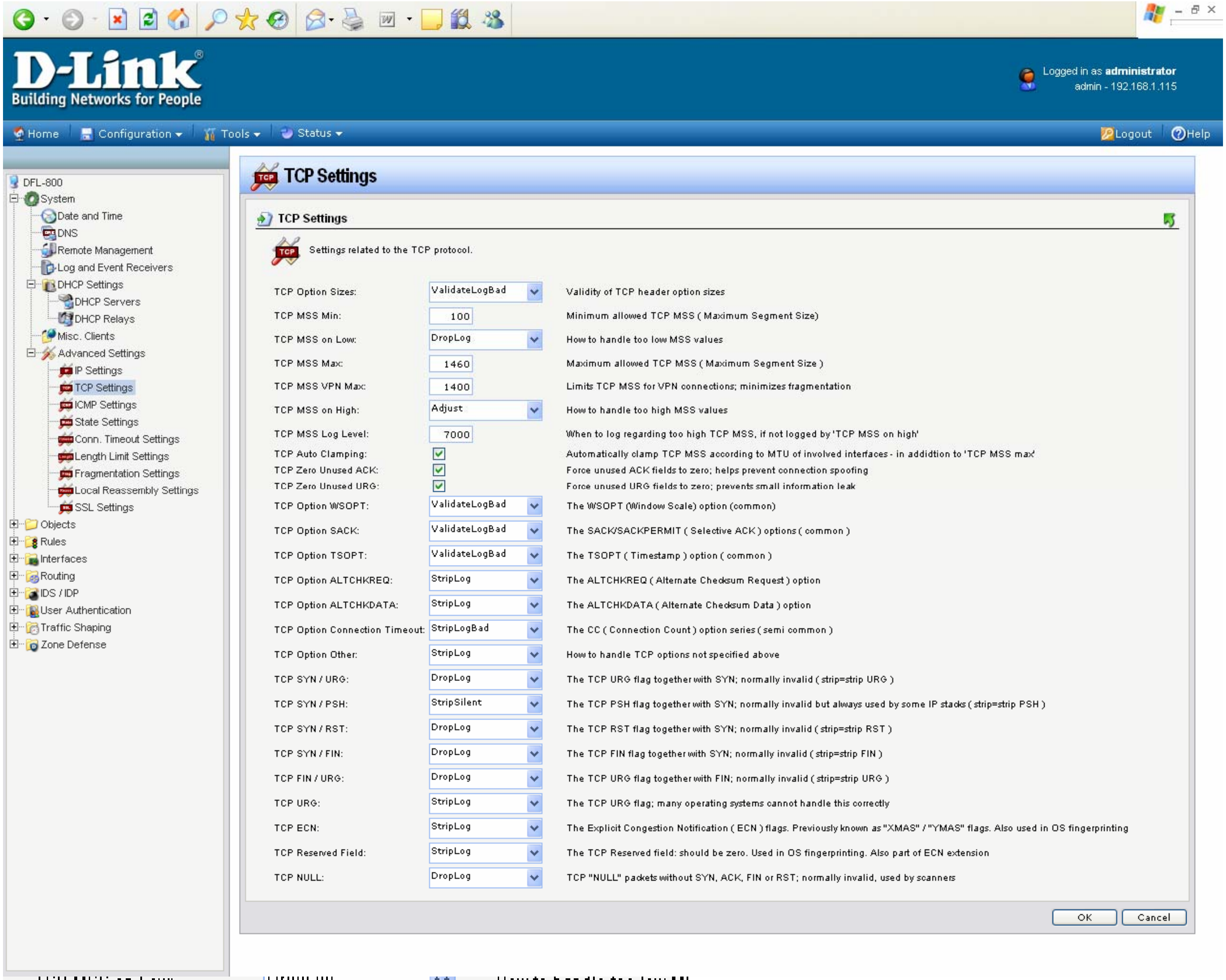
Log Checksum Errors:	☑	Log IP packets with bad checksun
Log non IP4:	☑	Log occurences of non-IPv4 pack
Log Received TTL 0:	☑	Log received packets with TTL=0
Block 0000 SRC:	Drop	Block 0.0.0.0 as source address
Block 0 Net:		ses
Block 127 Net:		resses
Block Multicast SRC:		Block multicast source addresses
TTL Min:	3	The minimum IP Time-To-Live v

Ignore	Ignore and pass on
Log	Log and pass on
Drop	Drop the entire packet
DropLog	Drop and log the packet



TTL on Low:	DropLog	What action to take on too lo
Default TTL:	255	The default IP Time-To-Live
Layer Size Consistency:	ValidateLogBad	TCP/UDP/ICMP/etc layer da
SecuRemoteUDP Compability:		n eig AT-T
IP Option Sizes:	ValidateLogBad	Validity of IP header option

ValidateSilent	Validate and pass on
ValidateLogBad	Validate and pass on, log if bad

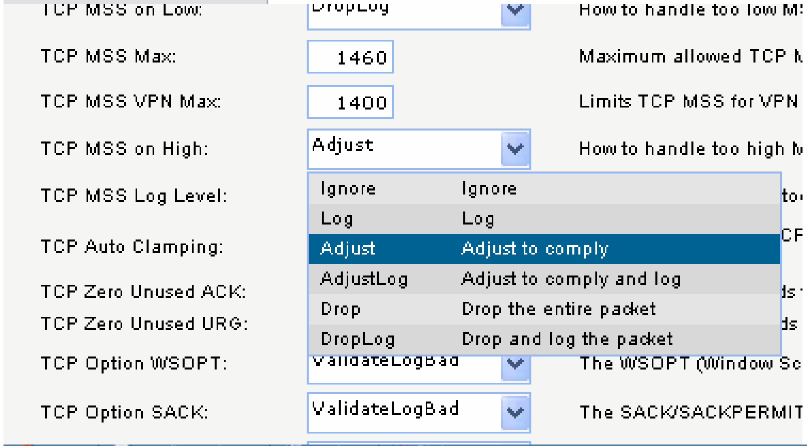


TCP Settings

TCP Settings

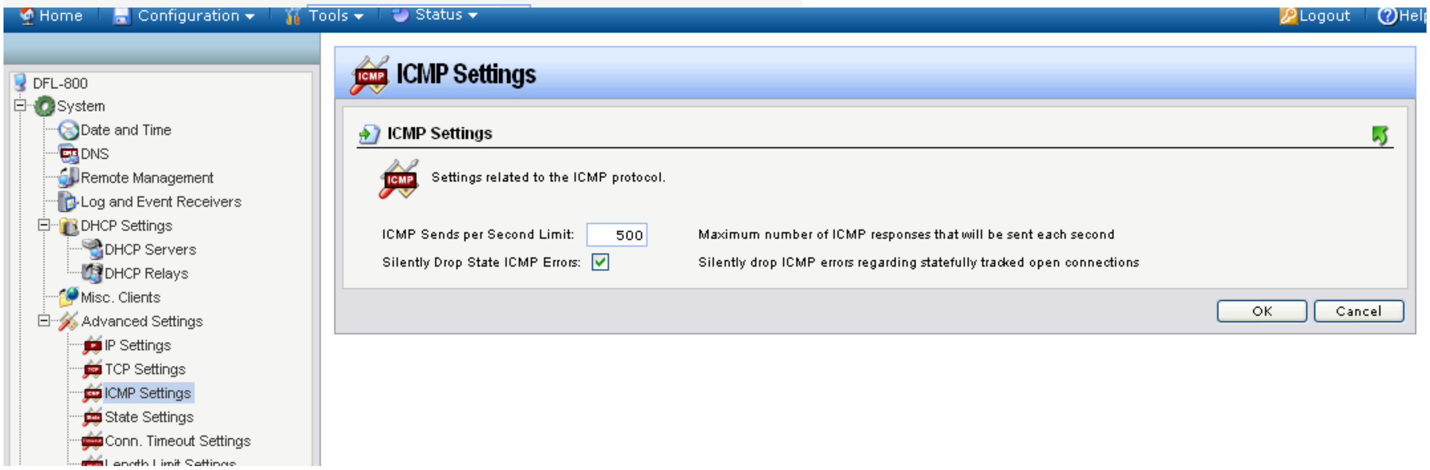
Settings related to the TCP protocol.

TCP Option Sizes:	ValidateLogBad	Validity of TCP header option sizes
TCP MSS Min:	100	Minimum allowed TCP MSS (Maximum Segment Size)
TCP MSS on Low:	DropLog	How to handle too low MSS values
TCP MSS Max:	1460	Maximum allowed TCP MSS (Maximum Segment Size)
TCP MSS VPN Max:	1400	Limits TCP MSS for VPN connections; minimizes fragmentation
TCP MSS on High:	Adjust	How to handle too high MSS values
TCP MSS Log Level:	7000	When to log regarding too high TCP MSS, if not logged by 'TCP MSS on high'
TCP Auto Clamping:	☑	Automatically clamp TCP MSS according to MTU of involved interfaces - in addidtion to 'TCP MSS max'
TCP Zero Unused ACK:	☑	Force unused ACK fields to zero; helps prevent connection spoofing
TCP Zero Unused URG:	☑	Force unused URG fields to zero; prevents small information leak
TCP Option WSOPT:	ValidateLogBad	The WSOPT (Window Scale) option (common)
TCP Option SACK:	ValidateLogBad	The SACK/SACKPERMIT (Selective ACK) options (common)
TCP Option TSOPT:	ValidateLogBad	The TSOPT (Timestamp) option (common)
TCP Option ALTCHKREQ:	StripLog	The ALTCHKREQ (Alternate Checksum Request) option
TCP Option ALTCHKDATA:	StripLog	The ALTCHKDATA (Alternate Checksum Data) option
TCP Option Connection Timeout:	StripLogBad	The CC (Connection Count) option series (semi common)
TCP Option Other:	StripLog	How to handle TCP options not specified above
TCP SYN / URG:	DropLog	The TCP URG flag together with SYN; normally invalid (strip=strip URG)
TCP SYN / PSH:	StripSilent	The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH)
TCP SYN / RST:	DropLog	The TCP RST flag together with SYN; normally invalid (strip=strip RST)
TCP SYN / FIN:	DropLog	The TCP FIN flag together with SYN; normally invalid (strip=strip FIN)
TCP FIN / URG:	DropLog	The TCP URG flag together with FIN; normally invalid (strip=strip URG)
TCP URG:	StripLog	The TCP URG flag; many operating systems cannot handle this correctly
TCP ECN:	StripLog	The Explicit Congestion Notification (ECN) flags. Previously known as "XMAS" / "YMAS" flags. Also used in OS fingerprinting
TCP Reserved Field:	StripLog	The TCP Reserved field: should be zero. Used in OS fingerprinting. Also part of ECN extension
TCP NULL:	DropLog	TCP "NULL" packets without SYN, ACK, FIN or RST; normally invalid, used by scanners



TCP MSS on Low:	DropLog	How to handle too low M
TCP MSS Max:	1460	Maximum allowed TCP M
TCP MSS VPN Max:	1400	Limits TCP MSS for VPN
TCP MSS on High:	Adjust	How to handle too high M
TCP MSS Log Level:		to
TCP Auto Clamping:		CF
TCP Zero Unused ACK:		ds
TCP Zero Unused URG:		ds
TCP Option WSOPT:	ValidateLogBad	The WSOPT (Window Sc
TCP Option SACK:	ValidateLogBad	The SACK/SACKPERMIT

Ignore	Ignore
Log	Log
Adjust	Adjust to comply
AdjustLog	Adjust to comply and log
Drop	Drop the entire packet
DropLog	Drop and log the packet

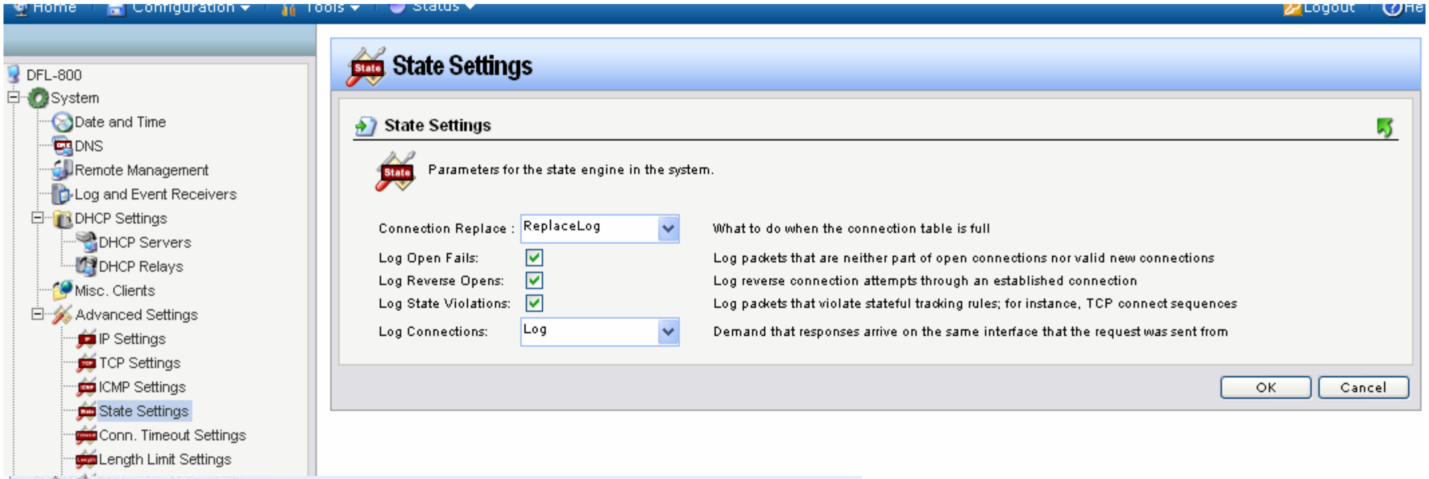


ICMP Settings

ICMP Settings

Settings related to the ICMP protocol.

ICMP Sends per Second Limit:	500	Maximum number of ICMP responses that will be sent each second
Silently Drop State ICMP Errors:	☑	Silently drop ICMP errors regarding statefully tracked open connections

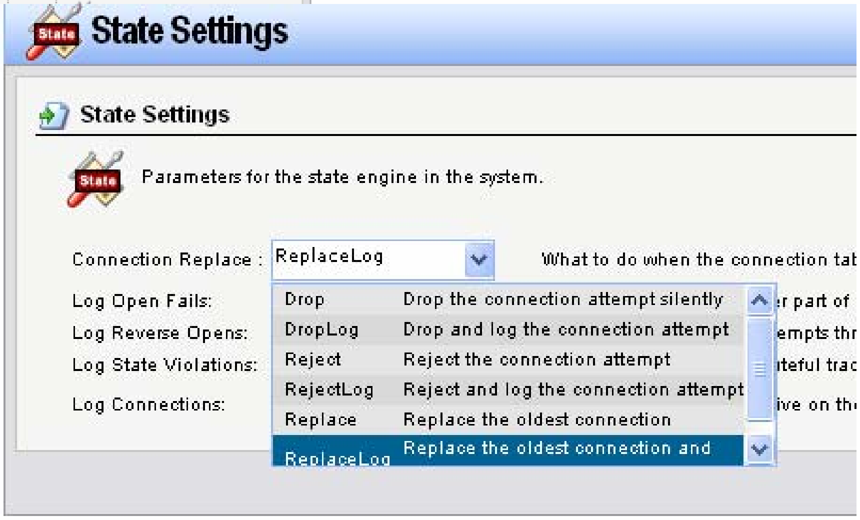


State Settings

State Settings

Parameters for the state engine in the system.

Connection Replace :	ReplaceLog	What to do when the connection table is full
Log Open Fails:	☑	Log packets that are neither part of open connections nor valid new connections
Log Reverse Opens:	☑	Log reverse connection attempts through an established connection
Log State Violations:	☑	Log packets that violate stateful tracking rules; for instance, TCP connect sequences
Log Connections:	Log	Demand that responses arrive on the same interface that the request was sent from



State Settings

State Settings

Parameters for the state engine in the system.

Connection Replace : ReplaceLog — What to do when the connection tab

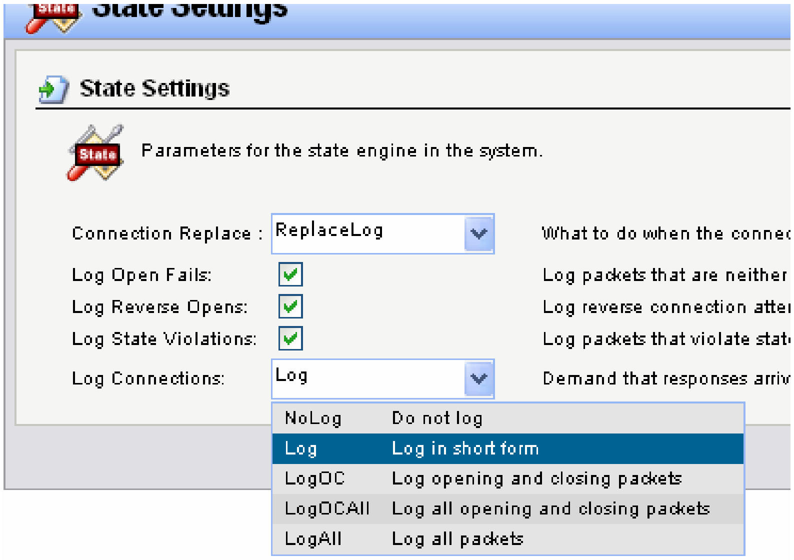
Log Open Fails: — r part of

Log Reverse Opens: — empts thr

Log State Violations: — teful trac

Log Connections: — ive on th

Drop	Drop the connection attempt silently
DropLog	Drop and log the connection attempt
Reject	Reject the connection attempt
RejectLog	Reject and log the connection attempt
Replace	Replace the oldest connection
ReplaceLog	Replace the oldest connection and



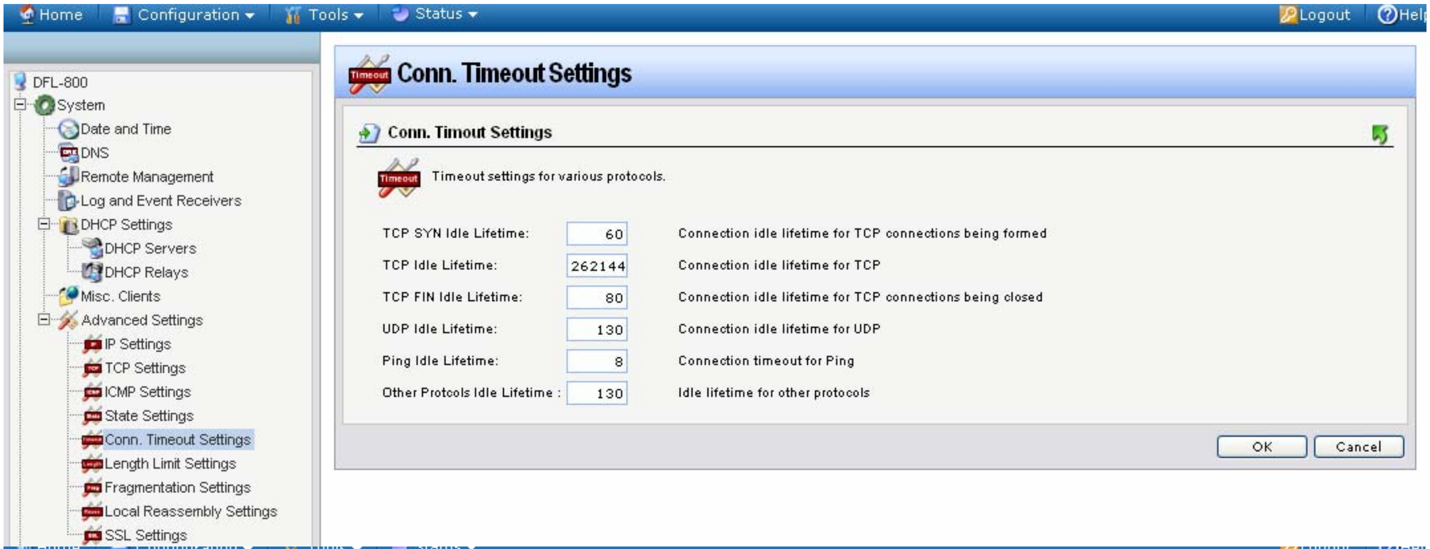
State Settings

State Settings

Parameters for the state engine in the system.

Connection Replace :	ReplaceLog	What to do when the connec
Log Open Fails:	☑	Log packets that are neither
Log Reverse Opens:	☑	Log reverse connection atte
Log State Violations:	☑	Log packets that violate stat
Log Connections:	Log	Demand that responses arriv

NoLog	Do not log
Log	Log in short form
LogOC	Log opening and closing packets
LogOCAll	Log all opening and closing packets
LogAll	Log all packets

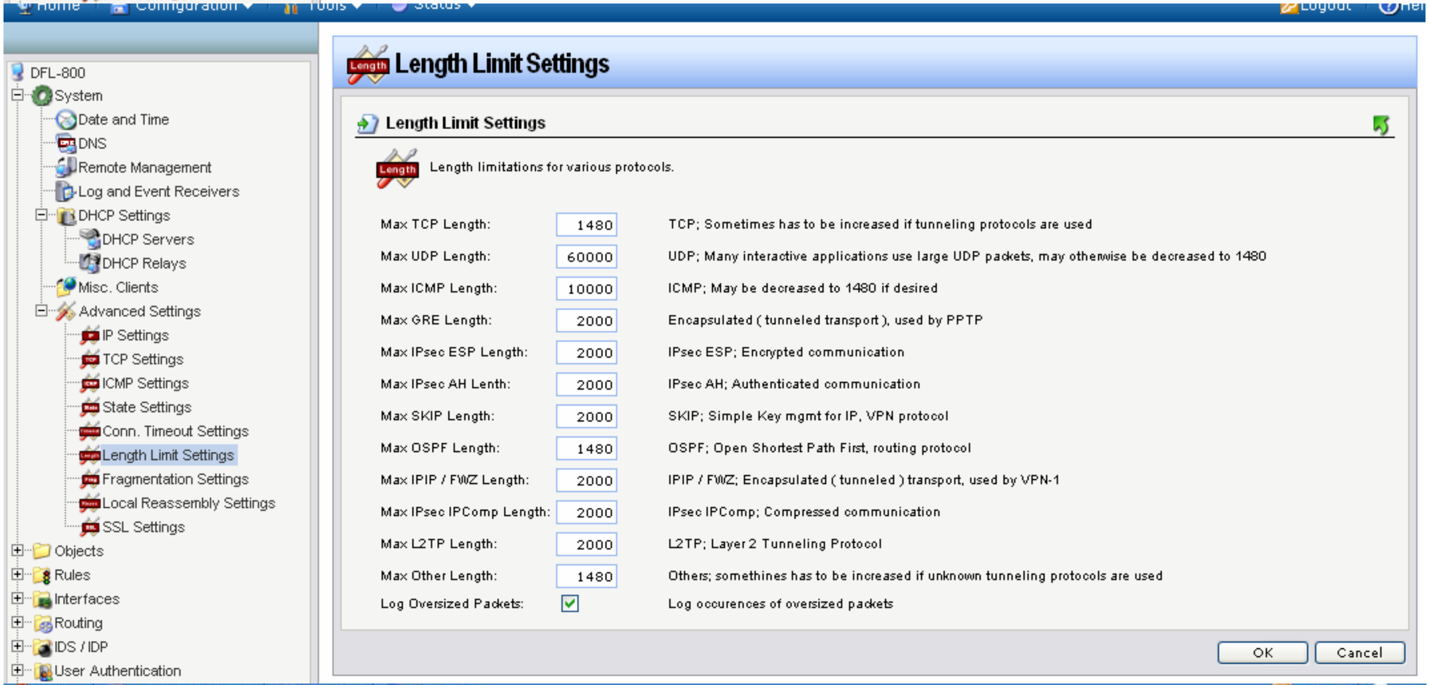


Conn. Timeout Settings

Conn. Timout Settings

Timeout settings for various protocols.

TCP SYN Idle Lifetime:	60	Connection idle lifetime for TCP connections being formed
TCP Idle Lifetime:	262144	Connection idle lifetime for TCP
TCP FIN Idle Lifetime:	80	Connection idle lifetime for TCP connections being closed
UDP Idle Lifetime:	130	Connection idle lifetime for UDP
Ping Idle Lifetime:	8	Connection timeout for Ping
Other Protocols Idle Lifetime :	130	Idle lifetime for other protocols

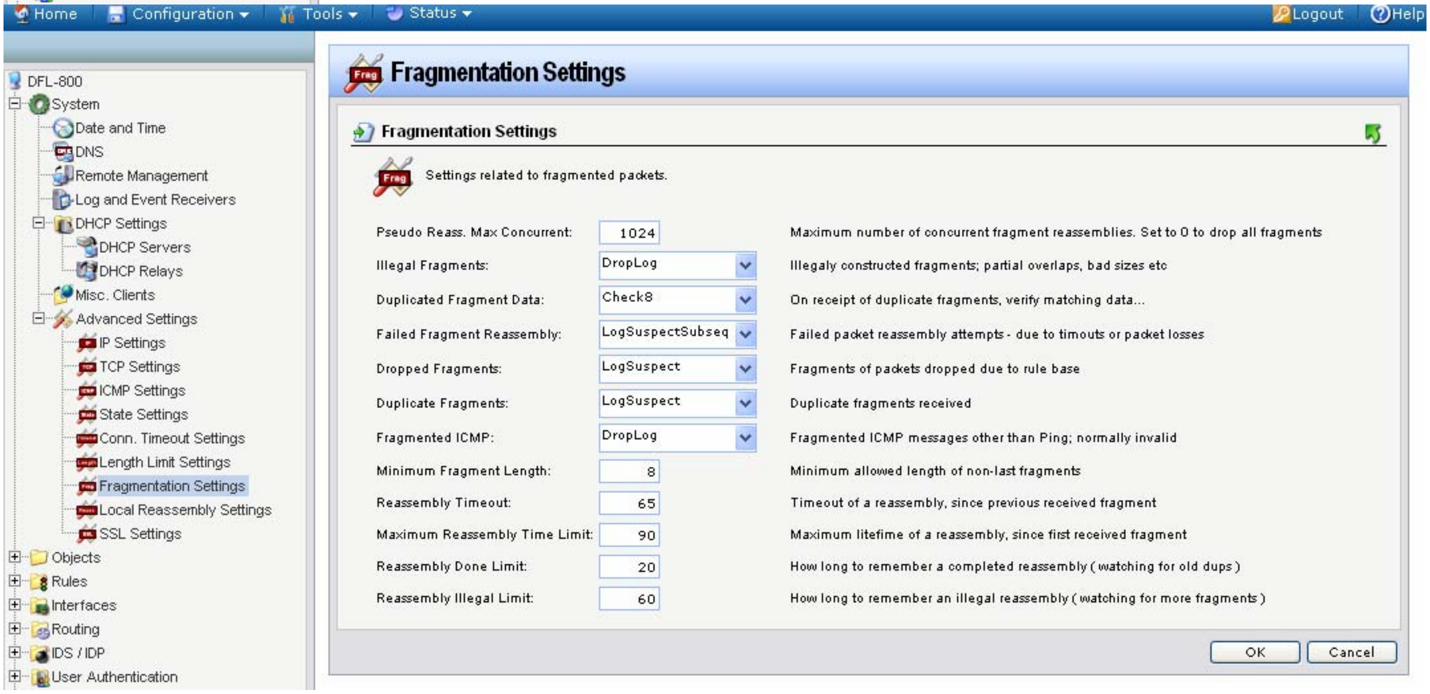


Length Limit Settings

Length Limit Settings

Length limitations for various protocols.

Max TCP Length:	1480	TCP; Sometimes has to be increased if tunneling protocols are used
Max UDP Length:	60000	UDP; Many interactive applications use large UDP packets, may otherwise be decreased to 1480
Max ICMP Length:	10000	ICMP; May be decreased to 1480 if desired
Max GRE Length:	2000	Encapsulated (tunneled transport), used by PPTP
Max IPsec ESP Length:	2000	IPsec ESP; Encrypted communication
Max IPsec AH Lenth:	2000	IPsec AH; Authenticated communication
Max SKIP Length:	2000	SKIP; Simple Key mgmt for IP, VPN protocol
Max OSPF Length:	1480	OSPF; Open Shortest Path First, routing protocol
Max IPIP / FWZ Length:	2000	IPIP / FWZ; Encapsulated (tunneled) transport, used by VPN-1
Max IPsec IPComp Length:	2000	IPsec IPComp; Compressed communication
Max L2TP Length:	2000	L2TP; Layer 2 Tunneling Protocol
Max Other Length:	1480	Others; somethines has to be increased if unknown tunneling protocols are used
Log Oversized Packets:	☑	Log occurences of oversized packets

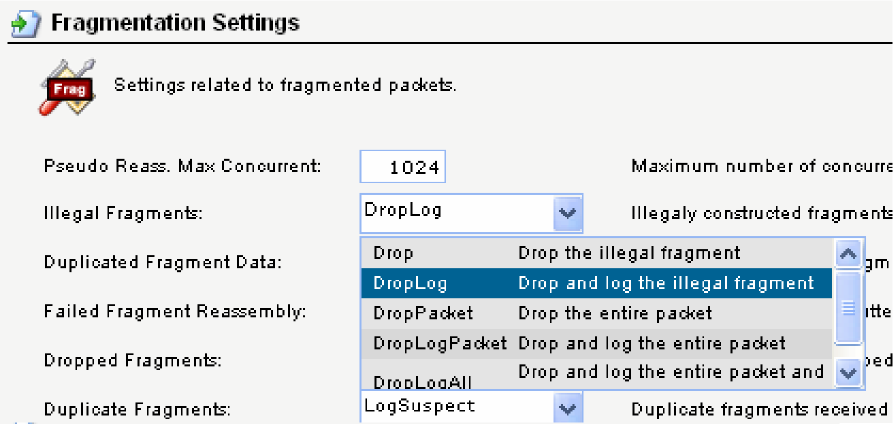


Fragmentation Settings

Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent:	1024	Maximum number of concurrent fragment reassemblies. Set to 0 to drop all fragments
Illegal Fragments:	DropLog	Illegaly constructed fragments; partial overlaps, bad sizes etc
Duplicated Fragment Data:	Check8	On receipt of duplicate fragments, verify matching data...
Failed Fragment Reassembly:	LogSuspectSubseq	Failed packet reassembly attempts - due to timouts or packet losses
Dropped Fragments:	LogSuspect	Fragments of packets dropped due to rule base
Duplicate Fragments:	LogSuspect	Duplicate fragments received
Fragmented ICMP:	DropLog	Fragmented ICMP messages other than Ping; normally invalid
Minimum Fragment Length:	8	Minimum allowed length of non-last fragments
Reassembly Timeout:	65	Timeout of a reassembly, since previous received fragment
Maximum Reassembly Time Limit:	90	Maximum lifetime of a reassembly, since first received fragment
Reassembly Done Limit:	20	How long to remember a completed reassembly (watching for old dups)
Reassembly Illegal Limit:	60	How long to remember an illegal reassembly (watching for more fragments)



Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent: 1024 Maximum number of concurre

Illegal Fragments: DropLog Illegaly constructed fragments

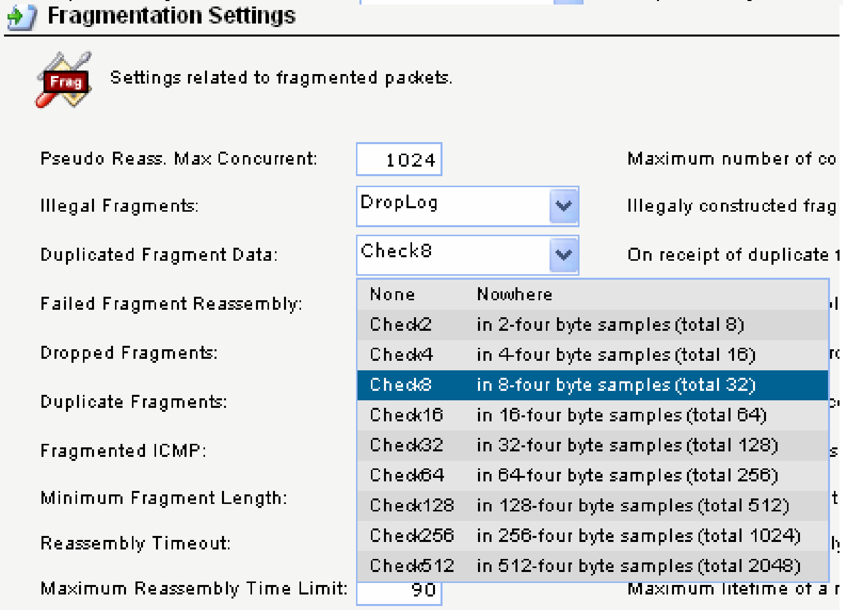
Duplicated Fragment Data: gm

Failed Fragment Reassembly: itte

Dropped Fragments: ped

Duplicate Fragments: LogSuspect Duplicate fragments received

Drop	Drop the illegal fragment
DropLog	Drop and log the illegal fragment
DropPacket	Drop the entire packet
DropLogPacket	Drop and log the entire packet
DropLogAll	Drop and log the entire packet and



Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent: 1024 Maximum number of co

Illegal Fragments: DropLog Illegaly constructed frag

Duplicated Fragment Data: Check8 On receipt of duplicate f

Failed Fragment Reassembly:

Dropped Fragments:

Duplicate Fragments:

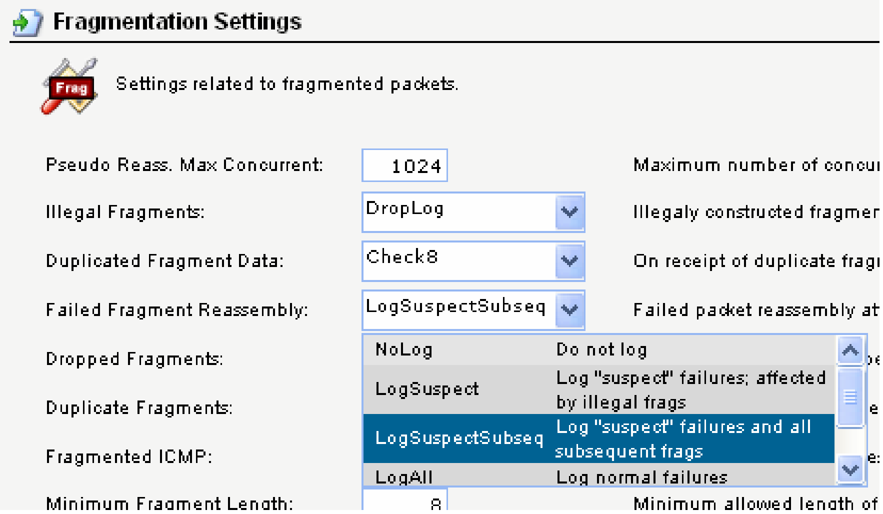
Fragmented ICMP:

Minimum Fragment Length:

Reassembly Timeout:

Maximum Reassembly Time Limit: 90 Maximum lifetime of a r

None	Nowhere
Check2	in 2-four byte samples (total 8)
Check4	in 4-four byte samples (total 16)
Check8	in 8-four byte samples (total 32)
Check16	in 16-four byte samples (total 64)
Check32	in 32-four byte samples (total 128)
Check64	in 64-four byte samples (total 256)
Check128	in 128-four byte samples (total 512)
Check256	in 256-four byte samples (total 1024)
Check512	in 512-four byte samples (total 2048)



Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent: 1024 Maximum number of concur

Illegal Fragments: DropLog Illegaly constructed fragmer

Duplicated Fragment Data: Check8 On receipt of duplicate frag

Failed Fragment Reassembly: LogSuspectSubseq Failed packet reassembly at

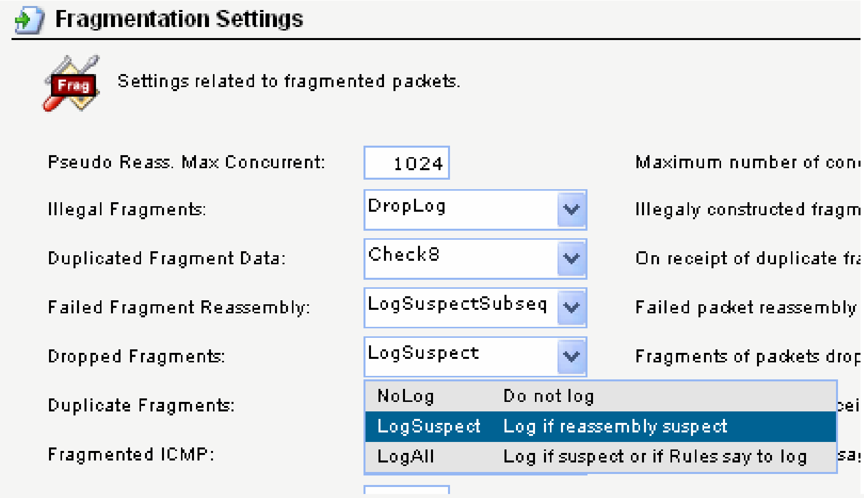
Dropped Fragments:

Duplicate Fragments:

Fragmented ICMP:

Minimum Fragment Length: 8 Minimum allowed length of

NoLog	Do not log
LogSuspect	Log "suspect" failures; affected by illegal frags
LogSuspectSubseq	Log "suspect" failures and all subsequent frags
LogAll	Log normal failures

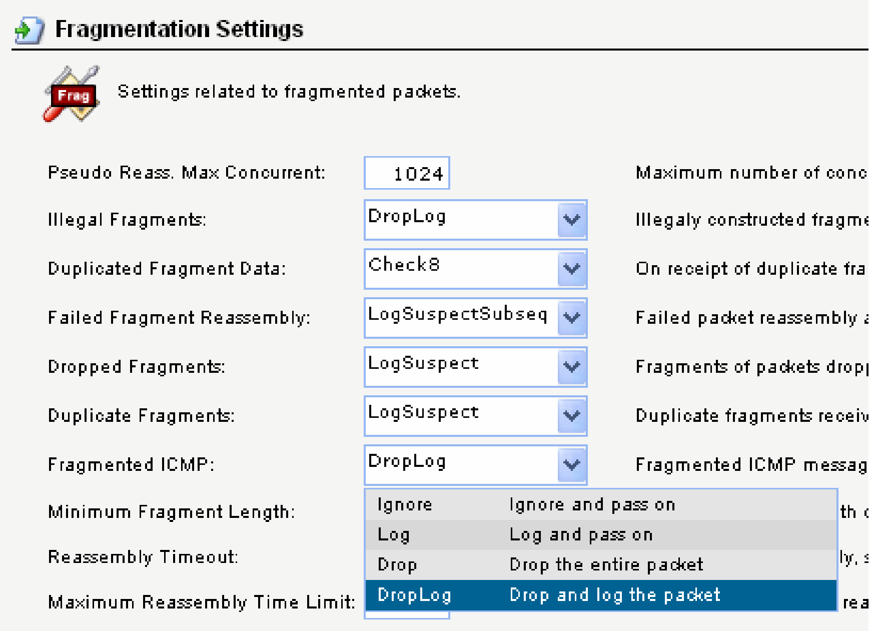


Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent:	1024	Maximum number of con
Illegal Fragments:	DropLog	Illegaly constructed fragm
Duplicated Fragment Data:	Check8	On receipt of duplicate fra
Failed Fragment Reassembly:	LogSuspectSubseq	Failed packet reassembly
Dropped Fragments:	LogSuspect	Fragments of packets drop
Duplicate Fragments:		cei
Fragmented ICMP:		sa

NoLog	Do not log
LogSuspect	Log if reassembly suspect
LogAll	Log if suspect or if Rules say to log

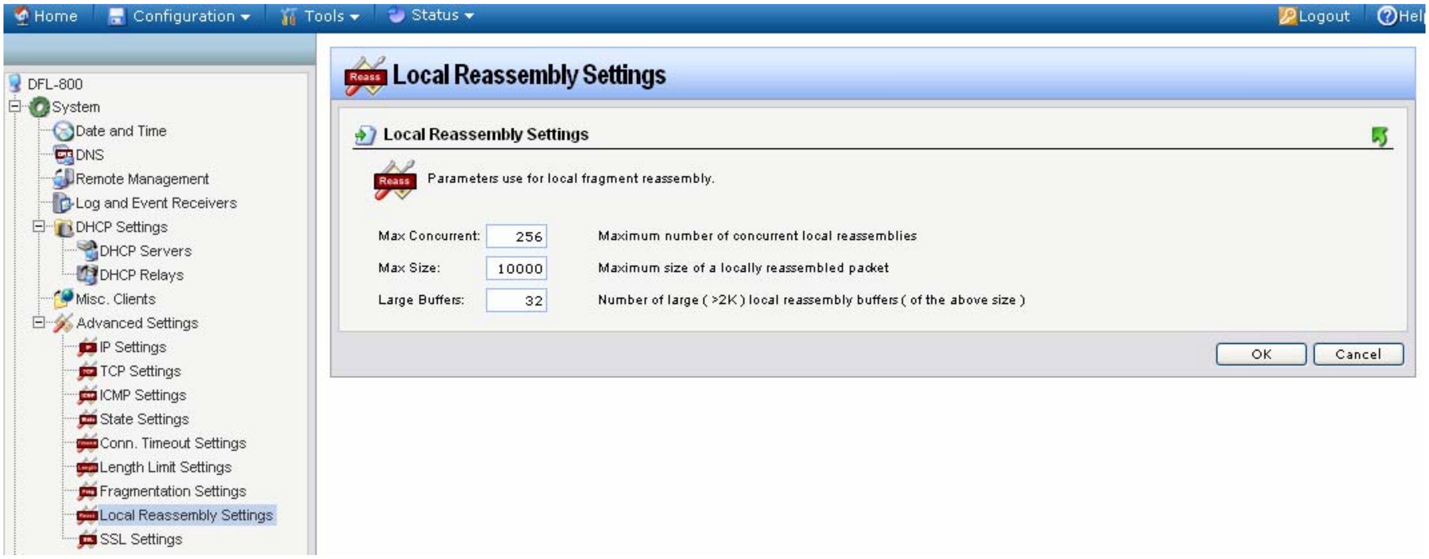


Fragmentation Settings

Settings related to fragmented packets.

Pseudo Reass. Max Concurrent:	1024	Maximum number of conc
Illegal Fragments:	DropLog	Illegaly constructed fragme
Duplicated Fragment Data:	Check8	On receipt of duplicate fra
Failed Fragment Reassembly:	LogSuspectSubseq	Failed packet reassembly a
Dropped Fragments:	LogSuspect	Fragments of packets drop
Duplicate Fragments:	LogSuspect	Duplicate fragments receiv
Fragmented ICMP:	DropLog	Fragmented ICMP messag
Minimum Fragment Length:		th
Reassembly Timeout:		ly,
Maximum Reassembly Time Limit:		rea

Ignore	Ignore and pass on
Log	Log and pass on
Drop	Drop the entire packet
DropLog	Drop and log the packet

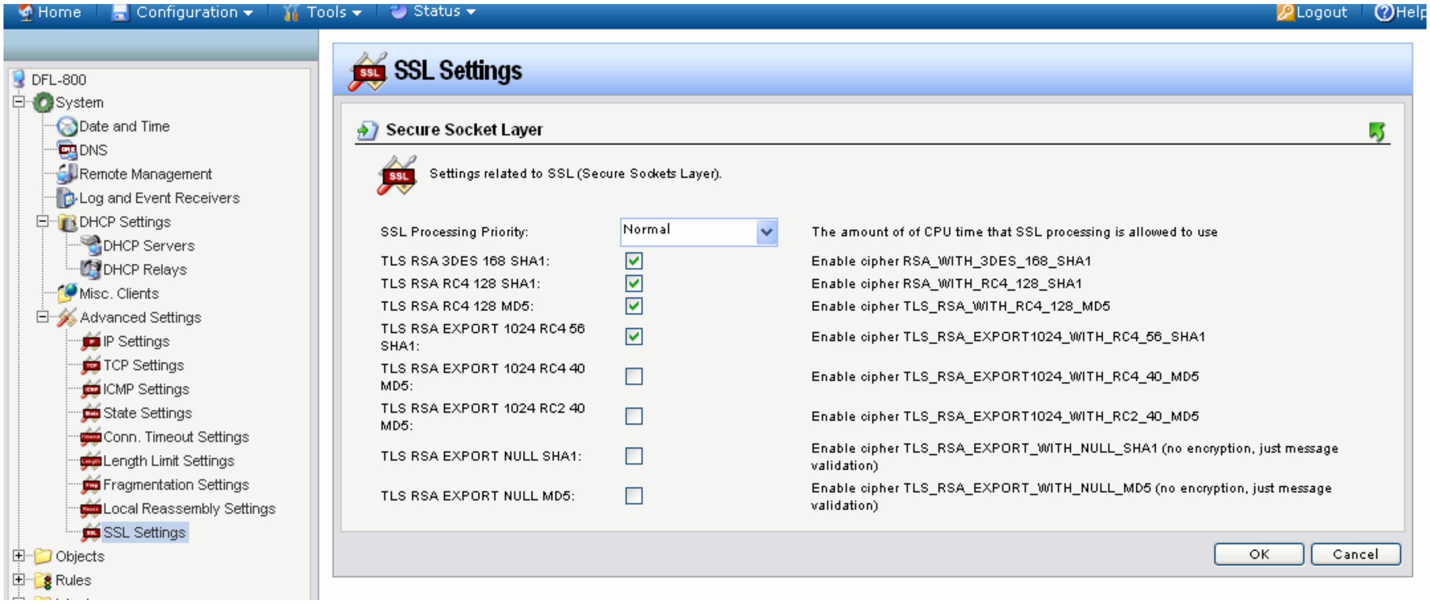


Local Reassembly Settings

Local Reassembly Settings

Parameters use for local fragment reassembly.

Max Concurrent:	256	Maximum number of concurrent local reassemblies
Max Size:	10000	Maximum size of a locally reassembled packet
Large Buffers:	32	Number of large (>2K) local reassembly buffers (of the above size)

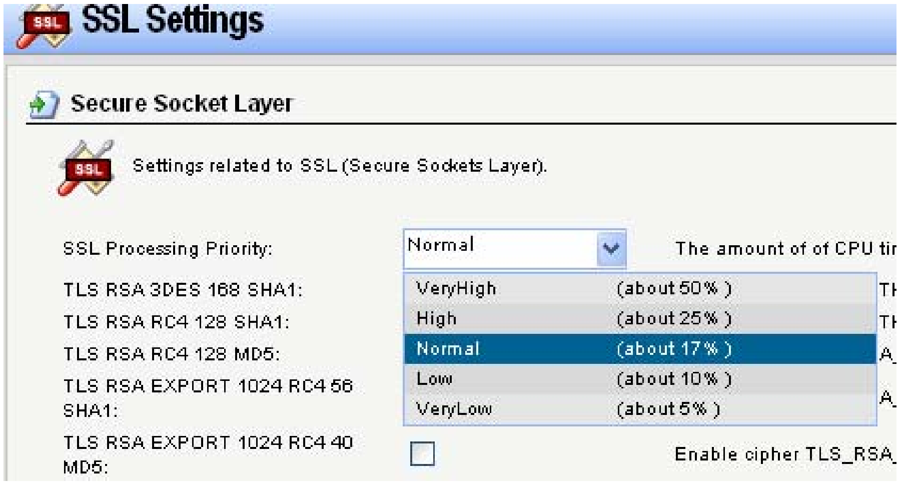


SSL Settings

Secure Socket Layer

Settings related to SSL (Secure Sockets Layer).

SSL Processing Priority:	Normal	The amount of of CPU time that SSL processing is allowed to use
TLS RSA 3DES 168 SHA1:	☑	Enable cipher RSA_WITH_3DES_168_SHA1
TLS RSA RC4 128 SHA1:	☑	Enable cipher RSA_WITH_RC4_128_SHA1
TLS RSA RC4 128 MD5:	☑	Enable cipher TLS_RSA_WITH_RC4_128_MD5
TLS RSA EXPORT 1024 RC4 56 SHA1:	☑	Enable cipher TLS_RSA_EXPORT1024_WITH_RC4_56_SHA1
TLS RSA EXPORT 1024 RC4 40 MD5:	□	Enable cipher TLS_RSA_EXPORT1024_WITH_RC4_40_MD5
TLS RSA EXPORT 1024 RC2 40 MD5:	□	Enable cipher TLS_RSA_EXPORT1024_WITH_RC2_40_MD5
TLS RSA EXPORT NULL SHA1:	□	Enable cipher TLS_RSA_EXPORT_WITH_NULL_SHA1 (no encryption, just message validation)
TLS RSA EXPORT NULL MD5:	□	Enable cipher TLS_RSA_EXPORT_WITH_NULL_MD5 (no encryption, just message validation)



SSL Settings

Secure Socket Layer

Settings related to SSL (Secure Sockets Layer).

SSL Processing Priority: Normal The amount of of CPU tir

TLS RSA 3DES 168 SHA1: Tl

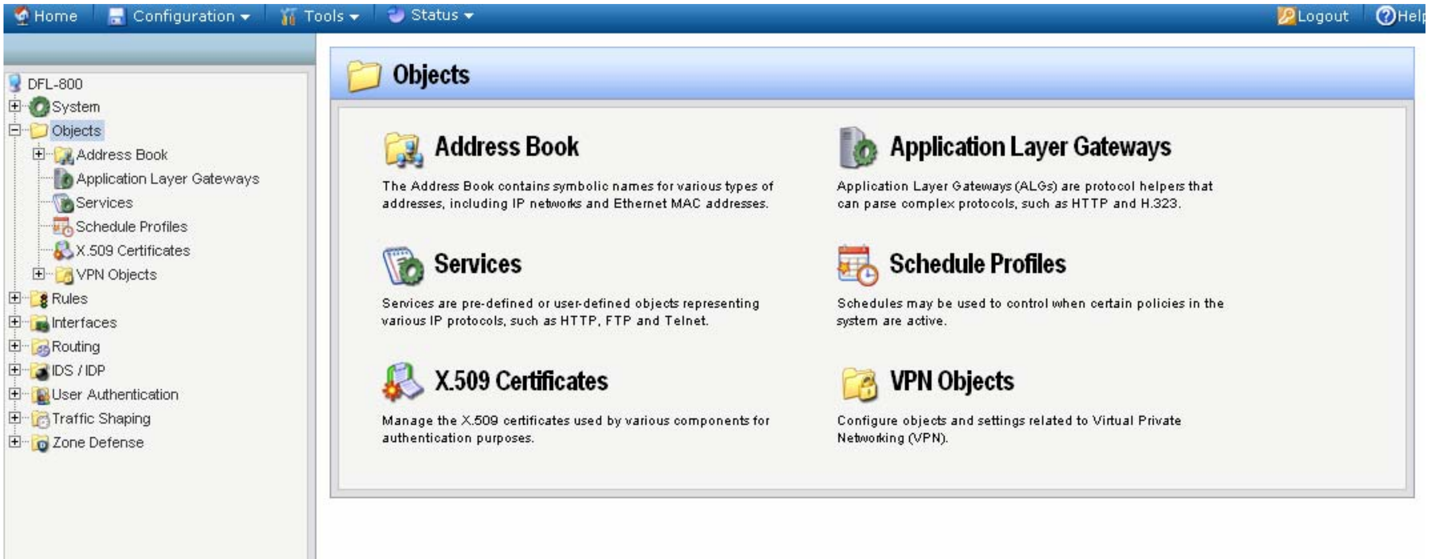
TLS RSA RC4 128 SHA1: Tl

TLS RSA RC4 128 MD5: A

TLS RSA EXPORT 1024 RC4 56 SHA1: A

TLS RSA EXPORT 1024 RC4 40 MD5: □ Enable cipher TLS_RSA_

VeryHigh	(about 50%)
High	(about 25%)
Normal	(about 17%)
Low	(about 10%)
VeryLow	(about 5%)



Objects

Address Book

The Address Book contains symbolic names for various types of addresses, including IP networks and Ethernet MAC addresses.

Application Layer Gateways

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

Services

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

Schedule Profiles

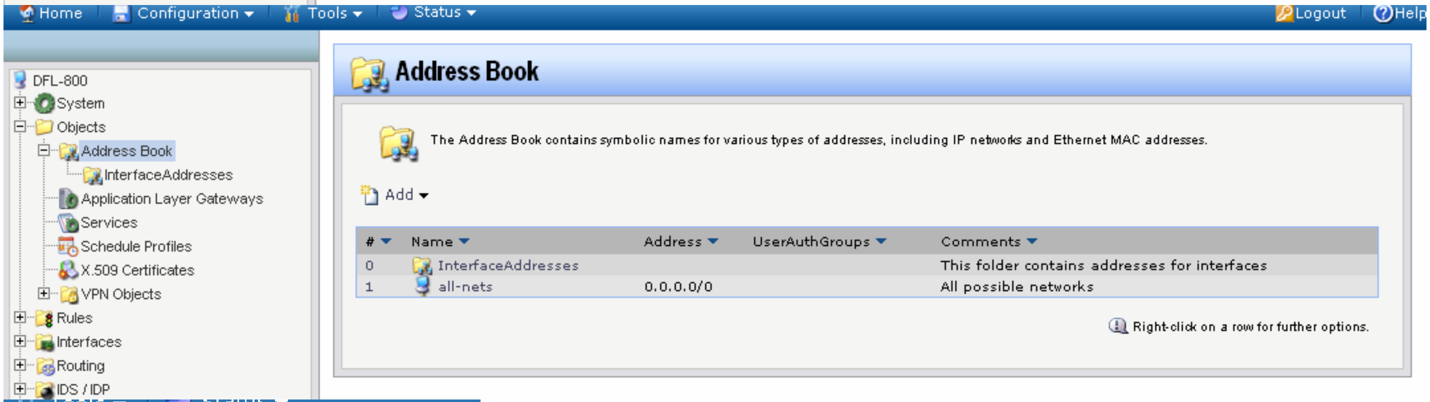
Schedules may be used to control when certain policies in the system are active.

X.509 Certificates

Manage the X.509 certificates used by various components for authentication purposes.

VPN Objects

Configure objects and settings related to Virtual Private Networking (VPN).

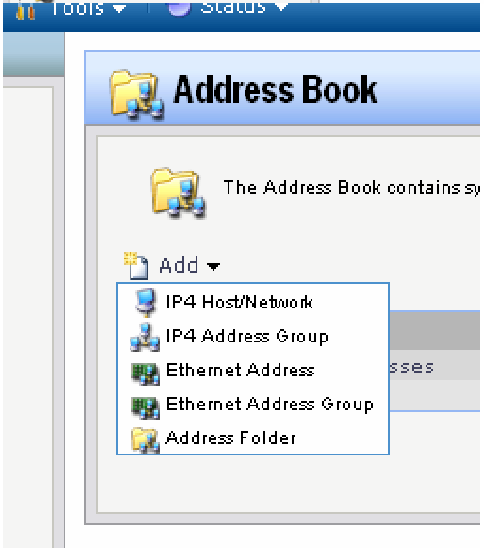


Address Book

The Address Book contains symbolic names for various types of addresses, including IP networks and Ethernet MAC addresses.

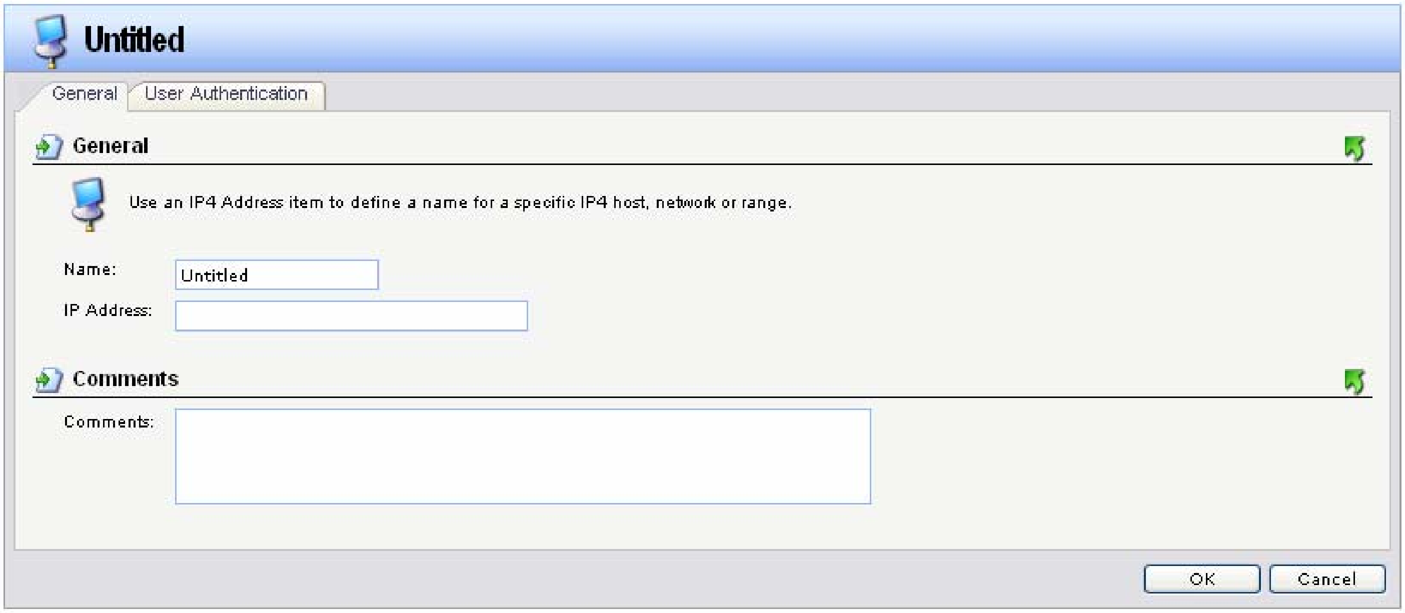
#	Name	Address	UserAuthGroups	Comments
0	InterfaceAddresses			This folder contains addresses for interfaces
1	all-nets	0.0.0.0/0		All possible networks

Right-click on a row for further options.



Address Book

The Address Book contains sy



Untitled

General

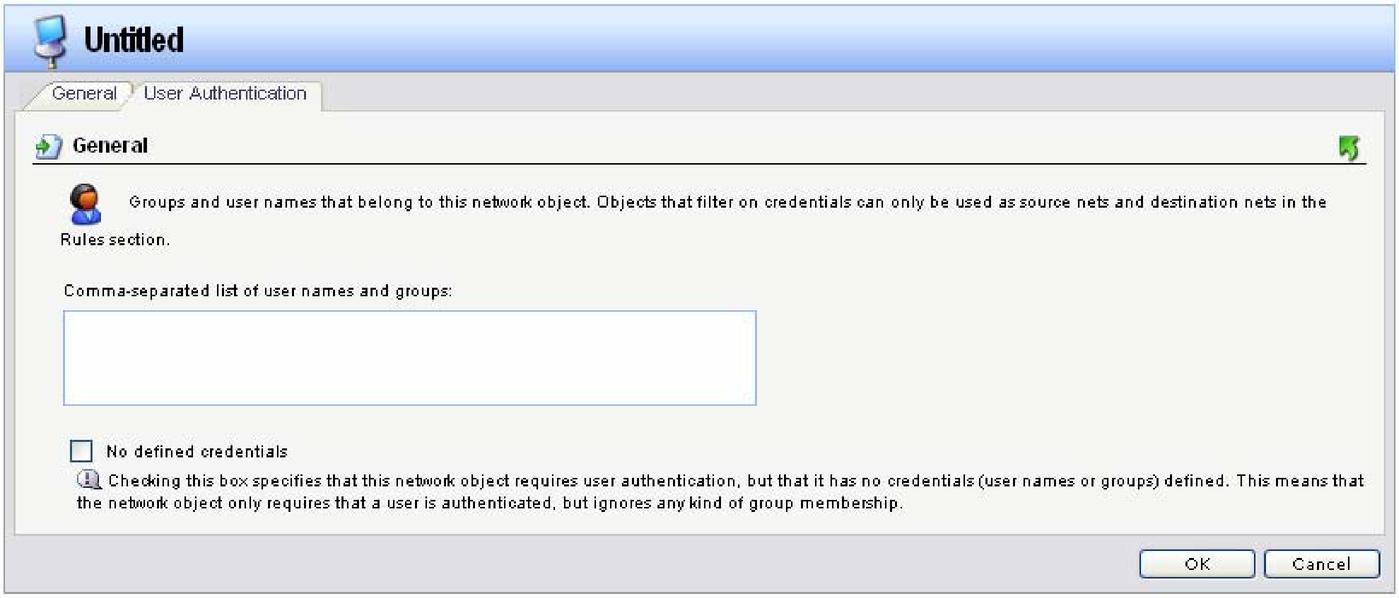
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: Untitled

IP Address:

Comments

Comments:



Untitled

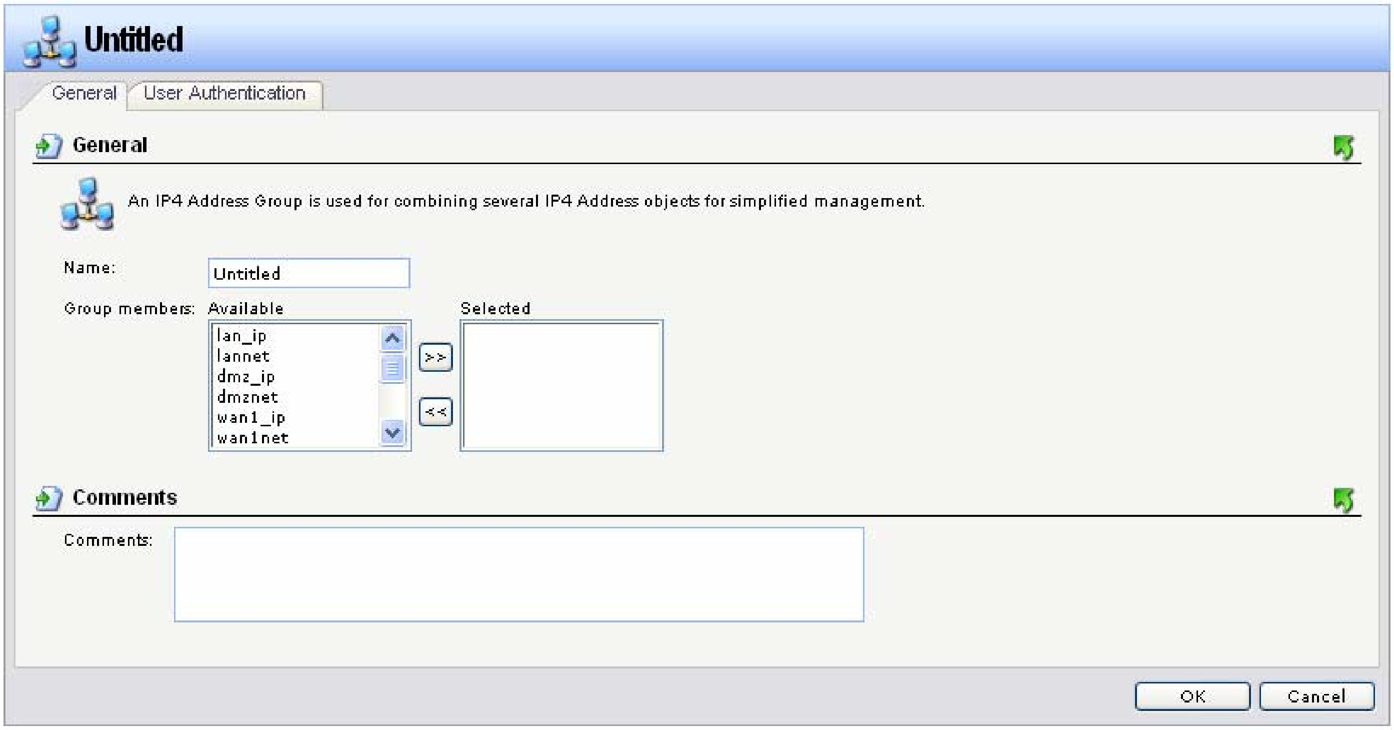
General

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:

□ 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.



Untitled

General

An IP4 Address Group is used for combining several IP4 Address objects for simplified management.

Name: Untitled

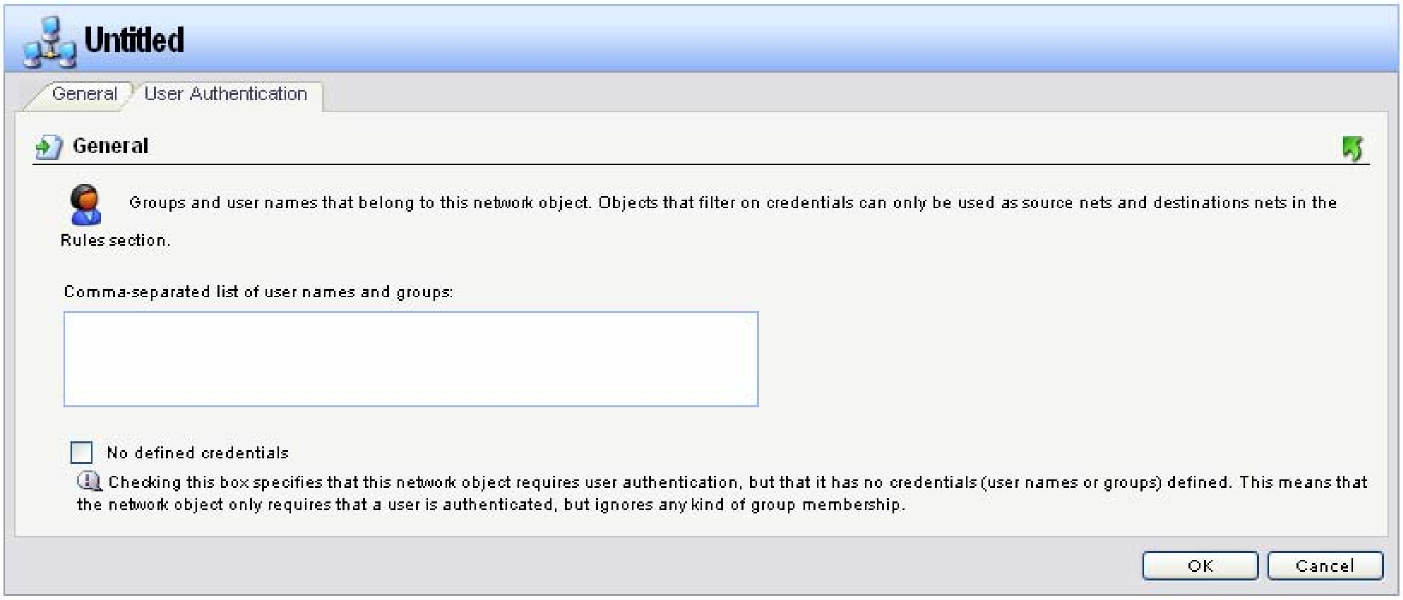
Group members: Available

lan_ip
lannet
dmz_ip
dmznet
wan1_ip
wan1net

Selected

Comments

Comments:

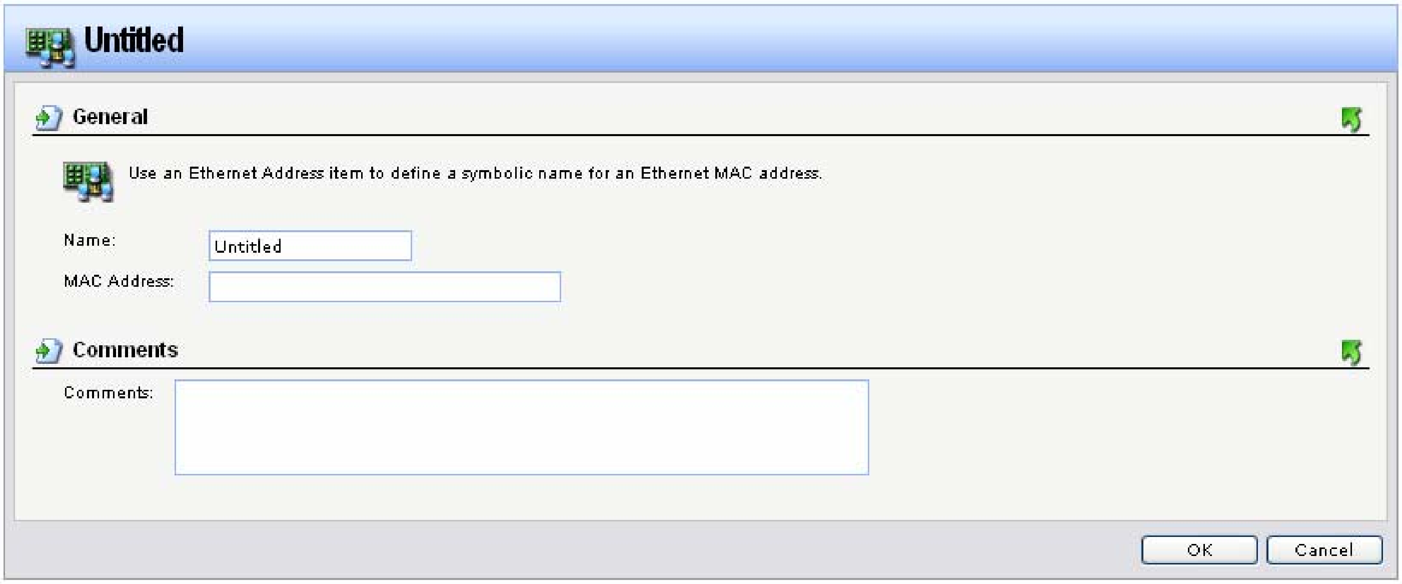


Groups and user names that belong to this network object. Objects that filter on credentials can only be used as source nets and destinations nets in the Rules section.

Comma-separated list of user names and groups:

□ No defined credentials

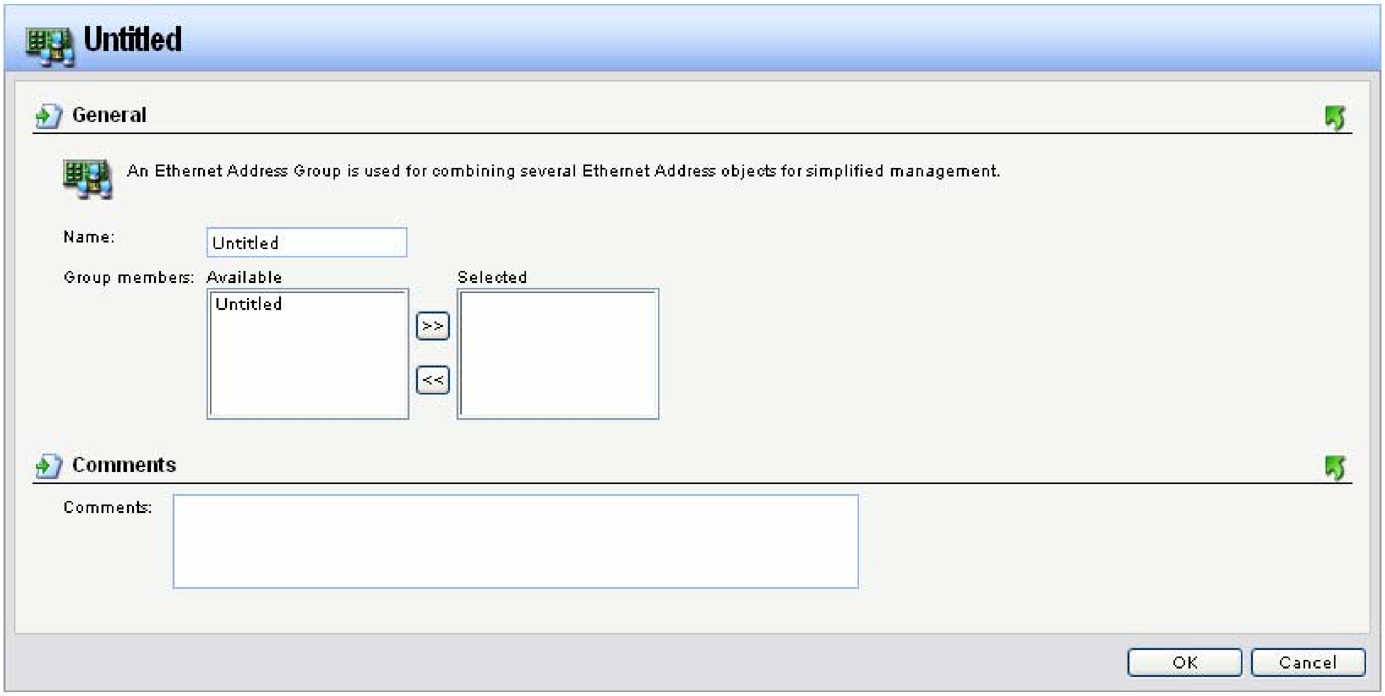
Checking this box specifies that this network object requires user authentication, but that it has no credentials (user names or groups) defined. This means that the network object only requires that a user is authenticated, but ignores any kind of group membership.



Use an Ethernet Address item to define a symbolic name for an Ethernet MAC address.

Name: Untitled

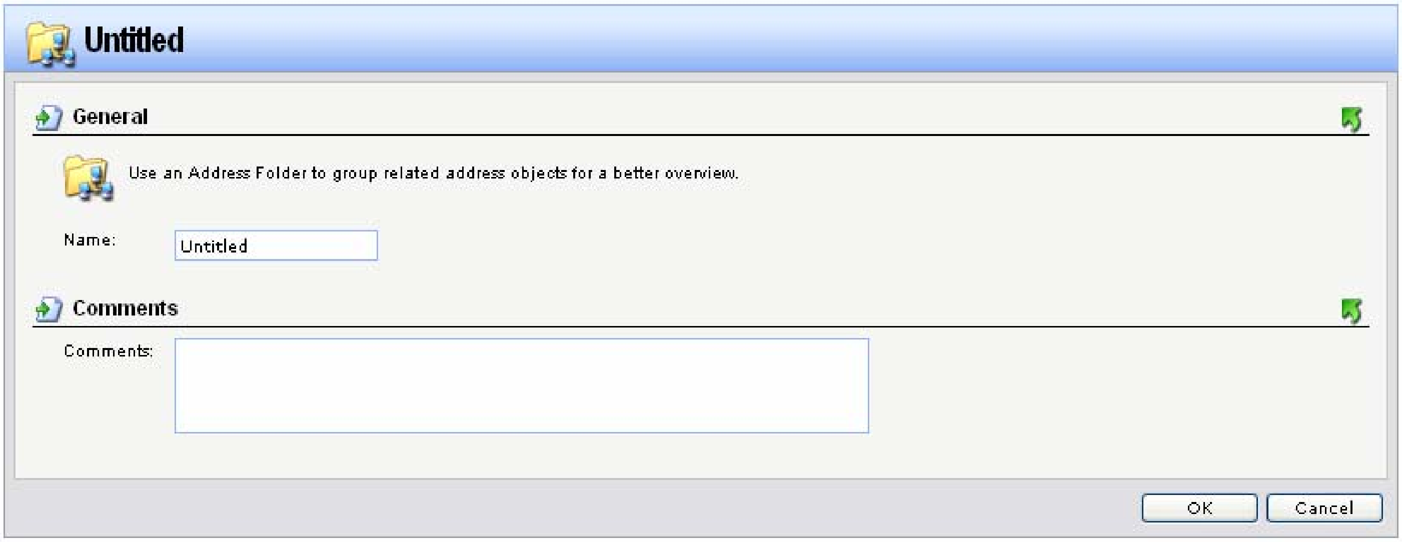
MAC Address:



An Ethernet Address Group is used for combining several Ethernet Address objects for simplified management.

Name: Untitled

Group members: Available: Untitled; Selected:



Untitled

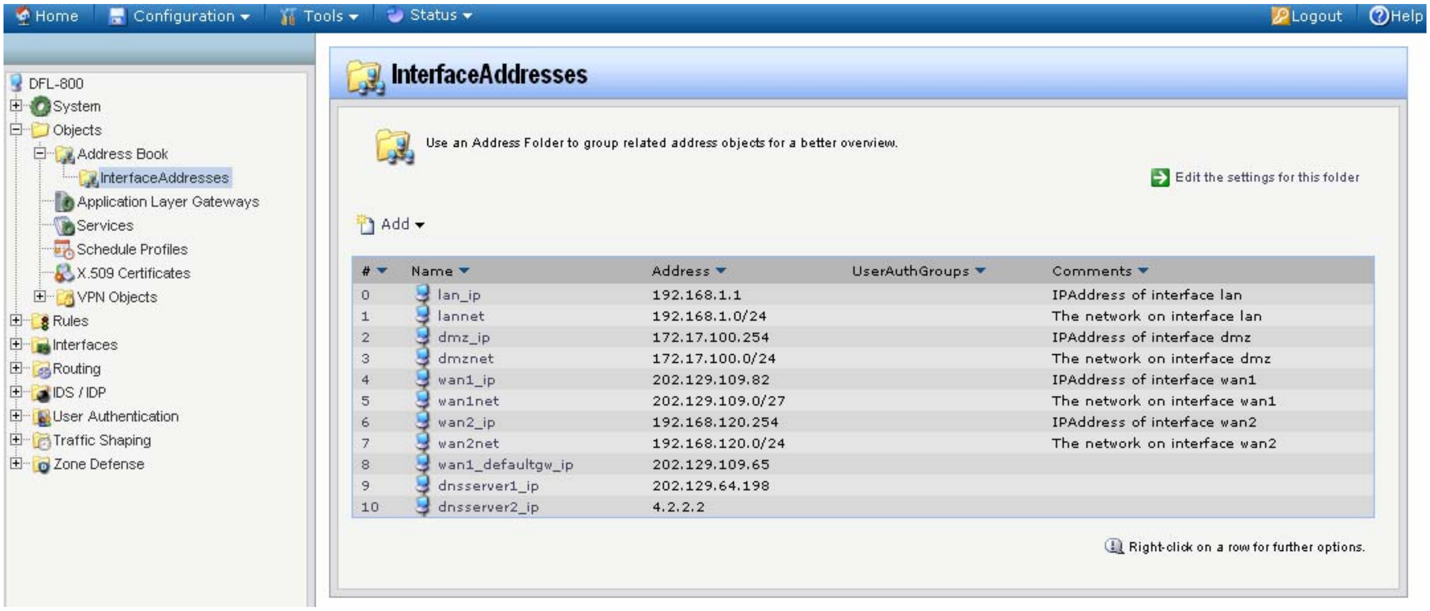
General

Use an Address Folder to group related address objects for a better overview.

Name: Untitled

Comments

Comments:



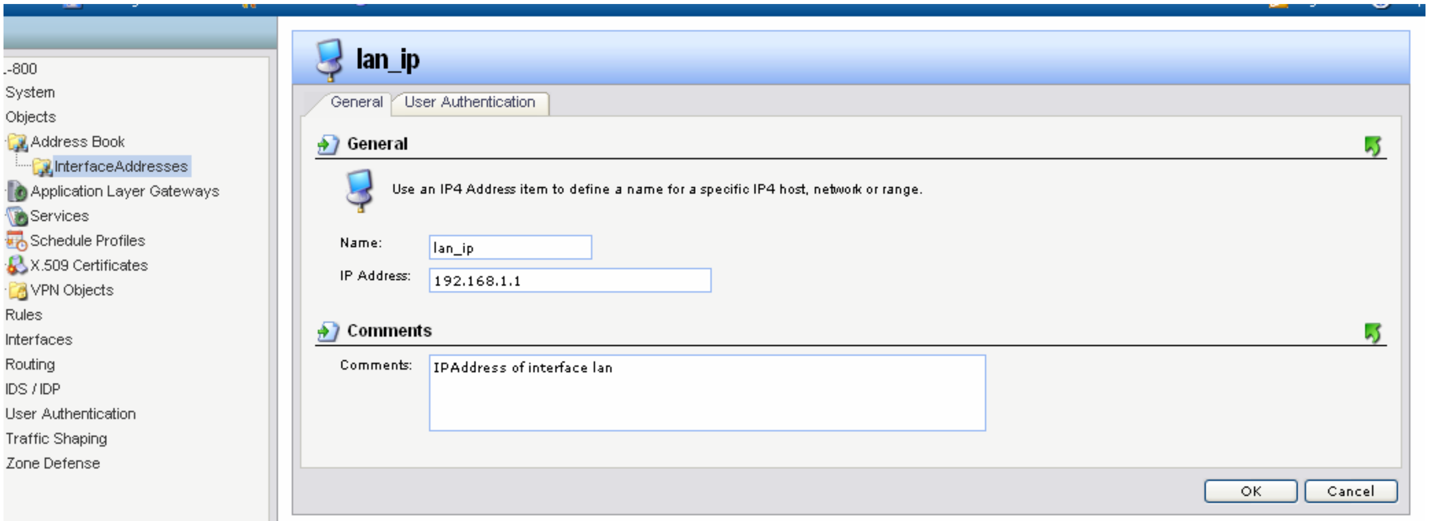
InterfaceAddresses

Use an Address Folder to group related address objects for a better overview.

Edit the settings for this folder

#	Name	Address	UserAuthGroups	Comments
0	lan_ip	192.168.1.1		IPAddress of interface lan
1	lannet	192.168.1.0/24		The network on interface lan
2	dmz_ip	172.17.100.254		IPAddress of interface dmz
3	dmznet	172.17.100.0/24		The network on interface dmz
4	wan1_ip	202.129.109.82		IPAddress of interface wan1
5	wan1net	202.129.109.0/27		The network on interface wan1
6	wan2_ip	192.168.120.254		IPAddress of interface wan2
7	wan2net	192.168.120.0/24		The network on interface wan2
8	wan1_defaultgw_ip	202.129.109.65		
9	dnsserver1_ip	202.129.64.198		
10	dnsserver2_ip	4.2.2.2		

Right-click on a row for further options.



lan_ip

General

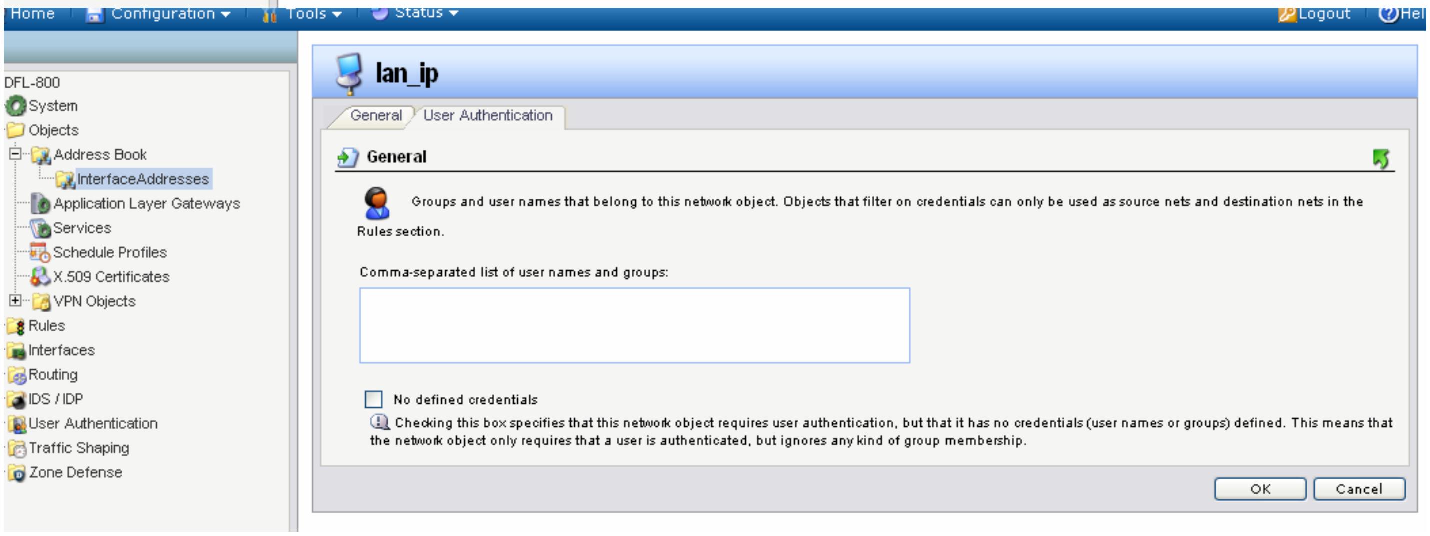
Use an IP4 Address item to define a name for a specific IP4 host, network or range.

Name: lan_ip

IP Address: 192.168.1.1

Comments

Comments: IPAddress of interface lan



lan_ip

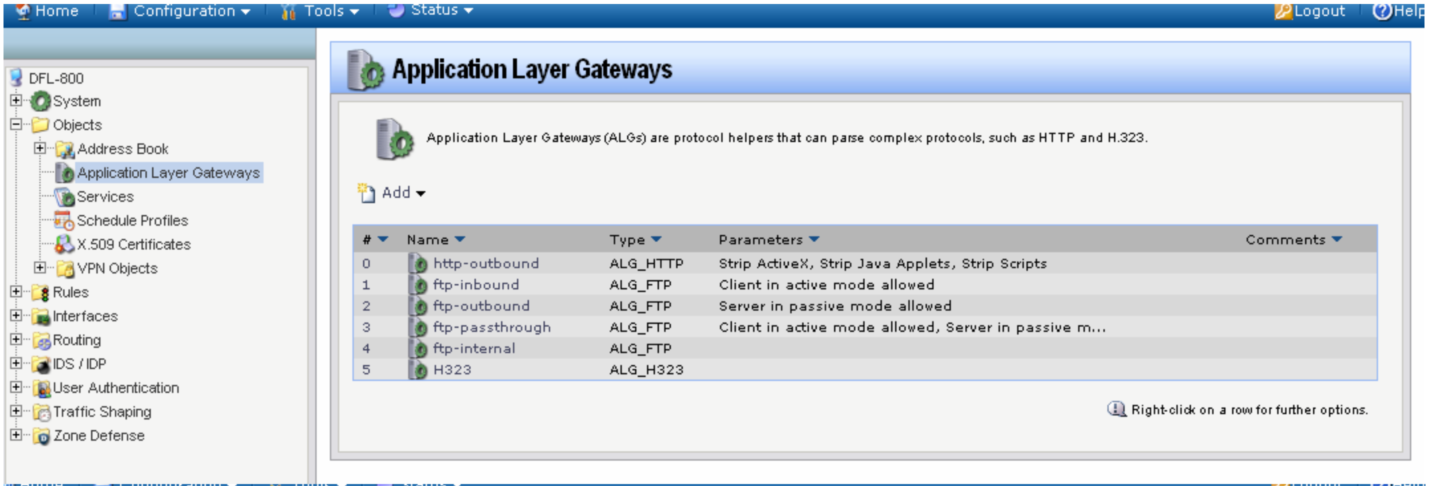
General

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:

☐ 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.

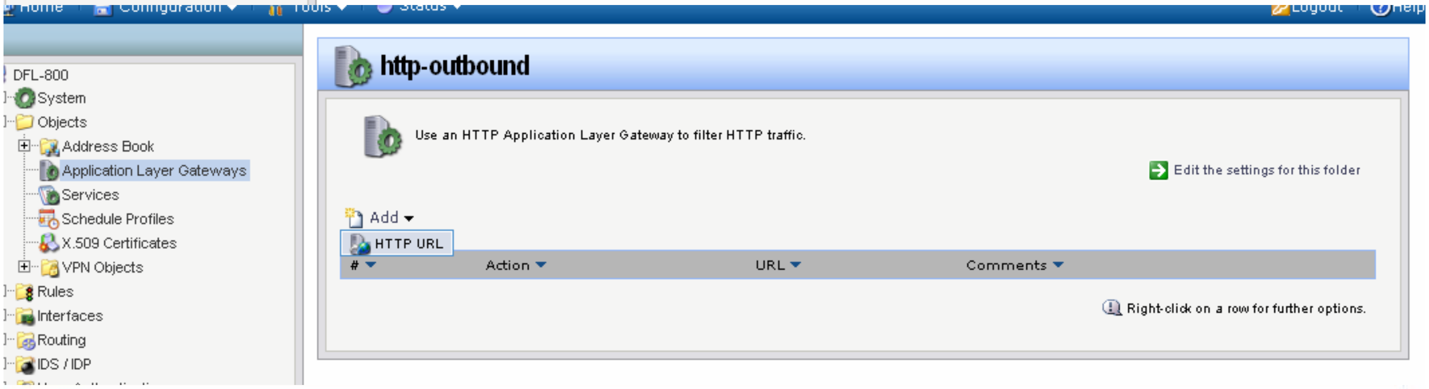


Application Layer Gateways

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

#	Name	Type	Parameters	Comments
0	http-outbound	ALG_HTTP	Strip ActiveX, Strip Java Applets, Strip Scripts	
1	ftp-inbound	ALG_FTP	Client in active mode allowed	
2	ftp-outbound	ALG_FTP	Server in passive mode allowed	
3	ftp-passthrough	ALG_FTP	Client in active mode allowed, Server in passive m...	
4	ftp-internal	ALG_FTP		
5	H323	ALG_H323		

Right-click on a row for further options.



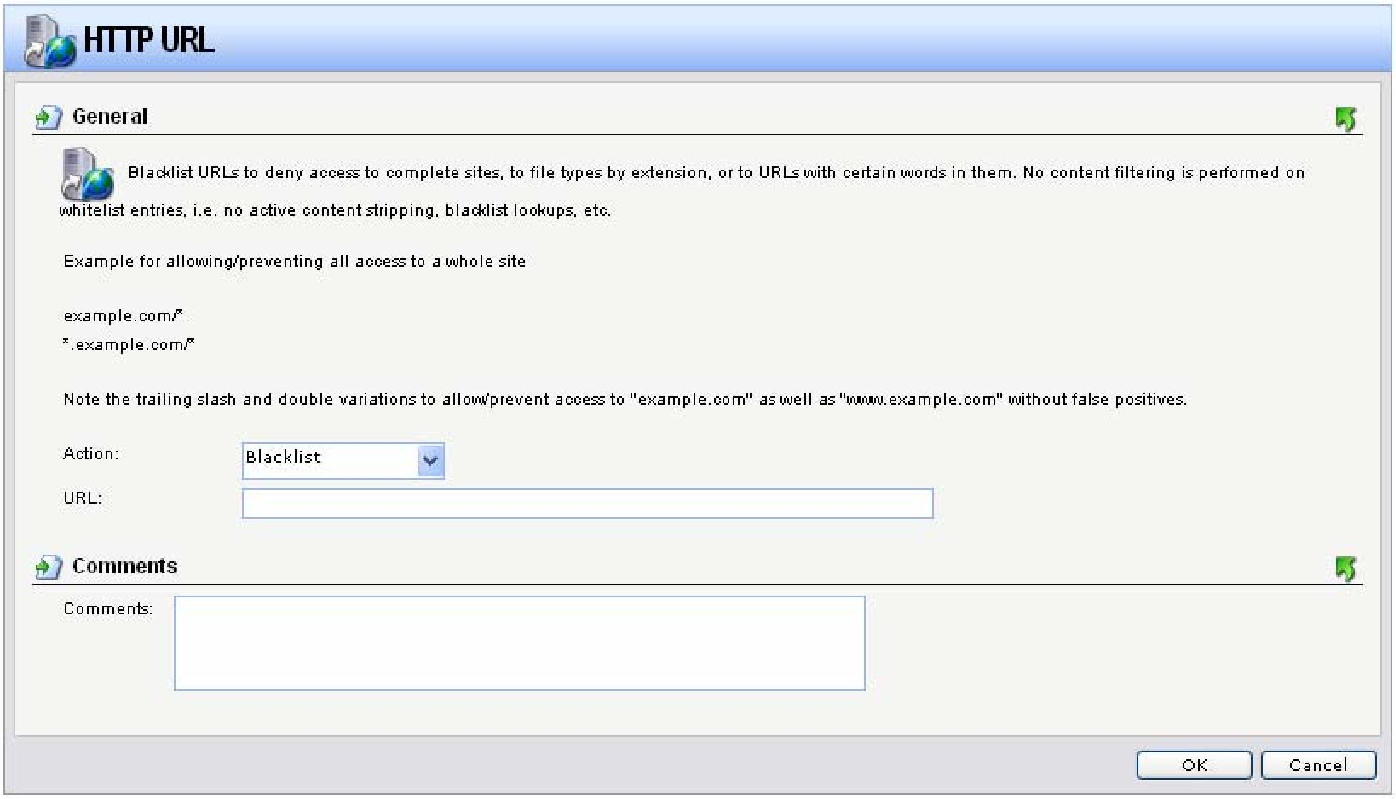
http-outbound

Use an HTTP Application Layer Gateway to filter HTTP traffic.

Edit the settings for this folder

#	Action	URL	Comments

Right-click on a row for further options.



HTTP URL

General

Blacklist URLs to deny access to complete sites, to file types by extension, or to URLs with certain words in them. No content filtering is performed on whitelist entries, i.e. no active content stripping, blacklist lookups, etc.

Example for allowing/preventing all access to a whole site

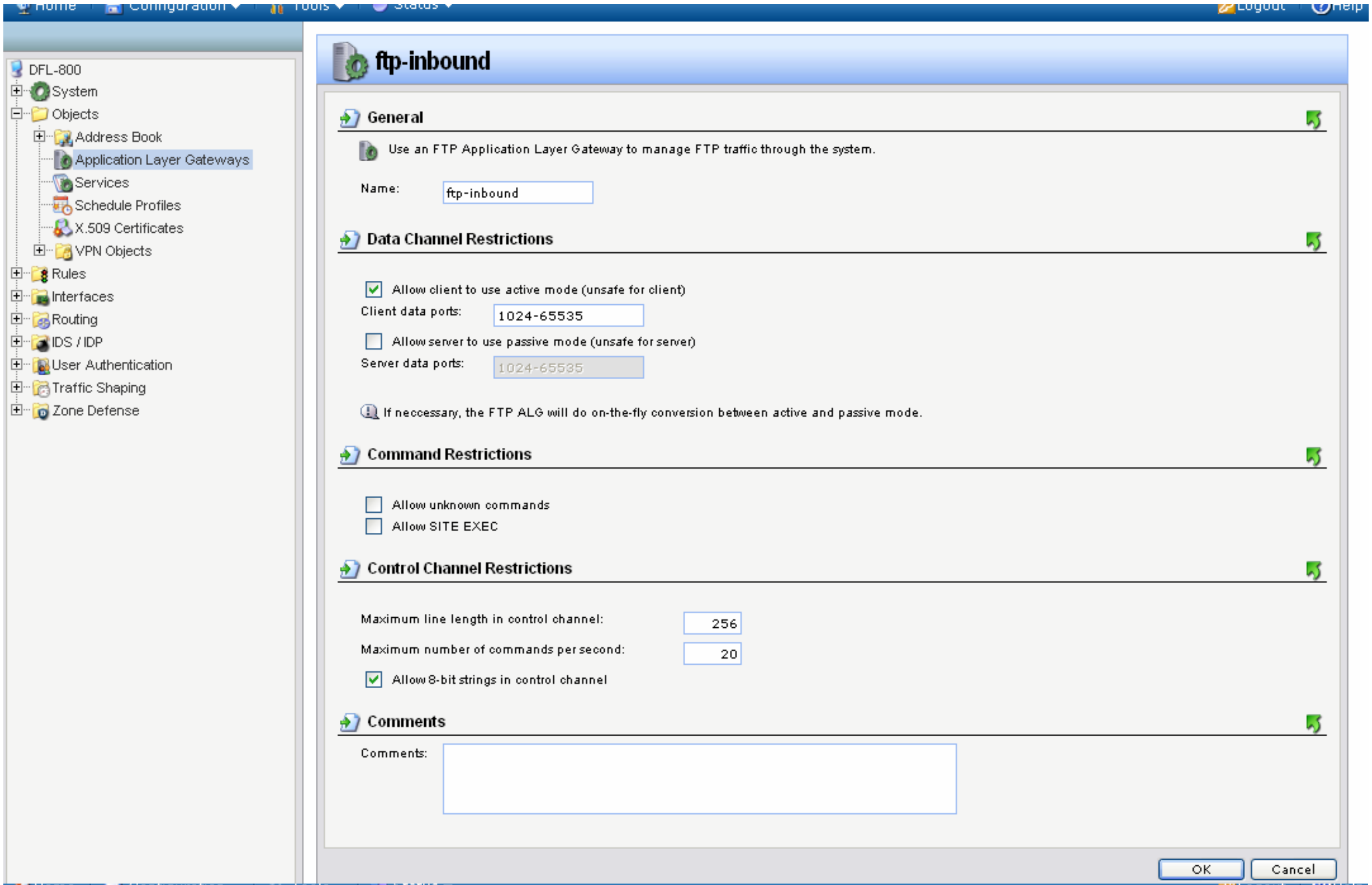
example.com/*
.example.com/

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

Comments:



ftp-inbound

General

Use an FTP Application Layer Gateway to manage FTP traffic through the system.

Name: ftp-inbound

Data Channel Restrictions

☑ Allow client to use active mode (unsafe for client)

Client data ports: 1024-65535

☐ Allow server to use passive mode (unsafe for server)

Server data ports: 1024-65535

If necessary, the FTP ALG will do on-the-fly conversion between active and passive mode.

Command Restrictions

☐ Allow unknown commands

☐ Allow SITE EXEC

Control Channel Restrictions

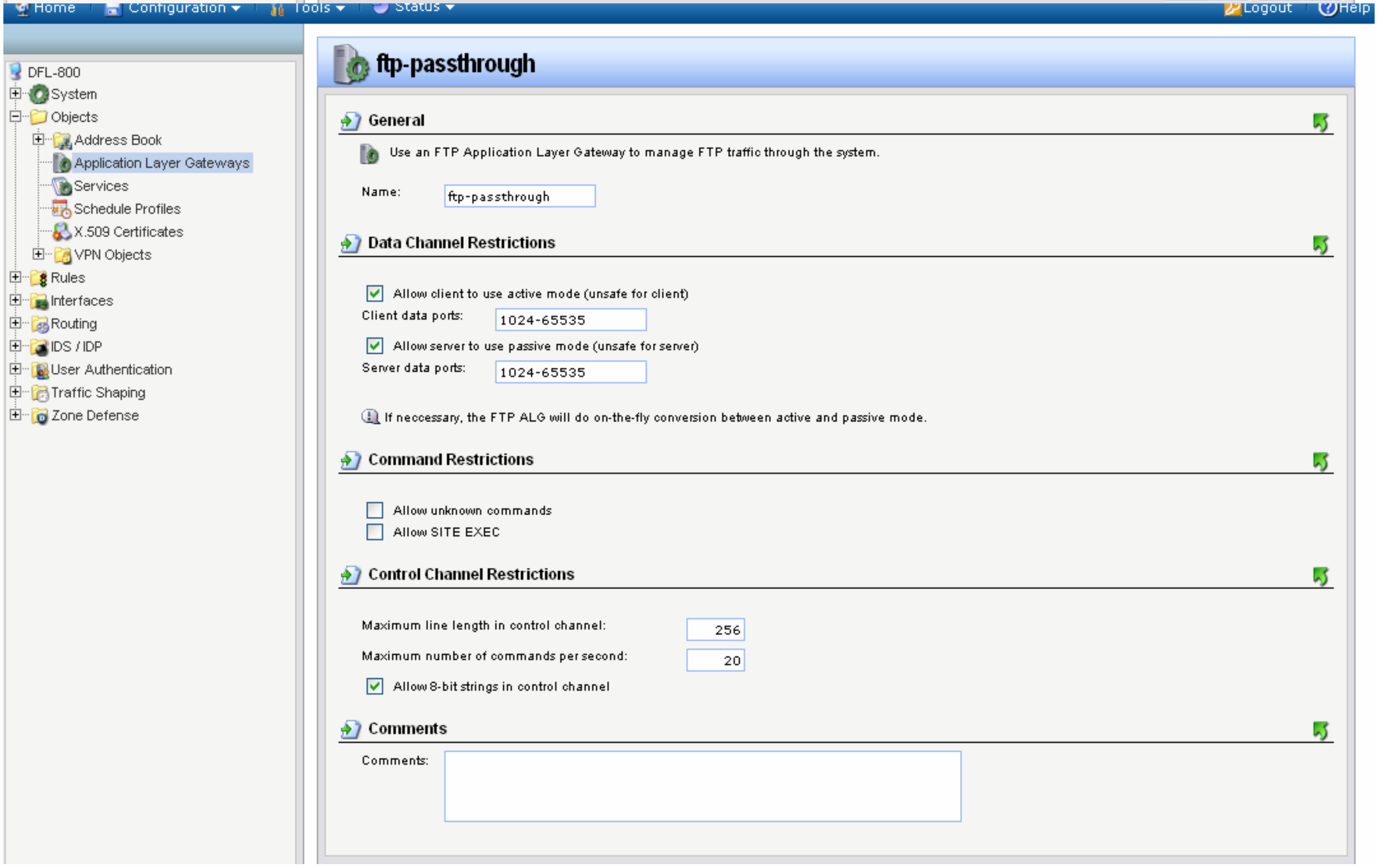
Maximum line length in control channel: 256

Maximum number of commands per second: 20

☑ Allow 8-bit strings in control channel

Comments

Comments:



ftp-passthrough

General

Use an FTP Application Layer Gateway to manage FTP traffic through the system.

Name: ftp-passthrough

Data Channel Restrictions

☑ Allow client to use active mode (unsafe for client)

Client data ports: 1024-65535

☑ Allow server to use passive mode (unsafe for server)

Server data ports: 1024-65535

If necessary, the FTP ALG will do on-the-fly conversion between active and passive mode.

Command Restrictions

☐ Allow unknown commands

☐ Allow SITE EXEC

Control Channel Restrictions

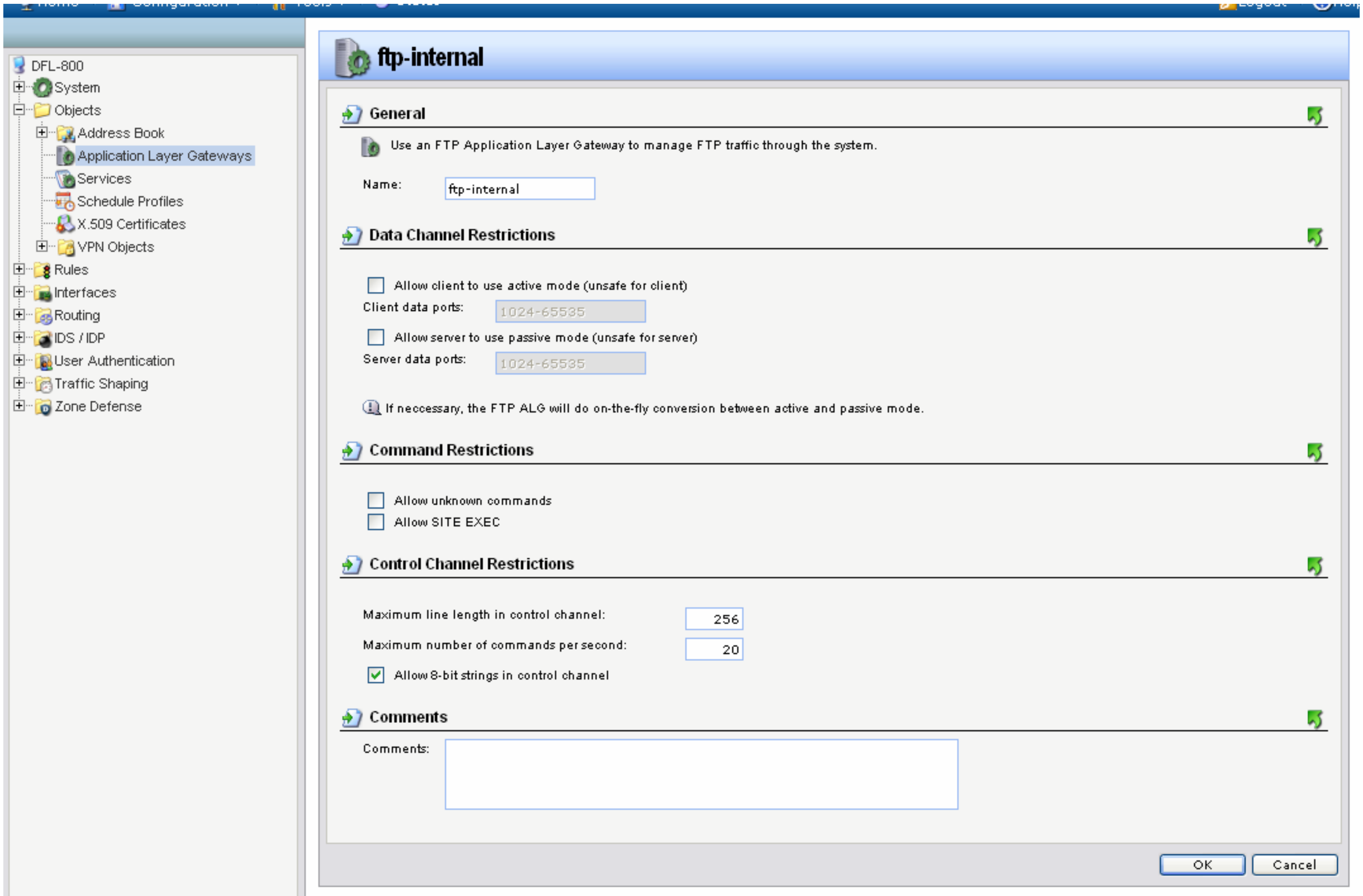
Maximum line length in control channel: 256

Maximum number of commands per second: 20

☑ Allow 8-bit strings in control channel

Comments

Comments:



ftp-internal

General

Use an FTP Application Layer Gateway to manage FTP traffic through the system.

Name: ftp-internal

Data Channel Restrictions

☐ Allow client to use active mode (unsafe for client)

Client data ports: 1024-65535

☐ Allow server to use passive mode (unsafe for server)

Server data ports: 1024-65535

If necessary, the FTP ALG will do on-the-fly conversion between active and passive mode.

Command Restrictions

☐ Allow unknown commands

☐ Allow SITE EXEC

Control Channel Restrictions

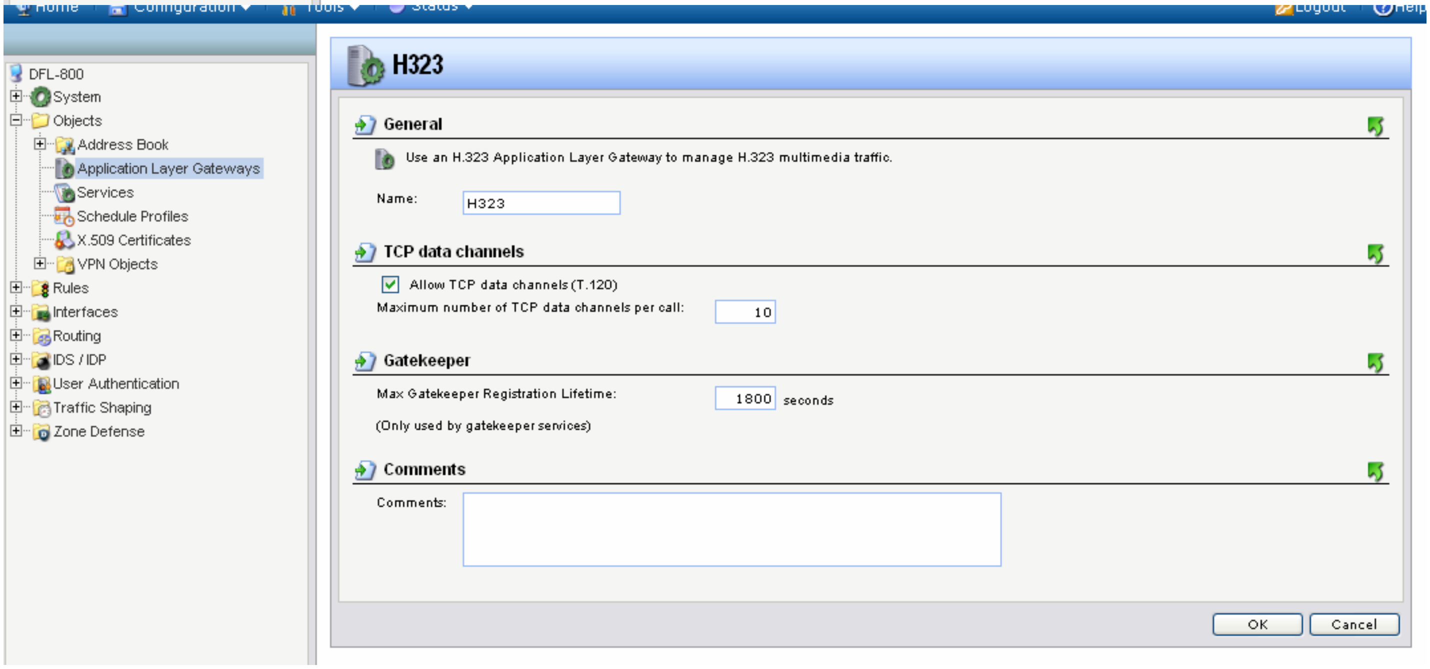
Maximum line length in control channel: 256

Maximum number of commands per second: 20

☑ Allow 8-bit strings in control channel

Comments

Comments:



H323

General

Use an H.323 Application Layer Gateway to manage H.323 multimedia traffic.

Name: H323

TCP data channels

☑ Allow TCP data channels (T.120)

Maximum number of TCP data channels per call: 10

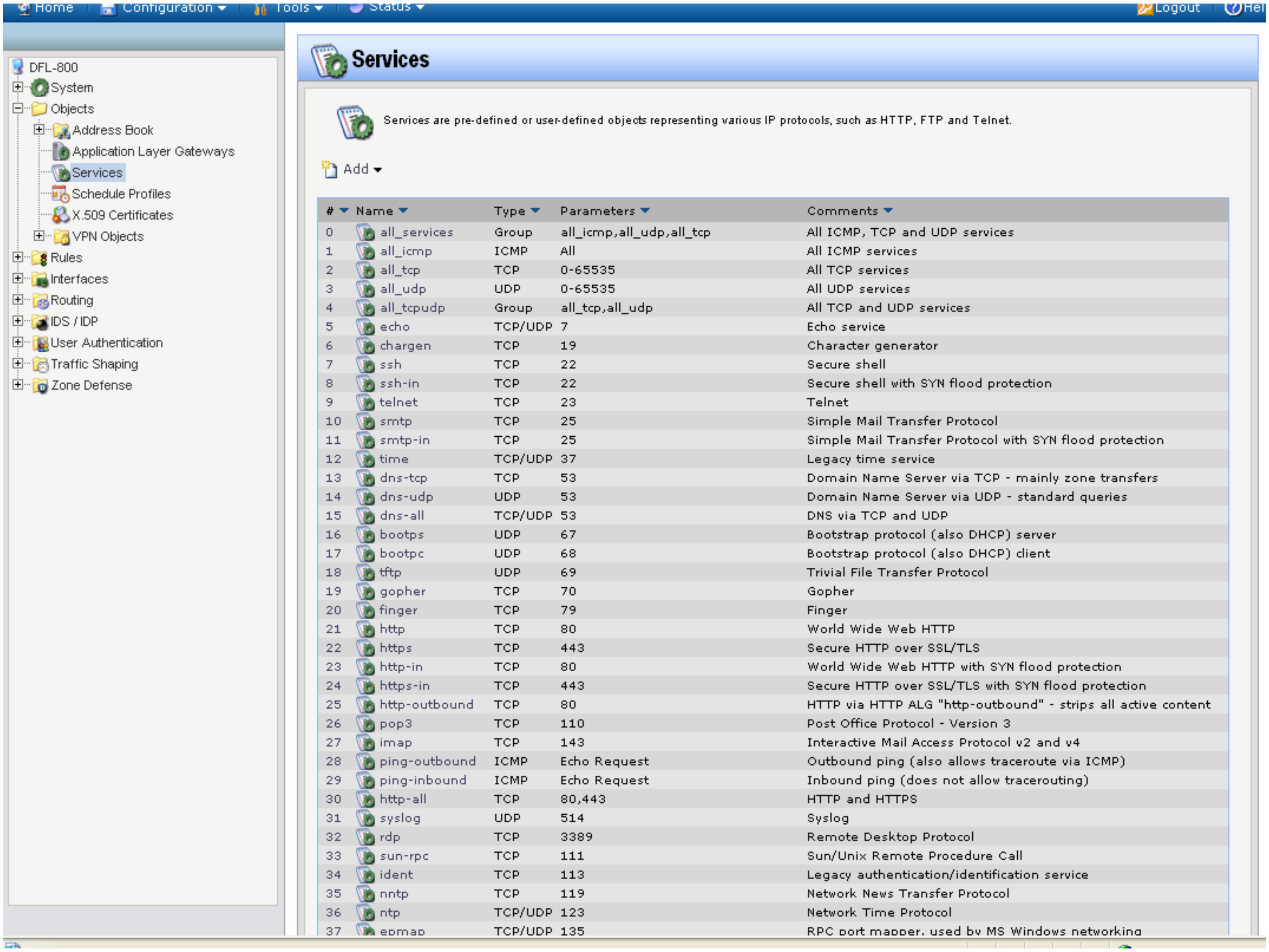
Gatekeeper

Max Gatekeeper Registration Lifetime: 1800 seconds

(Only used by gatekeeper services)

Comments

Comments:

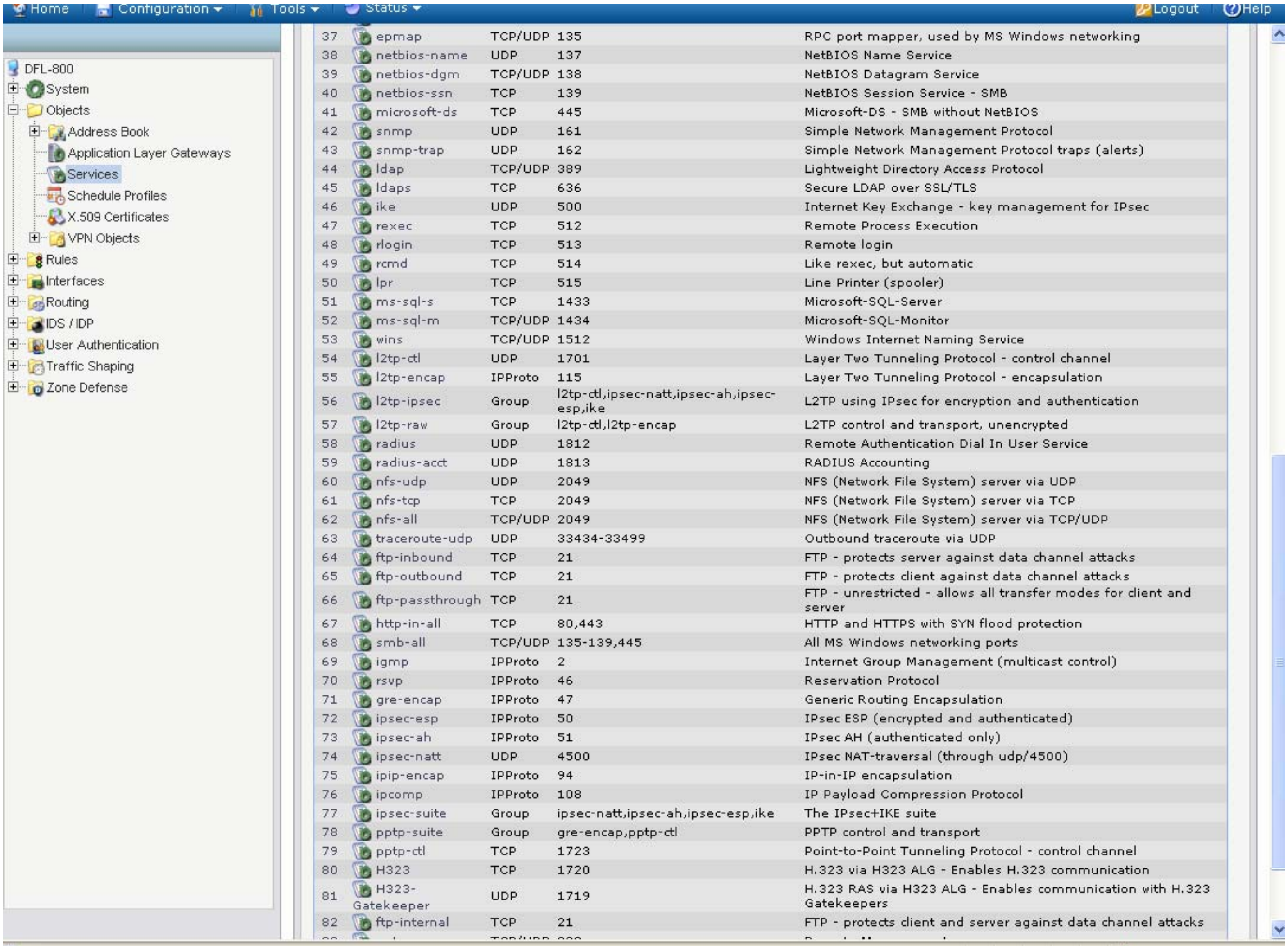


Services

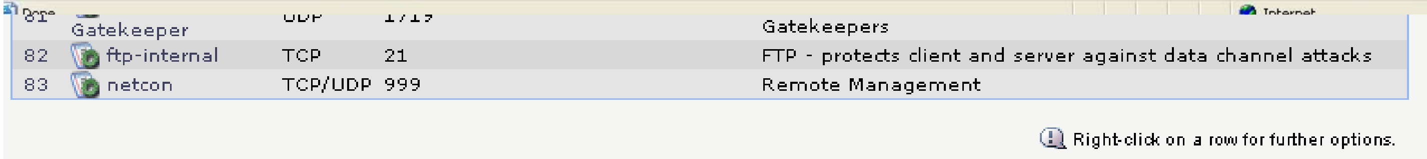
Services are pre-defined or user-defined objects representing various IP protocols, such as HTTP, FTP and Telnet.

Add

#	Name	Type	Parameters	Comments
0	all_services	Group	all_icmp,all_udp,all_tcp	All ICMP, TCP and UDP services
1	all_icmp	ICMP	All	All ICMP services
2	all_tcp	TCP	0-65535	All TCP services
3	all_udp	UDP	0-65535	All UDP services
4	all_tcpudp	Group	all_tcp,all_udp	All TCP and UDP services
5	echo	TCP/UDP	7	Echo service
6	chargen	TCP	19	Character generator
7	ssh	TCP	22	Secure shell
8	ssh-in	TCP	22	Secure shell with SYN flood protection
9	telnet	TCP	23	Telnet
10	smtp	TCP	25	Simple Mail Transfer Protocol
11	smtp-in	TCP	25	Simple Mail Transfer Protocol with SYN flood protection
12	time	TCP/UDP	37	Legacy time service
13	dns-tcp	TCP	53	Domain Name Server via TCP - mainly zone transfers
14	dns-udp	UDP	53	Domain Name Server via UDP - standard queries
15	dns-all	TCP/UDP	53	DNS via TCP and UDP
16	bootps	UDP	67	Bootstrap protocol (also DHCP) server
17	bootpc	UDP	68	Bootstrap protocol (also DHCP) client
18	tftp	UDP	69	Trivial File Transfer Protocol
19	gopher	TCP	70	Gopher
20	finger	TCP	79	Finger
21	http	TCP	80	World Wide Web HTTP
22	https	TCP	443	Secure HTTP over SSL/TLS
23	http-in	TCP	80	World Wide Web HTTP with SYN flood protection
24	https-in	TCP	443	Secure HTTP over SSL/TLS with SYN flood protection
25	http-outbound	TCP	80	HTTP via HTTP ALG "http-outbound" - strips all active content
26	pop3	TCP	110	Post Office Protocol - Version 3
27	imap	TCP	143	Interactive Mail Access Protocol v2 and v4
28	ping-outbound	ICMP	Echo Request	Outbound ping (also allows traceroute via ICMP)
29	ping-inbound	ICMP	Echo Request	Inbound ping (does not allow tracerouting)
30	http-all	TCP	80,443	HTTP and HTTPS
31	syslog	UDP	514	Syslog
32	rdp	TCP	3389	Remote Desktop Protocol
33	sun-rpc	TCP	111	Sun/Unix Remote Procedure Call
34	ident	TCP	113	Legacy authentication/identification service
35	nntp	TCP	119	Network News Transfer Protocol
36	ntp	TCP/UDP	123	Network Time Protocol
37	epmap	TCP/UDP	135	RPC port mapper, used by MS Windows networking

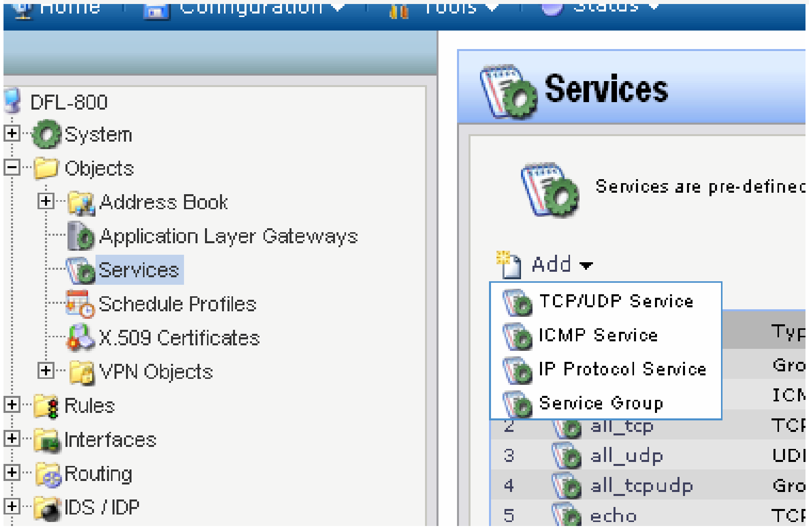


37	epmap	TCP/UDP	135	RPC port mapper, used by MS Windows networking
38	netbios-name	UDP	137	NetBIOS Name Service
39	netbios-dgm	TCP/UDP	138	NetBIOS Datagram Service
40	netbios-ssn	TCP	139	NetBIOS Session Service - SMB
41	microsoft-ds	TCP	445	Microsoft-DS - SMB without NetBIOS
42	snmp	UDP	161	Simple Network Management Protocol
43	snmp-trap	UDP	162	Simple Network Management Protocol traps (alerts)
44	ldap	TCP/UDP	389	Lightweight Directory Access Protocol
45	ldaps	TCP	636	Secure LDAP over SSL/TLS
46	ike	UDP	500	Internet Key Exchange - key management for IPsec
47	rexec	TCP	512	Remote Process Execution
48	rlogin	TCP	513	Remote login
49	rcmd	TCP	514	Like rexec, but automatic
50	lpr	TCP	515	Line Printer (spooler)
51	ms-sql-s	TCP	1433	Microsoft-SQL-Server
52	ms-sql-m	TCP/UDP	1434	Microsoft-SQL-Monitor
53	wins	TCP/UDP	1512	Windows Internet Naming Service
54	l2tp-ctl	UDP	1701	Layer Two Tunneling Protocol - control channel
55	l2tp-encap	IPProto	115	Layer Two Tunneling Protocol - encapsulation
56	l2tp-ipsec	Group	l2tp-ctl,ipsec-natt,ipsec-ah,ipsec-esp,ike	L2TP using IPsec for encryption and authentication
57	l2tp-raw	Group	l2tp-ctl,l2tp-encap	L2TP control and transport, unencrypted
58	radius	UDP	1812	Remote Authentication Dial In User Service
59	radius-acct	UDP	1813	RADIUS Accounting
60	nfs-udp	UDP	2049	NFS (Network File System) server via UDP
61	nfs-tcp	TCP	2049	NFS (Network File System) server via TCP
62	nfs-all	TCP/UDP	2049	NFS (Network File System) server via TCP/UDP
63	traceroute-udp	UDP	33434-33499	Outbound traceroute via UDP
64	ftp-inbound	TCP	21	FTP - protects server against data channel attacks
65	ftp-outbound	TCP	21	FTP - protects client against data channel attacks
66	ftp-passthrough	TCP	21	FTP - unrestricted - allows all transfer modes for client and server
67	http-in-all	TCP	80,443	HTTP and HTTPS with SYN flood protection
68	smb-all	TCP/UDP	135-139,445	All MS Windows networking ports
69	igmp	IPProto	2	Internet Group Management (multicast control)
70	rsvp	IPProto	46	Reservation Protocol
71	gre-encap	IPProto	47	Generic Routing Encapsulation
72	ipsec-esp	IPProto	50	IPsec ESP (encrypted and authenticated)
73	ipsec-ah	IPProto	51	IPsec AH (authenticated only)
74	ipsec-natt	UDP	4500	IPsec NAT-traversal (through udp/4500)
75	ipip-encap	IPProto	94	IP-in-IP encapsulation
76	ipcomp	IPProto	108	IP Payload Compression Protocol
77	ipsec-suite	Group	ipsec-natt,ipsec-ah,ipsec-esp,ike	The IPsec+IKE suite
78	pptp-suite	Group	gre-encap,pptp-ctl	PPTP control and transport
79	pptp-ctl	TCP	1723	Point-to-Point Tunneling Protocol - control channel
80	H323	TCP	1720	H.323 via H323 ALG - Enables H.323 communication
81	H323-Gatekeeper	UDP	1719	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers
82	ftp-internal	TCP	21	FTP - protects client and server against data channel attacks



81	Gatekeeper	UDP	1719	Gatekeepers
82	ftp-internal	TCP	21	FTP - protects client and server against data channel attacks
83	netcon	TCP/UDP	999	Remote Management

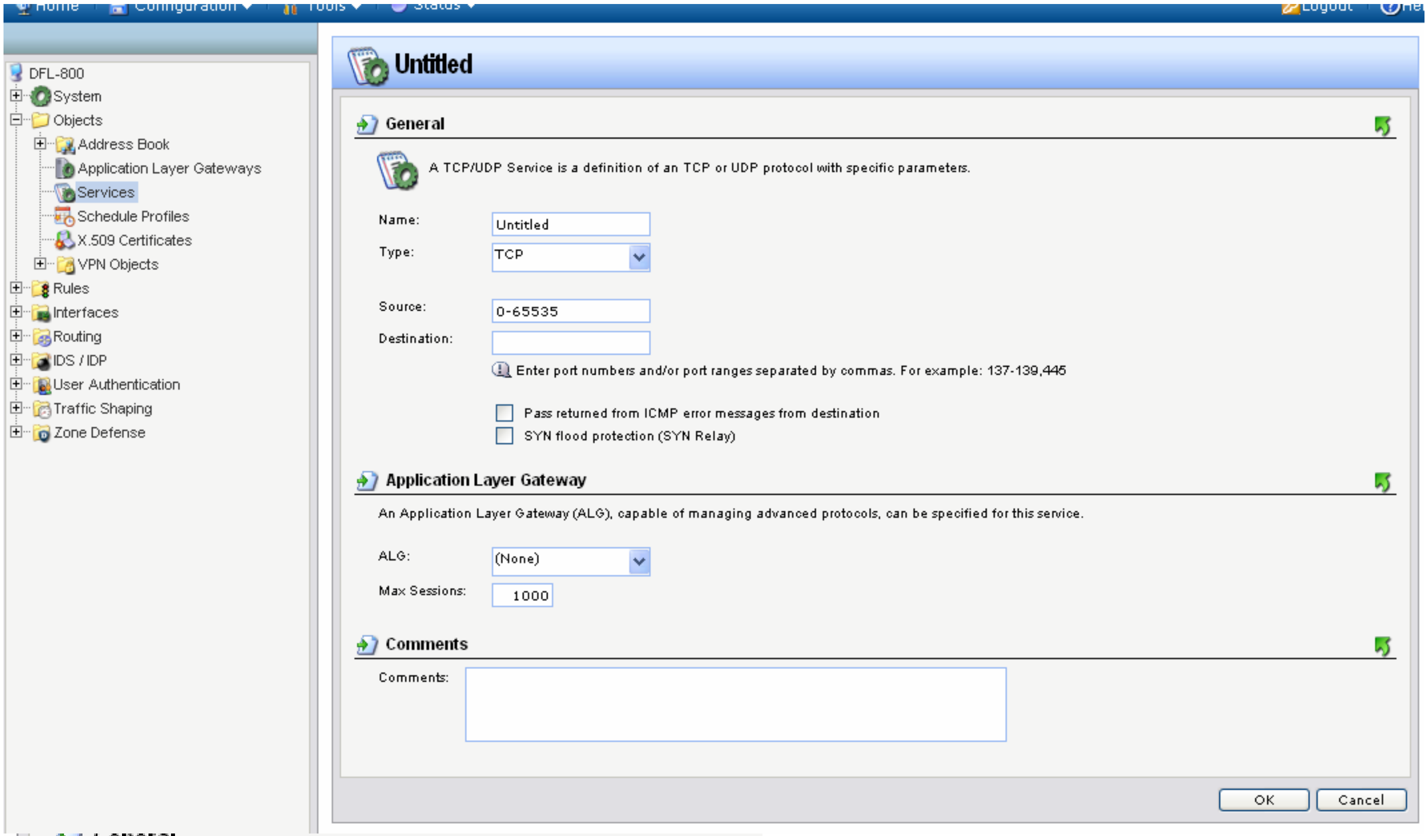
Right-click on a row for further options.



Services

Services are pre-definec

		Typ
		Gro
		ICM
2	all_tcp	TCF
3	all_udp	UDI
4	all_tcpudp	Gro
5	echo	TCF



Untitled

General

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

Name: Untitled

Type: TCP

Source: 0-65535

Destination:

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

□ Pass returned from ICMP error messages from destination

□ SYN flood protection (SYN Relay)

Application Layer Gateway

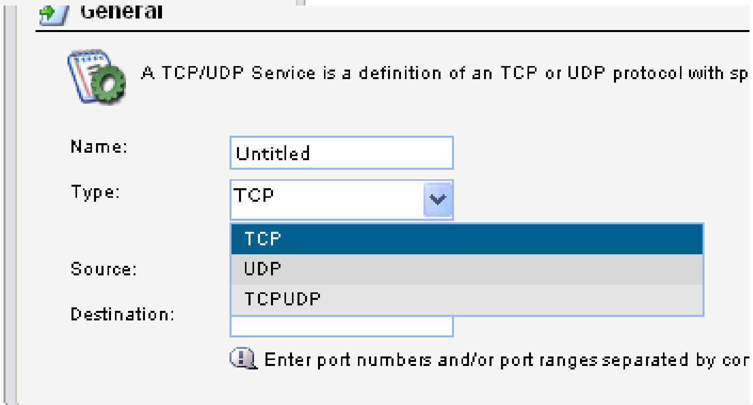
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: (None)

Max Sessions: 1000

Comments

Comments:



General

A TCP/UDP Service is a definition of an TCP or UDP protocol with sp

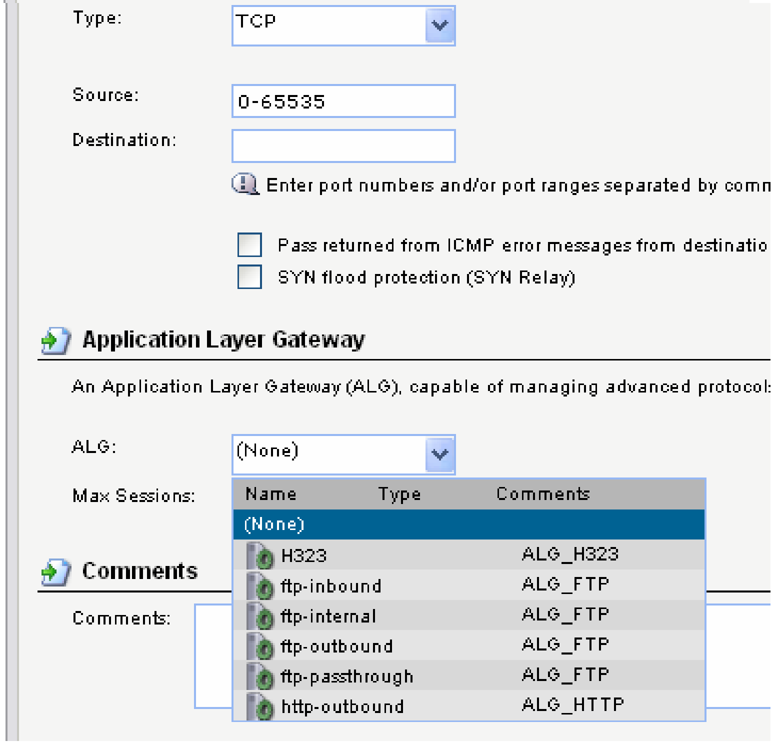
Name: Untitled

Type: TCP

Source:

Destination:

Enter port numbers and/or port ranges separated by cor



Type: TCP

Source: 0-65535

Destination:

Enter port numbers and/or port ranges separated by comm

□ Pass returned from ICMP error messages from destinatio

□ SYN flood protection (SYN Relay)

Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocol:

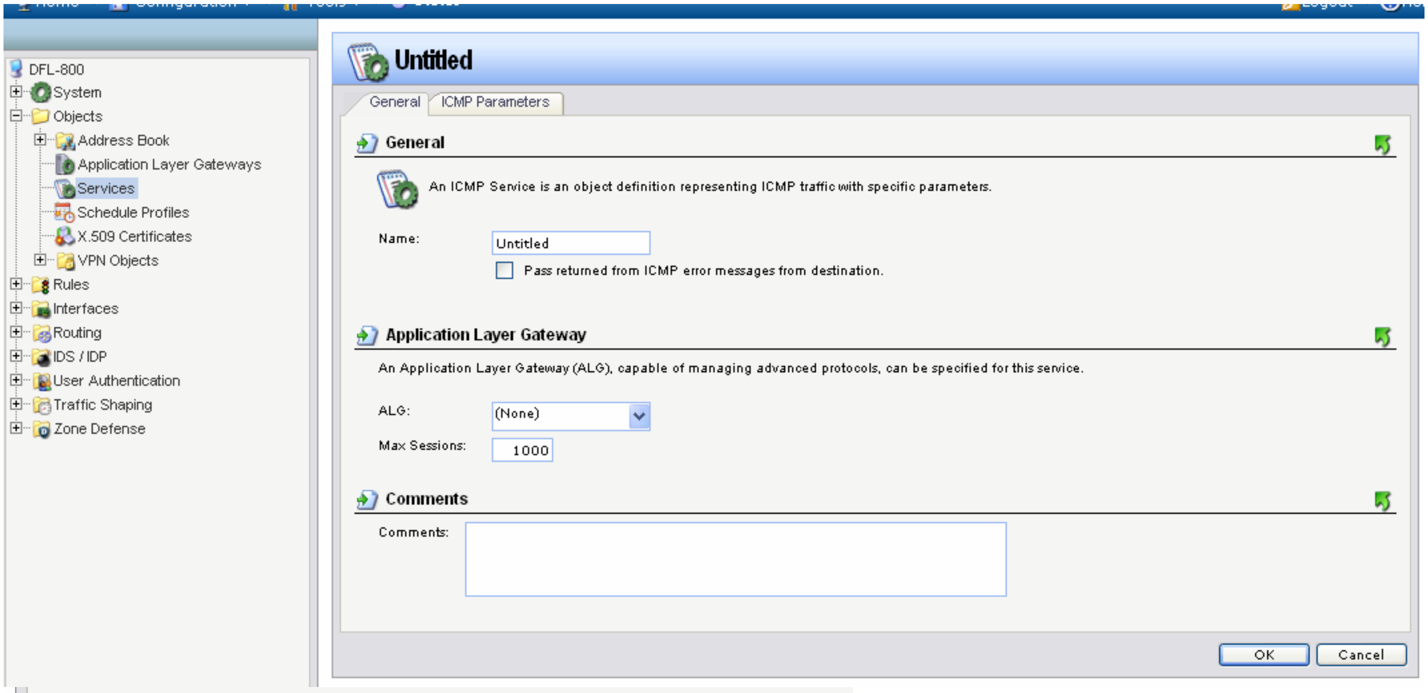
ALG: (None)

Max Sessions:

Name	Type	Comments
(None)		
H323	ALG_H323	
ftp-inbound	ALG_FTP	
ftp-internal	ALG_FTP	
ftp-outbound	ALG_FTP	
ftp-passthrough	ALG_FTP	
http-outbound	ALG_HTTP	

Comments

Comments:



Untitled

General

An ICMP Service is an object definition representing ICMP traffic with specific parameters.

Name: Untitled

□ Pass returned from ICMP error messages from destination.

Application Layer Gateway

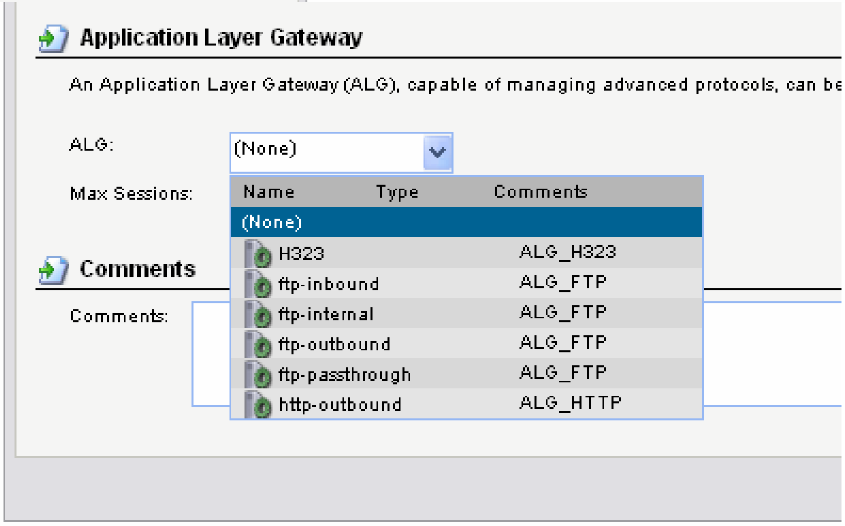
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: (None)

Max Sessions: 1000

Comments

Comments:



Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be

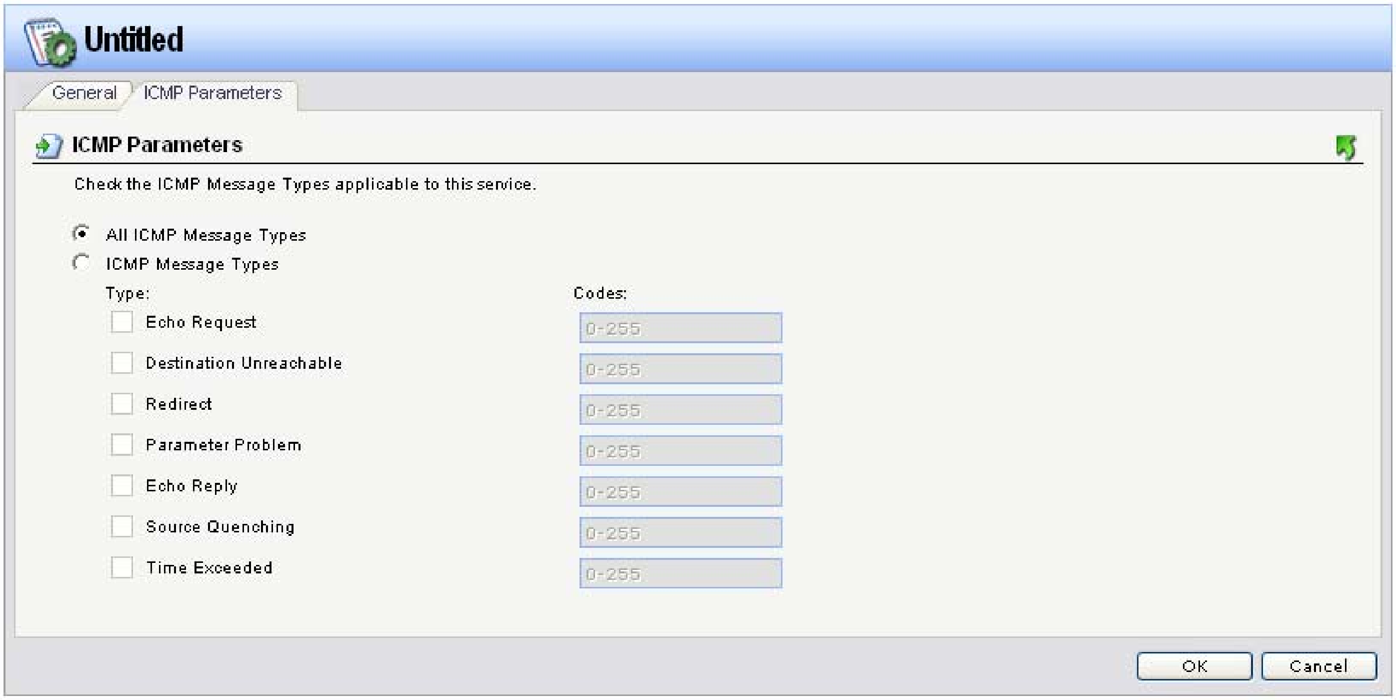
ALG: (None)

Max Sessions:

Name	Type	Comments
(None)		
H323	ALG_H323	
ftp-inbound	ALG_FTP	
ftp-internal	ALG_FTP	
ftp-outbound	ALG_FTP	
ftp-passthrough	ALG_FTP	
http-outbound	ALG_HTTP	

Comments

Comments:



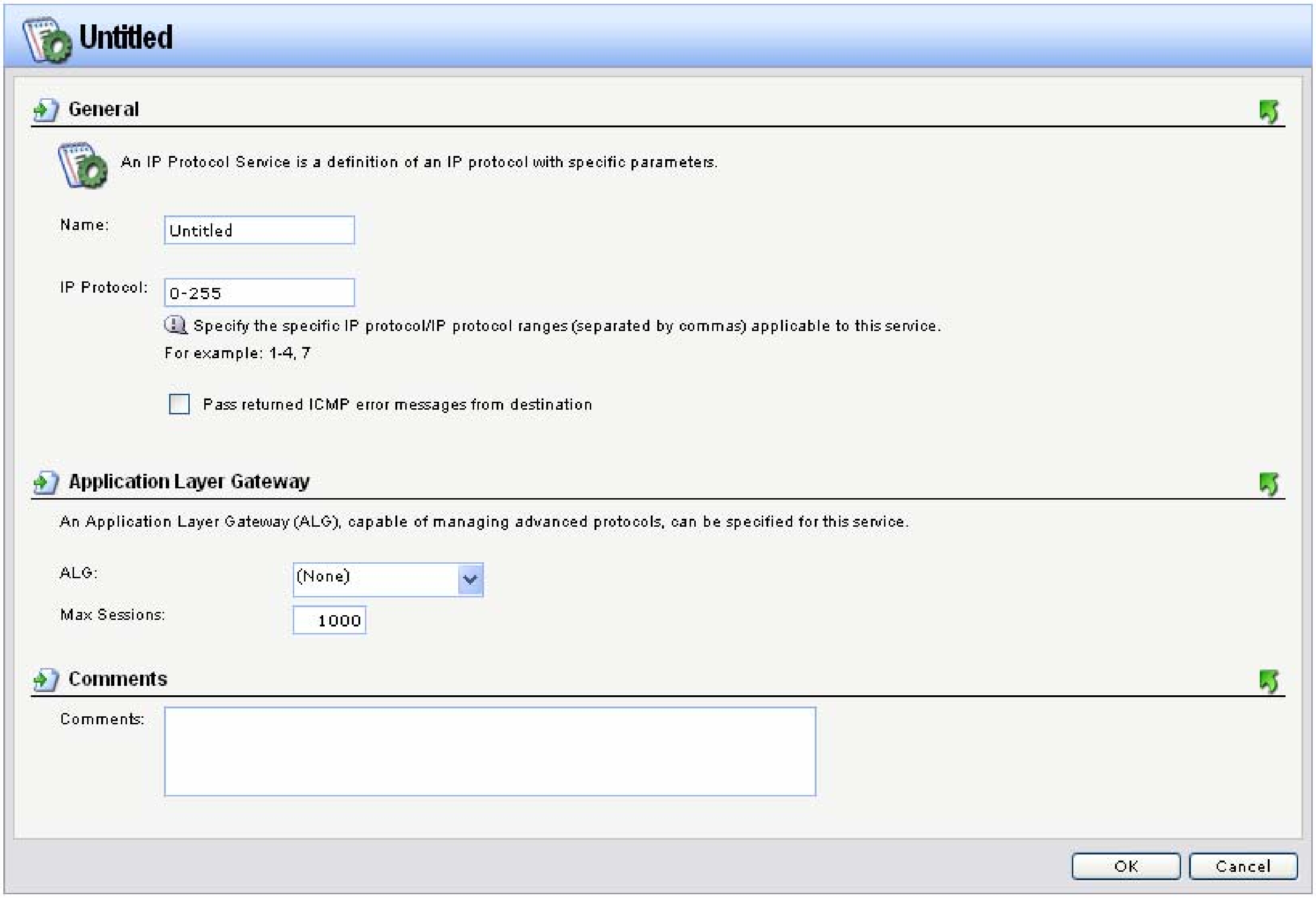
Untitled

ICMP Parameters

Check the ICMP Message Types applicable to this service.

● All ICMP Message Types
○ ICMP Message Types

Type:	Codes:
□ Echo Request	0-255
□ Destination Unreachable	0-255
□ Redirect	0-255
□ Parameter Problem	0-255
□ Echo Reply	0-255
□ Source Quenching	0-255
□ Time Exceeded	0-255



Untitled

General

An IP Protocol Service is a definition of an IP protocol with specific parameters.

Name: Untitled

IP Protocol: 0-255

Specify the specific IP protocol/IP protocol ranges (separated by commas) applicable to this service.

For example: 1-4, 7

□ Pass returned ICMP error messages from destination

Application Layer Gateway

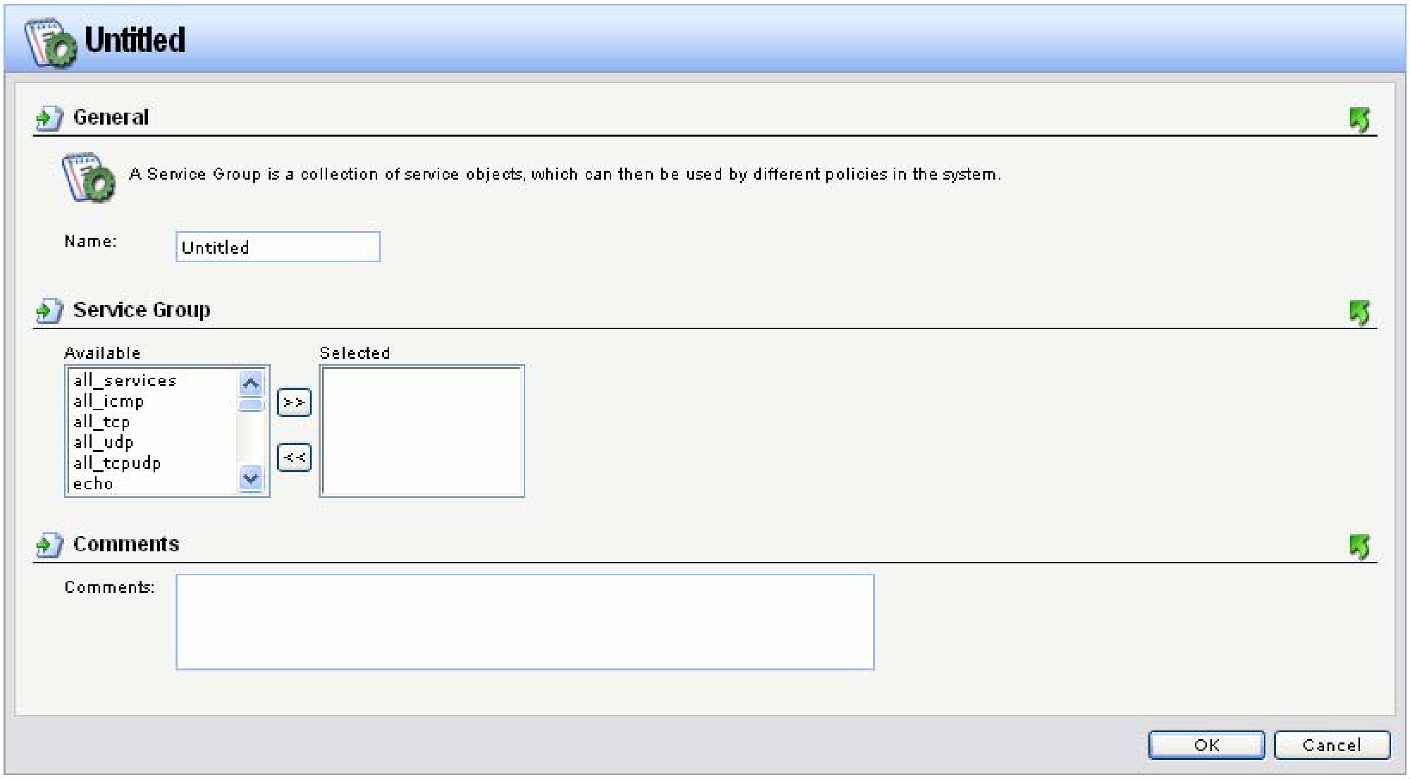
An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this service.

ALG: (None)

Max Sessions: 1000

Comments

Comments:



Untitled

General

A Service Group is a collection of service objects, which can then be used by different policies in the system.

Name: Untitled

Service Group

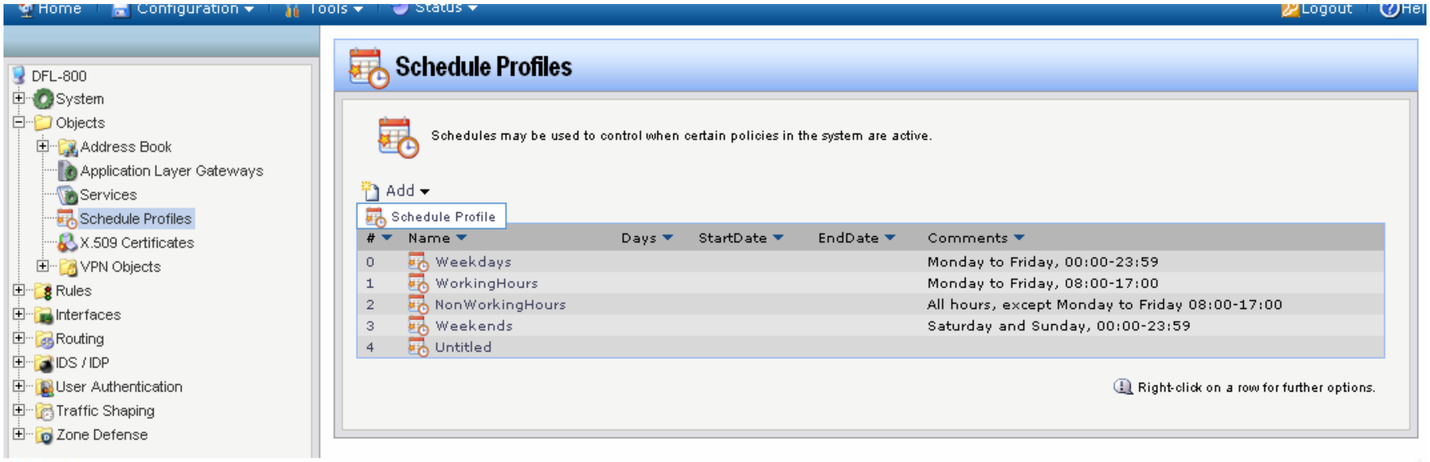
Available

all_services
all_icmp
all_tcp
all_udp
all_tcpudp
echo

Selected

Comments

Comments:

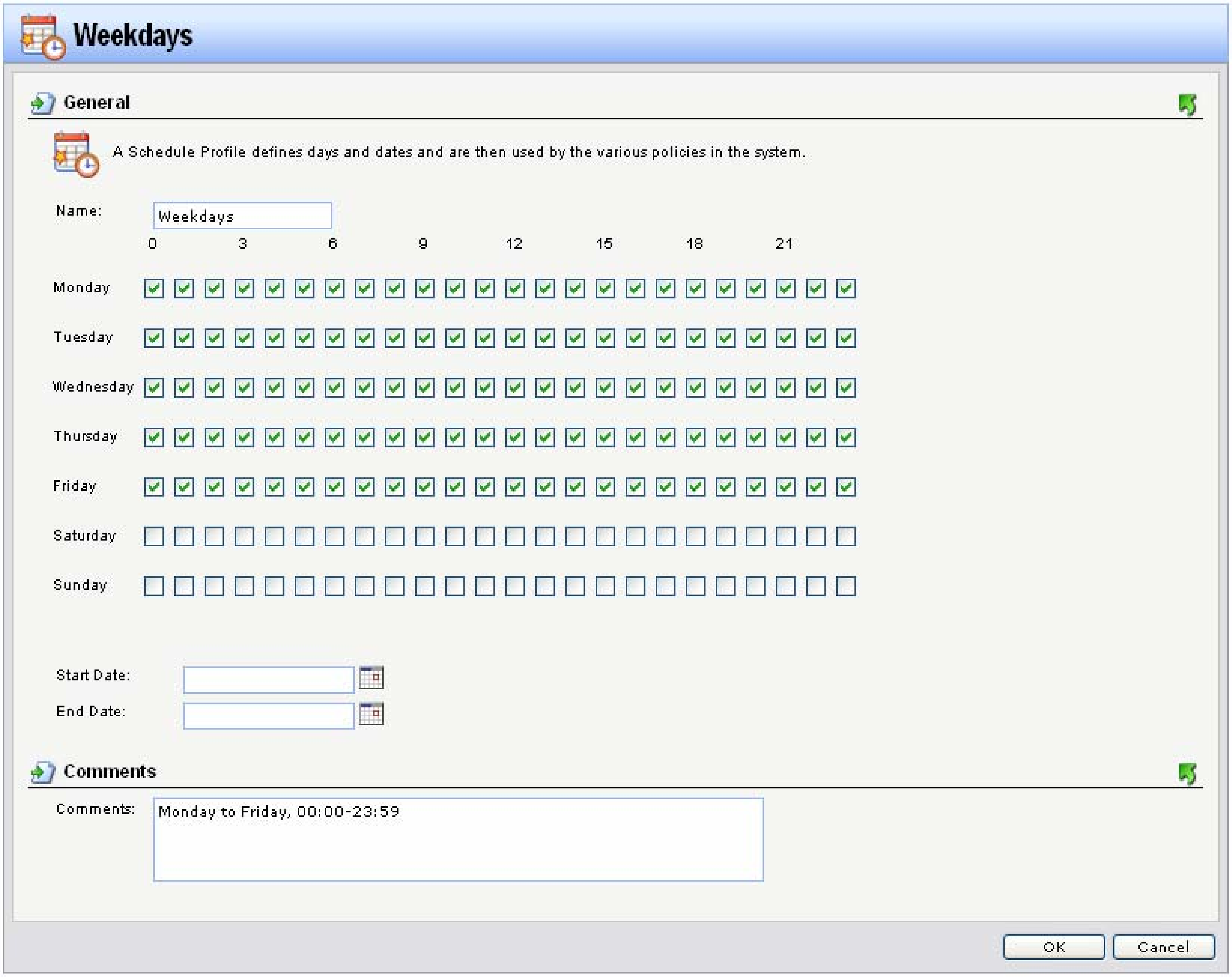


Schedule Profiles

Schedules may be used to control when certain policies in the system are active.

#	Name	Days	StartDate	EndDate	Comments
0	Weekdays				Monday to Friday, 00:00-23:59
1	WorkingHours				Monday to Friday, 08:00-17:00
2	NonWorkingHours				All hours, except Monday to Friday 08:00-17:00
3	Weekends				Saturday and Sunday, 00:00-23:59
4	Untitled				

Right-click on a row for further options.



Weekdays

General

A Schedule Profile defines days and dates and are then used by the various policies in the system.

Name: Weekdays

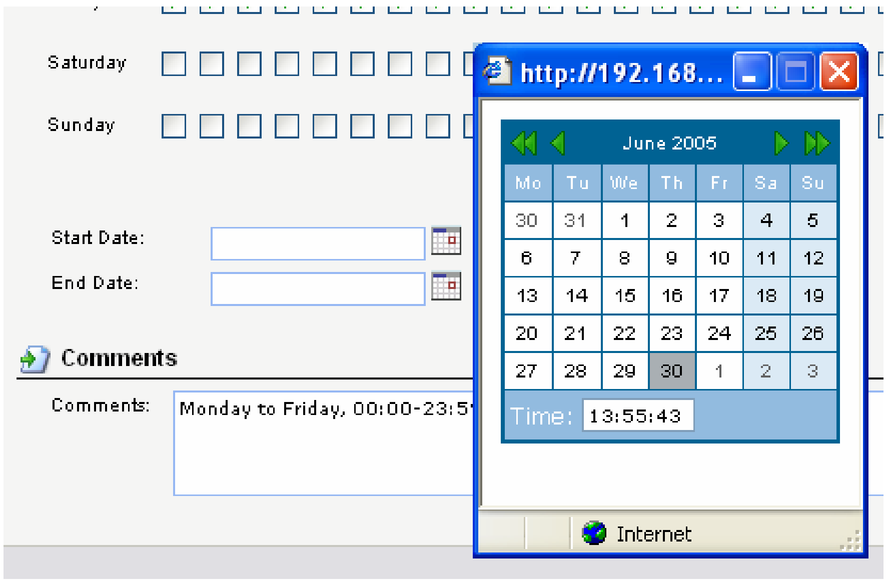
	0			3			6			9			12			15			18			21		
Monday	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Tuesday	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Wednesday	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Thursday	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Friday	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Saturday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Sunday	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Start Date:

End Date:

Comments

Comments: Monday to Friday, 00:00-23:59



Start Date:

End Date:

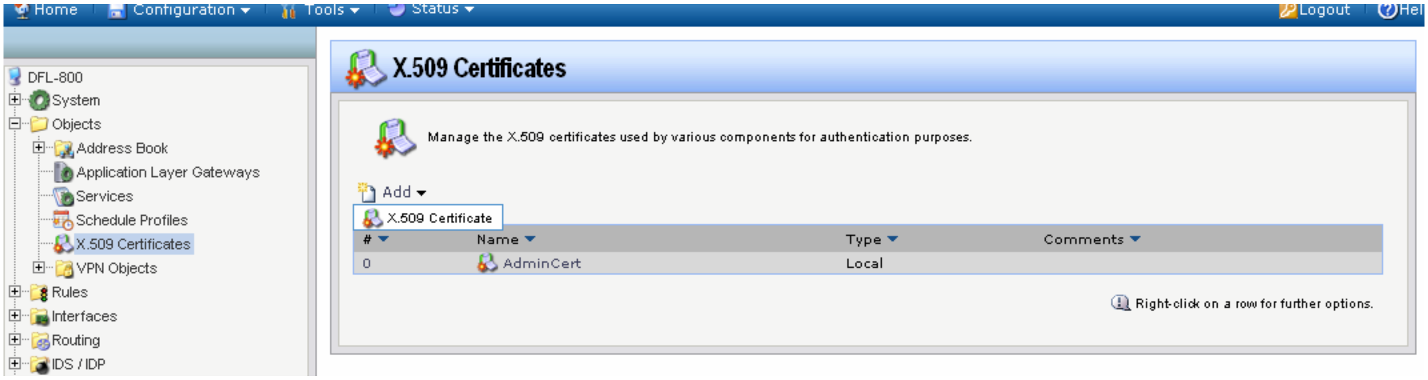
Comments

Comments: Monday to Friday, 00:00-23:5

June 2005

Mo	Tu	We	Th	Fr	Sa	Su
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	1	2	3

Time: 13:55:43

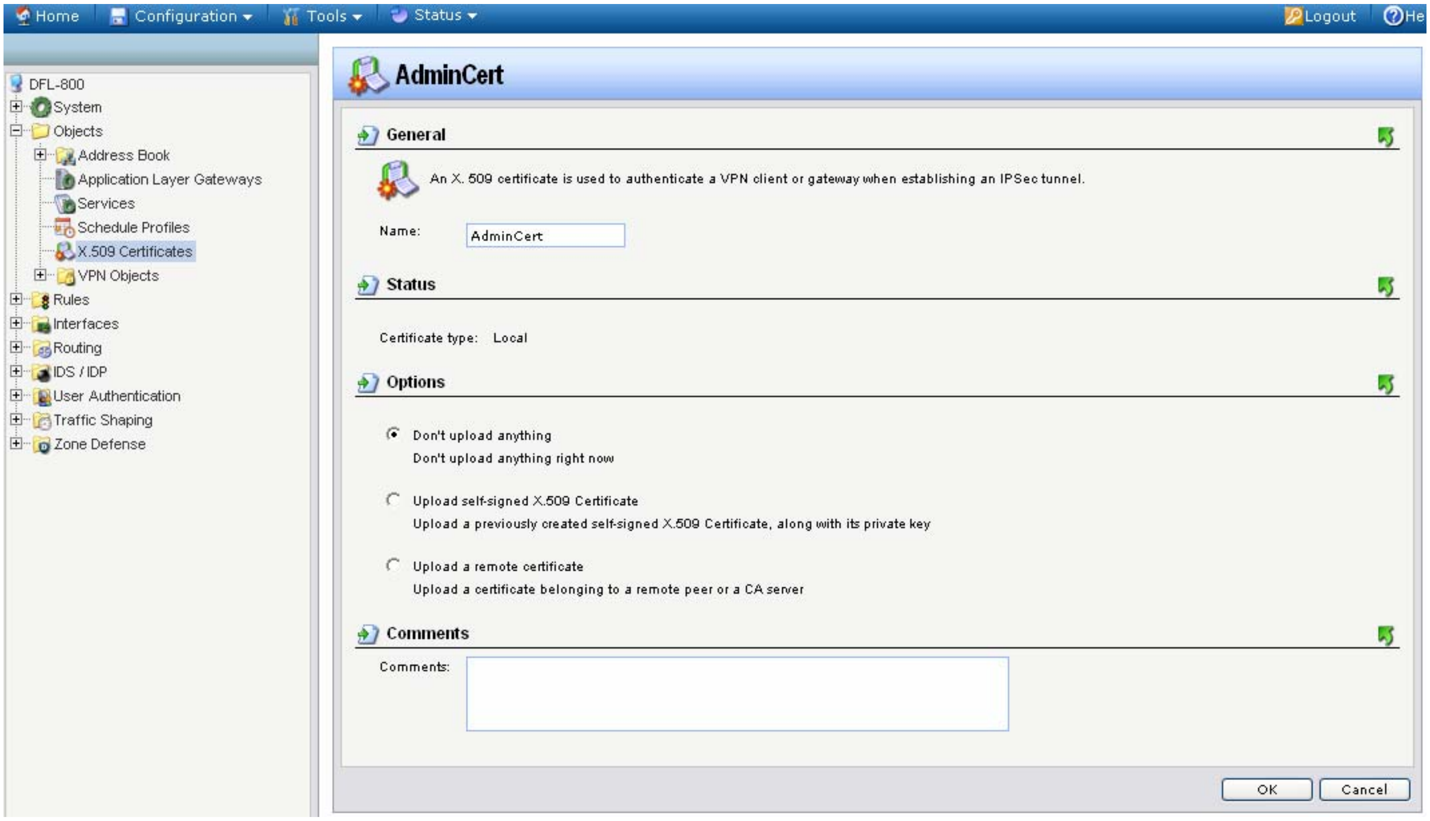


X.509 Certificates

Manage the X.509 certificates used by various components for authentication purposes.

#	Name	Type	Comments
0	AdminCert	Local	

Right-click on a row for further options.



AdminCert

General

An X. 509 certificate is used to authenticate a VPN client or gateway when establishing an IPSec tunnel.

Name: AdminCert

Status

Certificate type: Local

Options

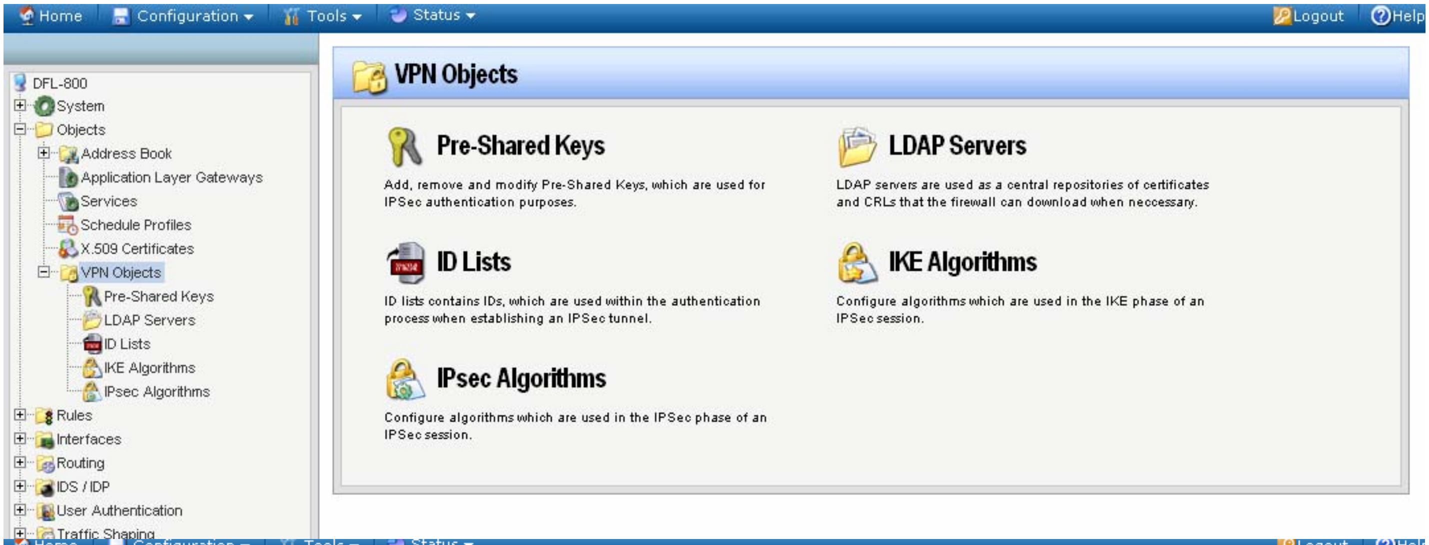
● Don't upload anything
Don't upload anything right now

○ Upload self-signed X.509 Certificate
Upload a previously created self-signed X.509 Certificate, along with its private key

○ Upload a remote certificate
Upload a certificate belonging to a remote peer or a CA server

Comments

Comments:



VPN Objects

Pre-Shared Keys

Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.

LDAP Servers

LDAP servers are used as a central repositories of certificates and CRLs that the firewall can download when neccessary.

ID Lists

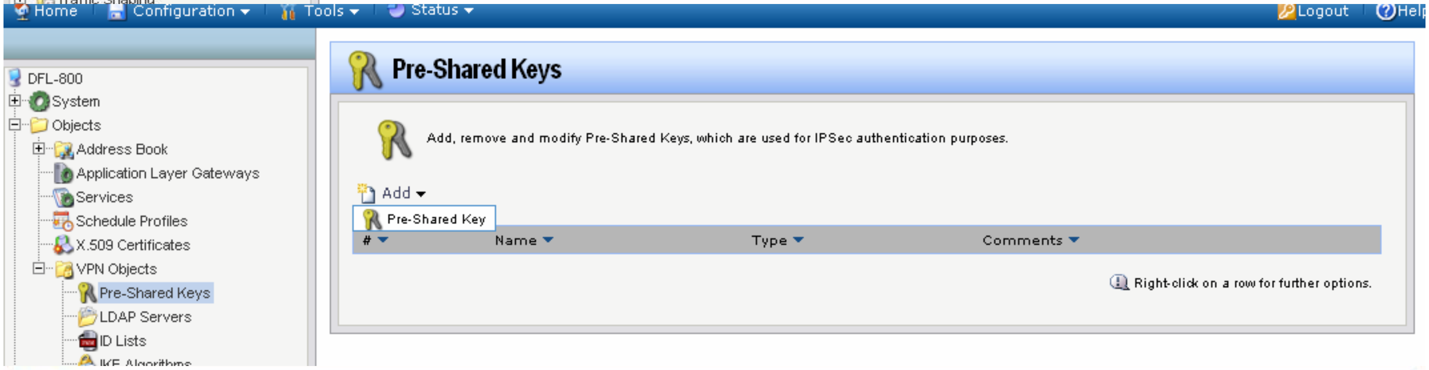
ID lists contains IDs, which are used within the authentication process when establishing an IPSec tunnel.

IKE Algorithms

Configure algorithms which are used in the IKE phase of an IPSec session.

IPsec Algorithms

Configure algorithms which are used in the IPSec phase of an IPSec session.

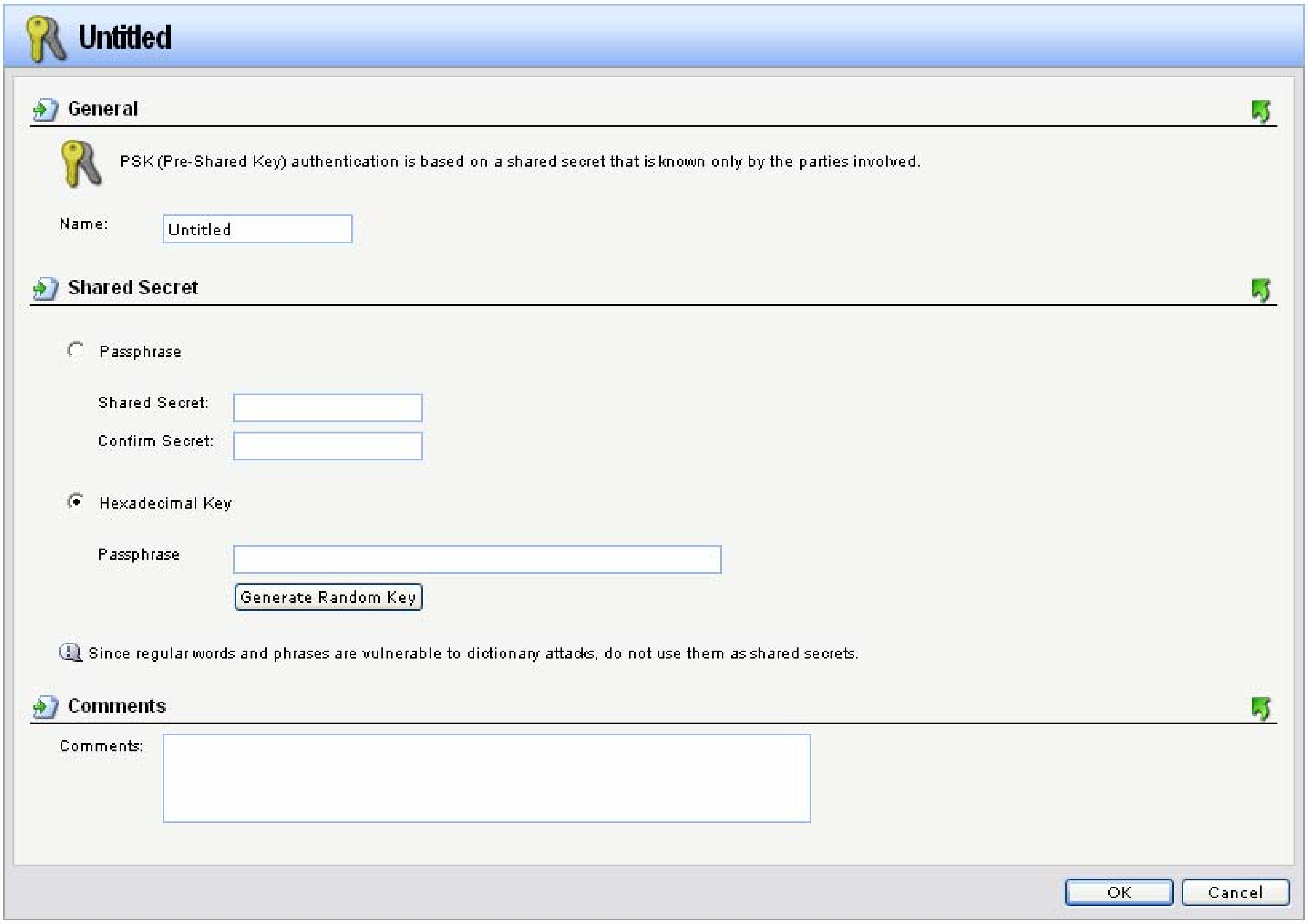


Pre-Shared Keys

Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.

#	Name	Type	Comments

Right-click on a row for further options.



Untitled

General

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

Name: Untitled

Shared Secret

○ Passphrase

Shared Secret:

Confirm Secret:

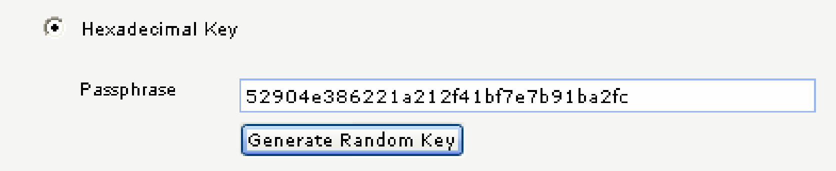
● Hexadecimal Key

Passphrase

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

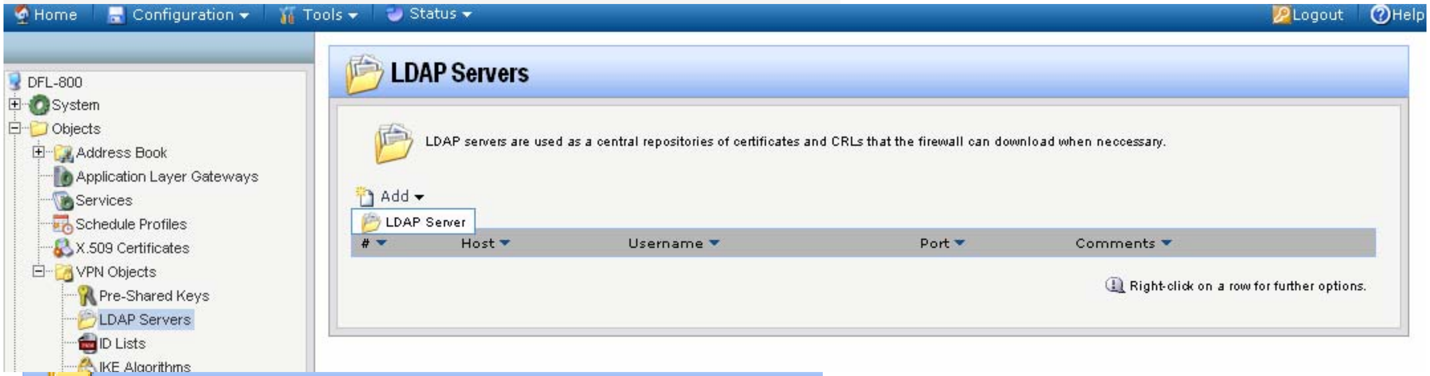
Comments

Comments:



● Hexadecimal Key

Passphrase 52904e386221a212f41bf7e7b91ba2fc

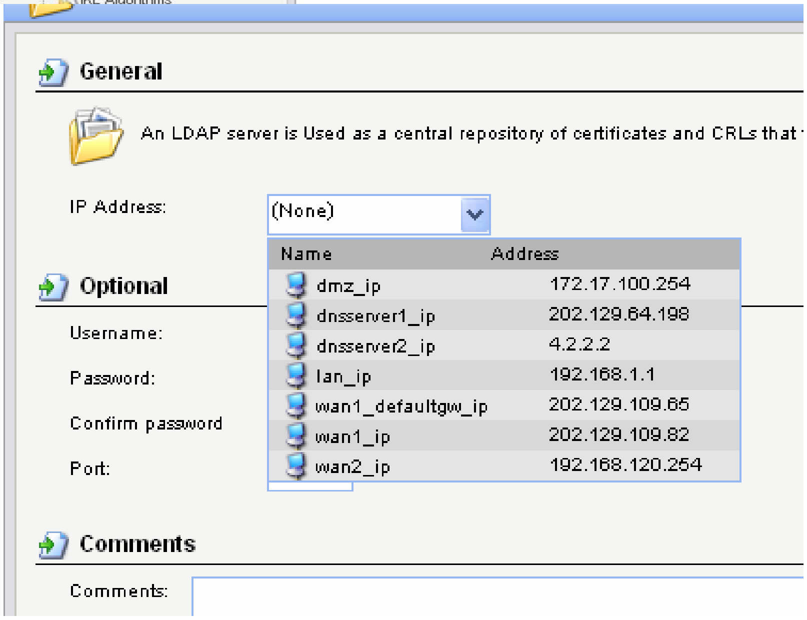


LDAP Servers

LDAP servers are used as a central repositories of certificates and CRLs that the firewall can download when neccessary.

#	Host	Username	Port	Comments

Right-click on a row for further options.



General

An LDAP server is Used as a central repository of certificates and CRLs that

IP Address: (None)

Name	Address
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254

Optional

Username:

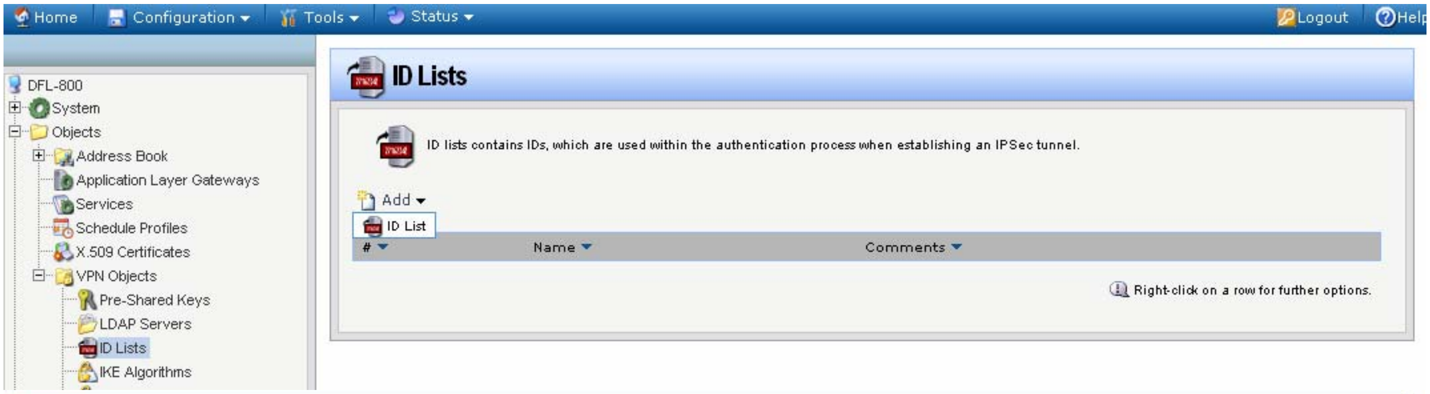
Password:

Confirm password

Port:

Comments

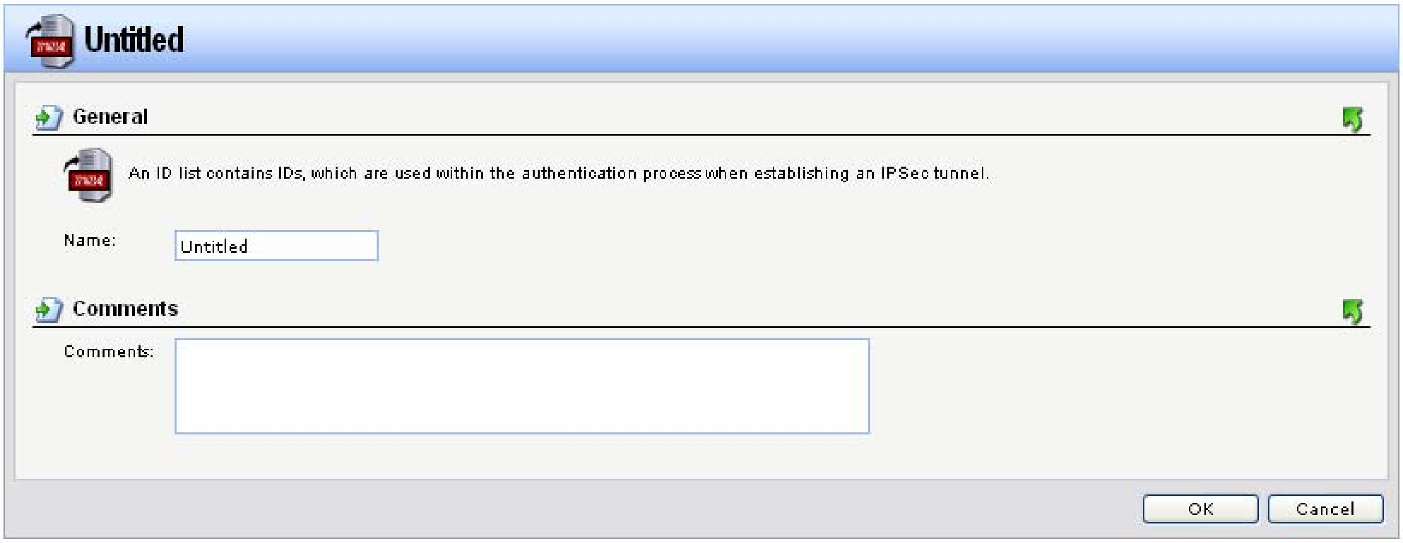
Comments:



ID Lists

ID lists contains IDs, which are used within the authentication process when establishing an IPSec tunnel.

Right-click on a row for further options.



Untitled

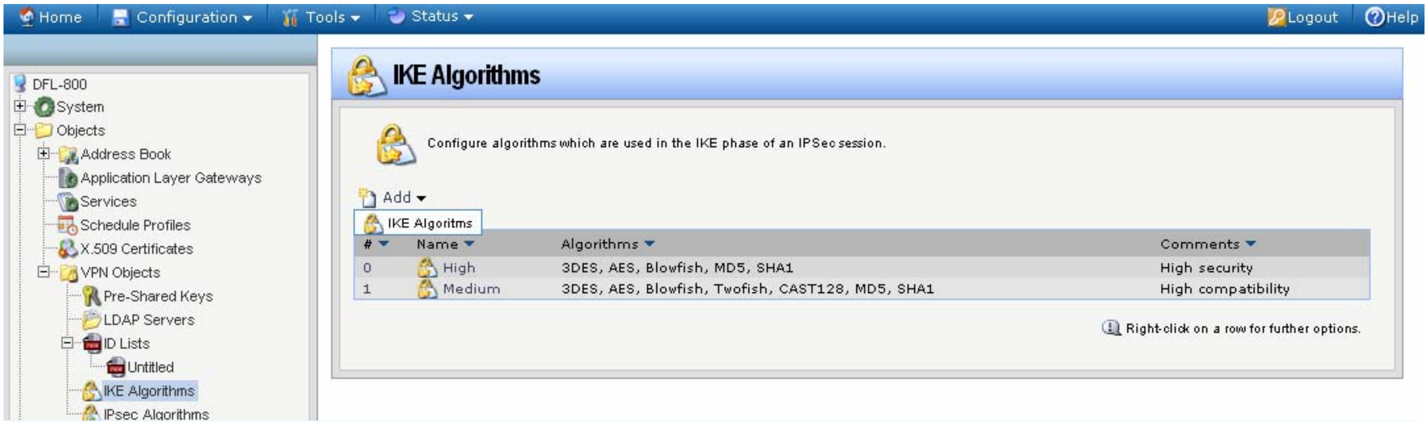
General

An ID list contains IDs, which are used within the authentication process when establishing an IPSec tunnel.

Name: Untitled

Comments

Comments:

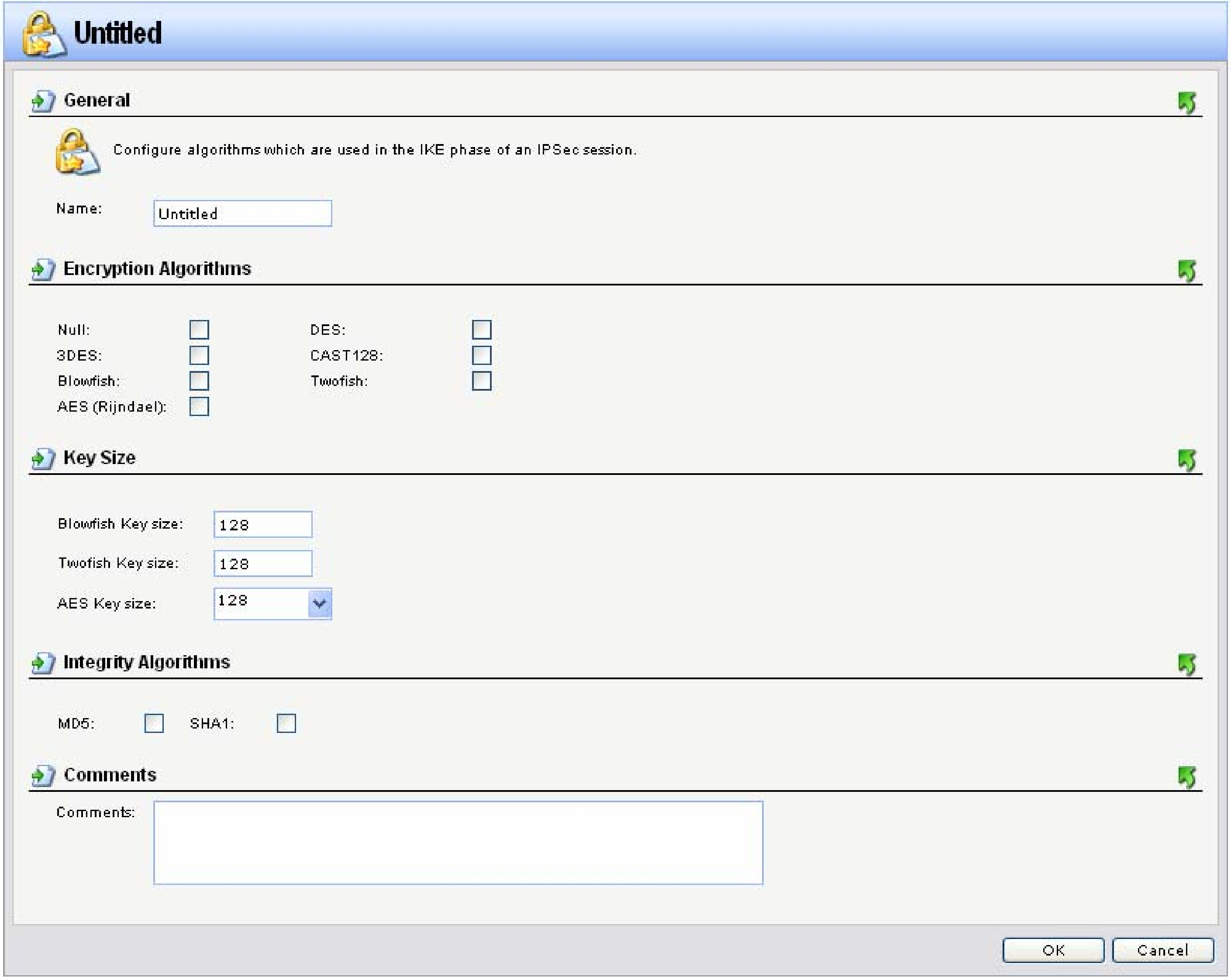


IKE Algorithms

Configure algorithms which are used in the IKE phase of an IPSec session.

#	Name	Algorithms	Comments
0	High	3DES, AES, Blowfish, MD5, SHA1	High security
1	Medium	3DES, AES, Blowfish, Twofish, CAST128, MD5, SHA1	High compatibility

Right-click on a row for further options.



Untitled

General

Configure algorithms which are used in the IKE phase of an IPSec session.

Name: Untitled

Encryption Algorithms

Null: □ DES: □
3DES: □ CAST128: □
Blowfish: □ Twofish: □
AES (Rijndael): □

Key Size

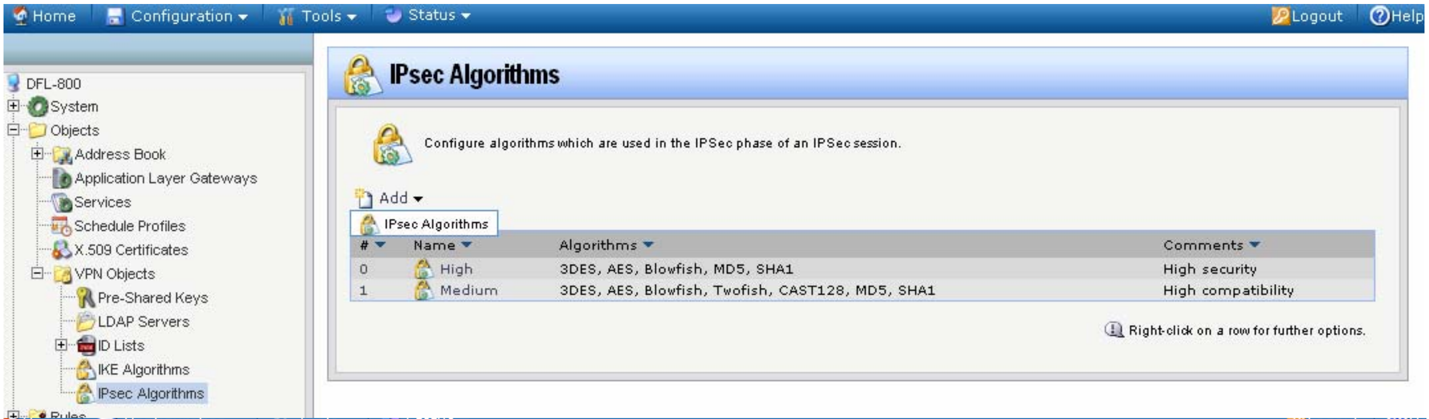
Blowfish Key size: 128
Twofish Key size: 128
AES Key size: 128

Integrity Algorithms

MD5: □ SHA1: □

Comments

Comments:

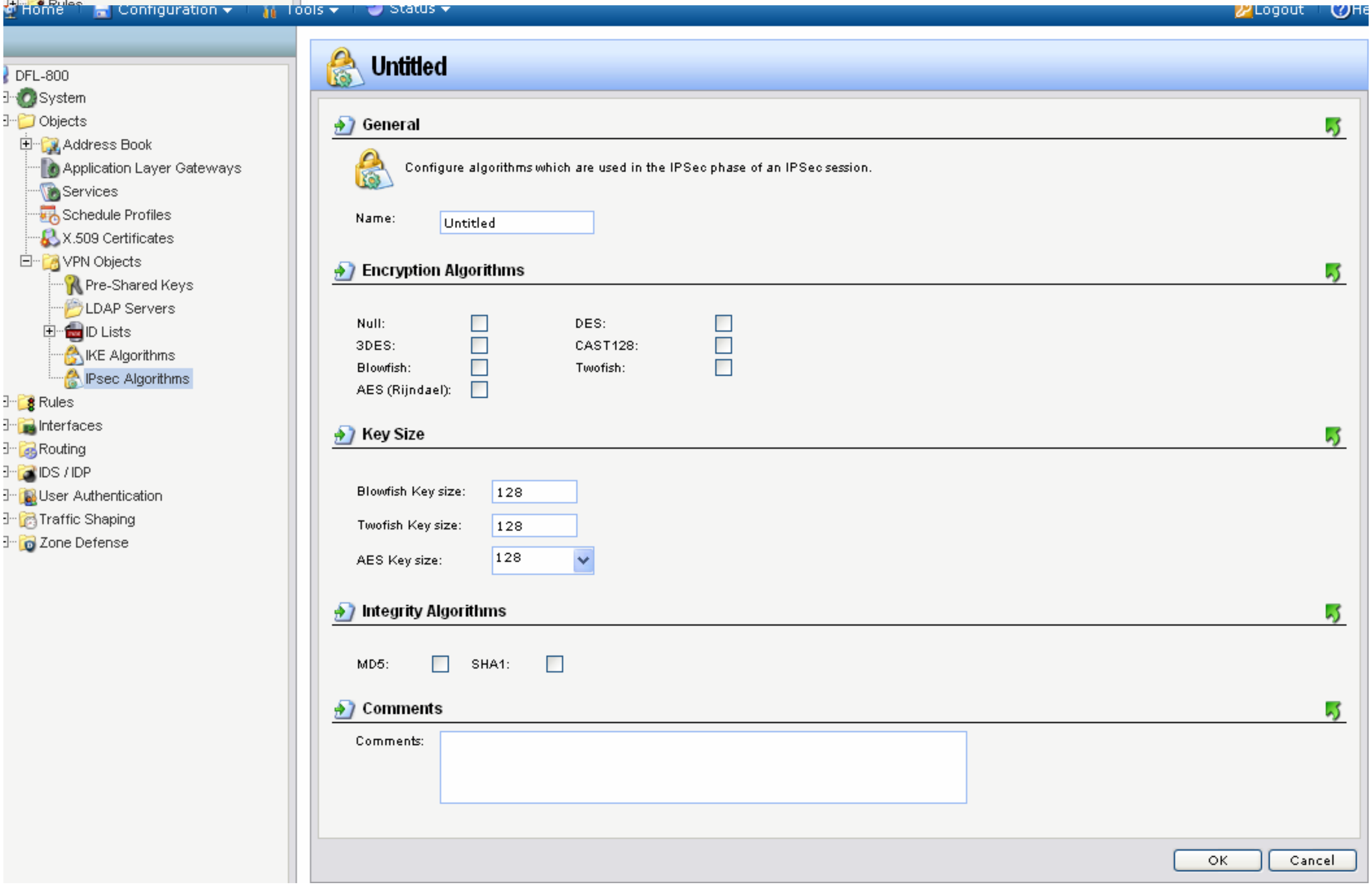


IPsec Algorithms

Configure algorithms which are used in the IPSec phase of an IPSec session.

#	Name	Algorithms	Comments
0	High	3DES, AES, Blowfish, MD5, SHA1	High security
1	Medium	3DES, AES, Blowfish, Twofish, CAST128, MD5, SHA1	High compatibility

Right-click on a row for further options.



Untitled

General

Configure algorithms which are used in the IPSec phase of an IPSec session.

Name: Untitled

Encryption Algorithms

Null:	□	DES:	□
3DES:	□	CAST128:	□
Blowfish:	□	Twofish:	□
AES (Rijndael):	□		

Key Size

Blowfish Key size: 128

Twofish Key size: 128

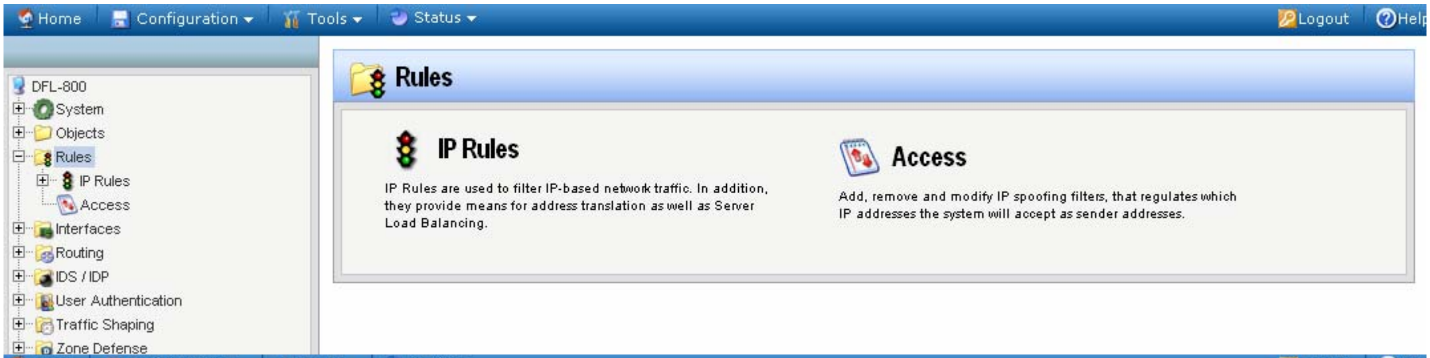
AES Key size: 128

Integrity Algorithms

MD5: □ SHA1: □

Comments

Comments:



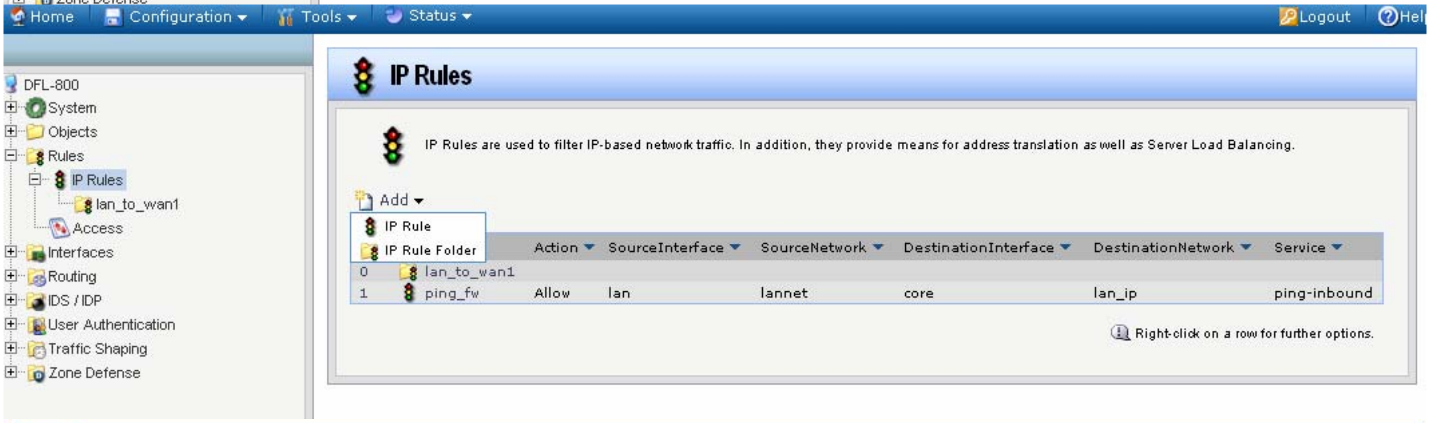
Rules

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.

Access

Add, remove and modify IP spoofing filters, that regulates which IP addresses the system will accept as sender addresses.

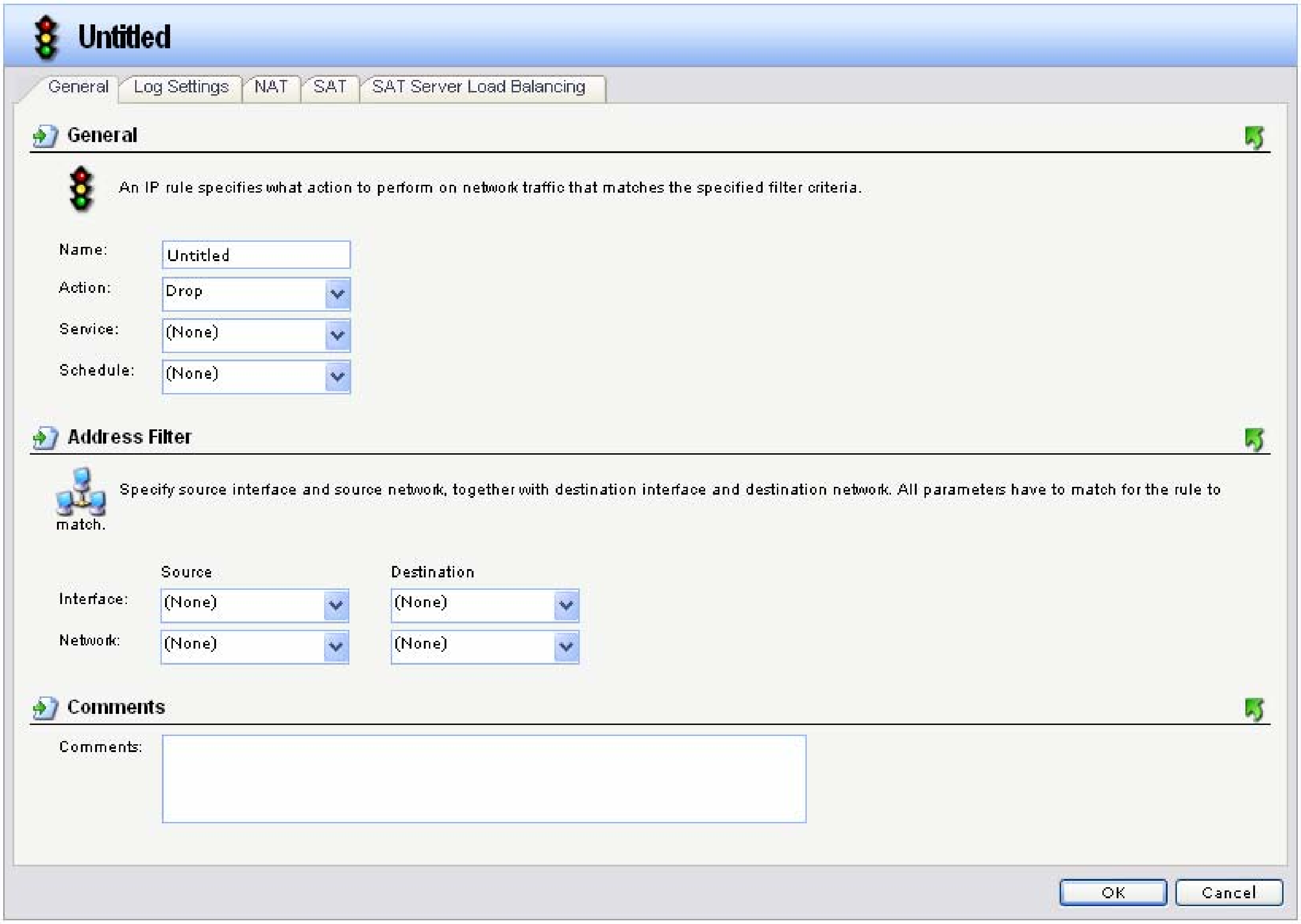


IP Rules

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	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
0	lan_to_wan1						
1	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound

Right-click on a row for further options.



Untitled

General

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

Name: Untitled

Action: Drop

Service: (None)

Schedule: (None)

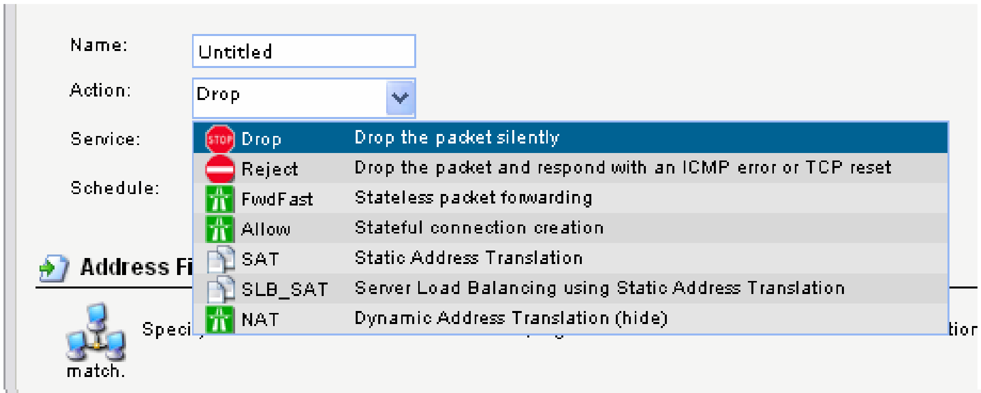
Address Filter

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

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:



Name: Untitled

Action: Drop

Service:

Schedule:

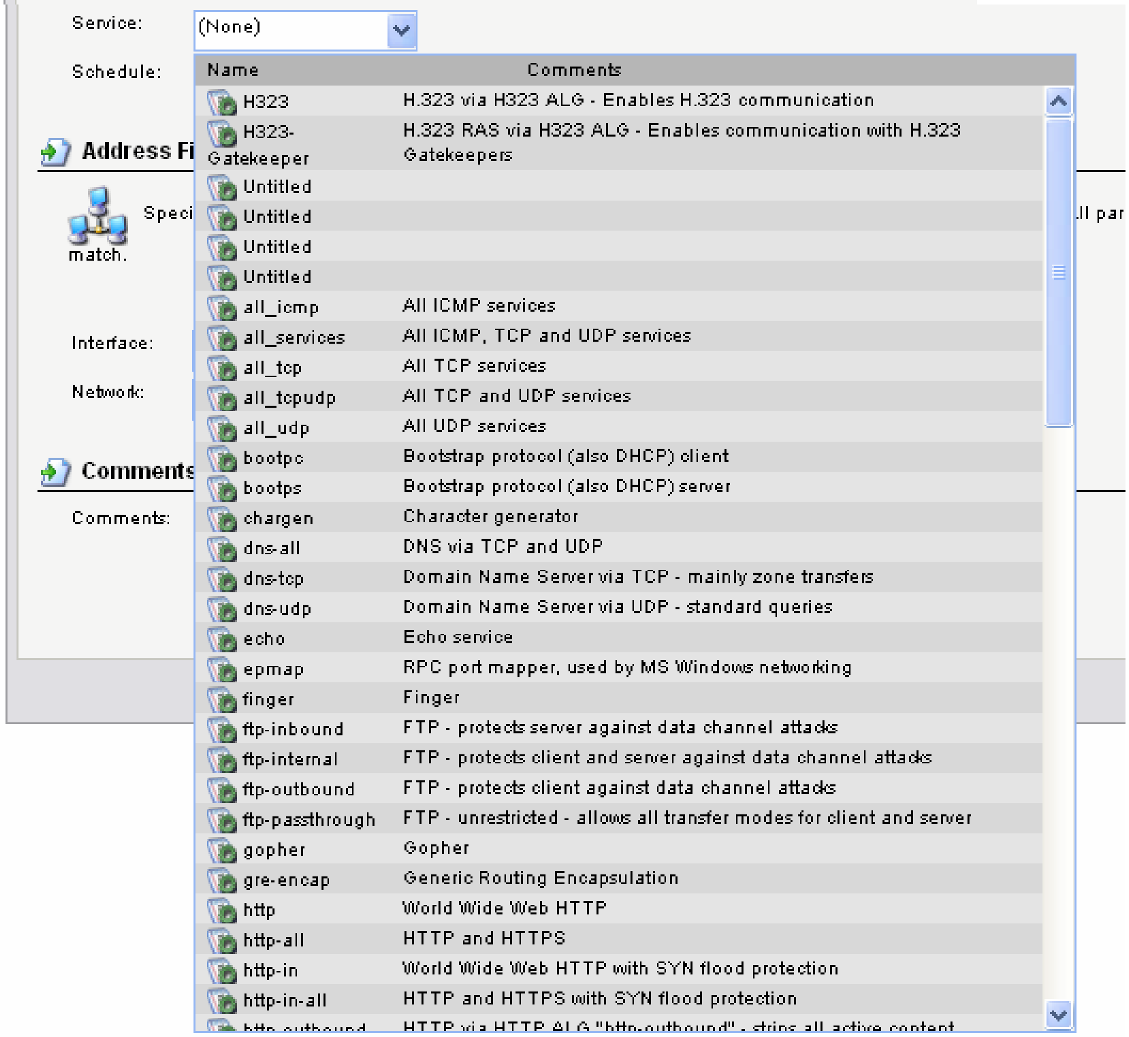
Address Fi

Speci

match.

tior

Drop	Drop the packet silently
Reject	Drop the packet and respond with an ICMP error or TCP reset
FwdFast	Stateless packet forwarding
Allow	Stateful connection creation
SAT	Static Address Translation
SLB_SAT	Server Load Balancing using Static Address Translation
NAT	Dynamic Address Translation (hide)



Service: (None)

Schedule:

Address Fi

Speci

match.

Interface:

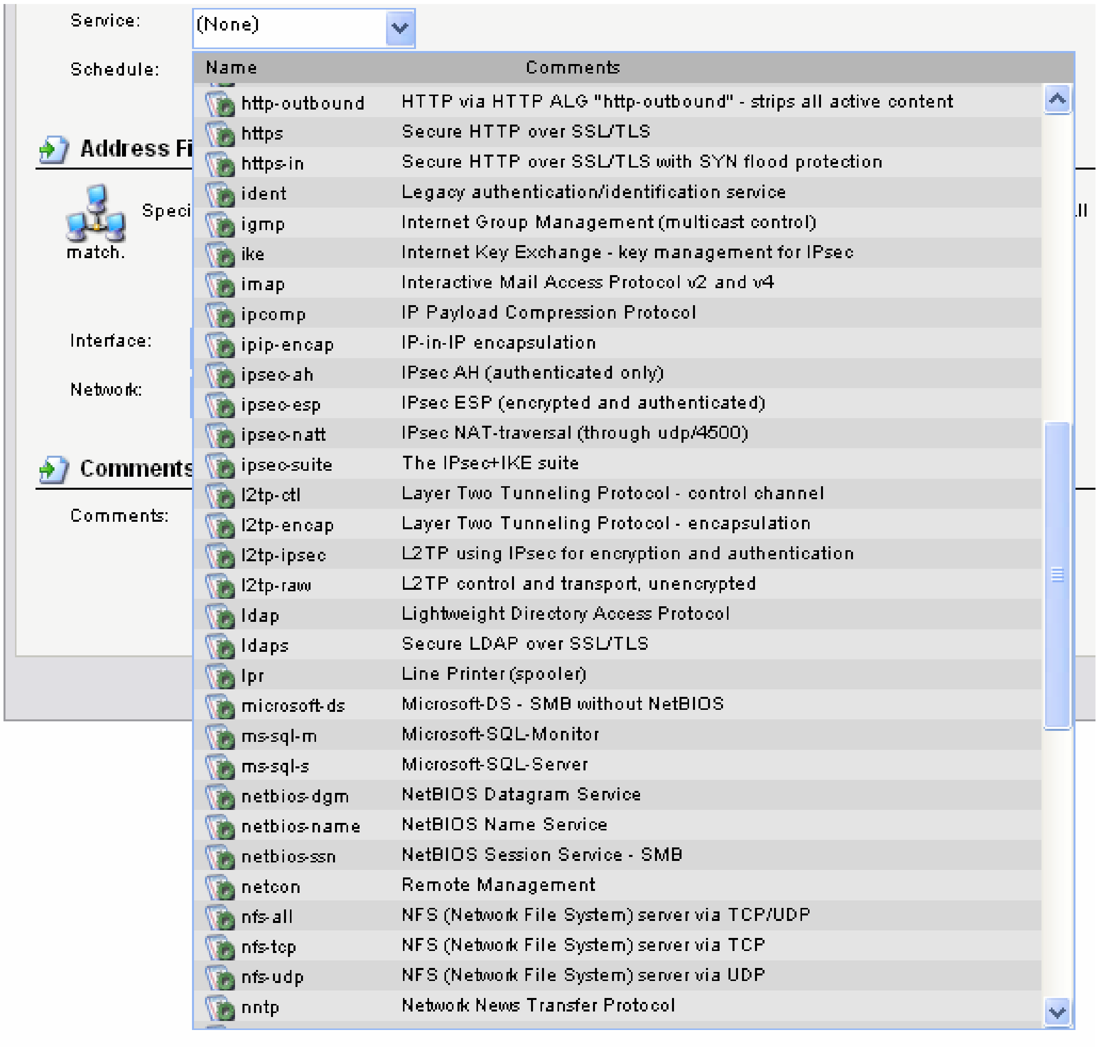
Network:

Comments

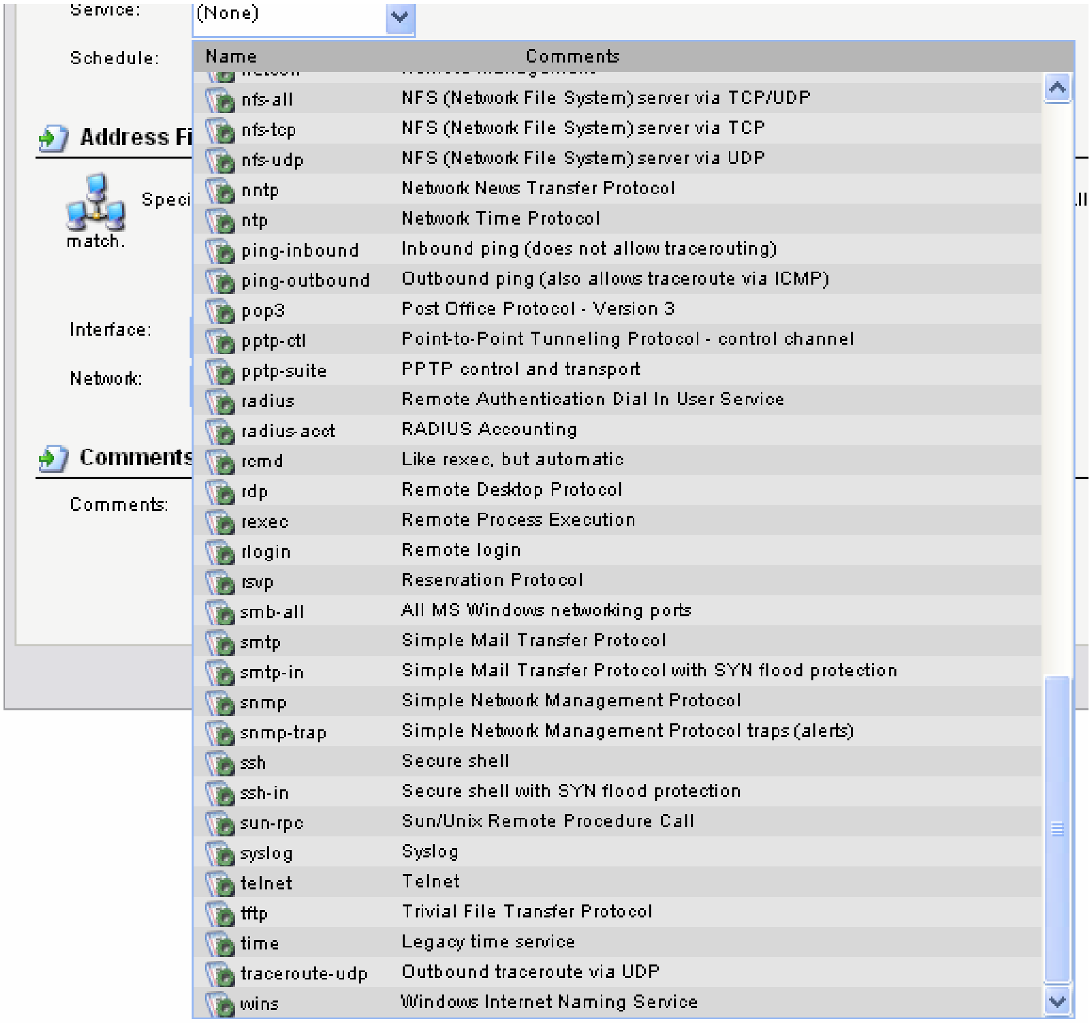
Comments:

ll par

Name	Comments
H323	H.323 via H323 ALG - Enables H.323 communication
H323-Gatekeeper	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers
Untitled	
Untitled	
Untitled	
Untitled	
all_icmp	All ICMP services
all_services	All ICMP, TCP and UDP services
all_tcp	All TCP services
all_tcpudp	All TCP and UDP services
all_udp	All UDP services
bootpc	Bootstrap protocol (also DHCP) client
bootps	Bootstrap protocol (also DHCP) server
chargen	Character generator
dns-all	DNS via TCP and UDP
dns-tcp	Domain Name Server via TCP - mainly zone transfers
dns-udp	Domain Name Server via UDP - standard queries
echo	Echo service
epmap	RPC port mapper, used by MS Windows networking
finger	Finger
ftp-inbound	FTP - protects server against data channel attacks
ftp-internal	FTP - protects client and server against data channel attacks
ftp-outbound	FTP - protects client against data channel attacks
ftp-passthrough	FTP - unrestricted - allows all transfer modes for client and server
gopher	Gopher
gre-encap	Generic Routing Encapsulation
http	World Wide Web HTTP
http-all	HTTP and HTTPS
http-in	World Wide Web HTTP with SYN flood protection
http-in-all	HTTP and HTTPS with SYN flood protection
http-outbound	HTTP via HTTP ALG "http-outbound" - strips all active content



Name	Comments
http-outbound	HTTP via HTTP ALG "http-outbound" - strips all active content
https	Secure HTTP over SSL/TLS
https-in	Secure HTTP over SSL/TLS with SYN flood protection
ident	Legacy authentication/identification service
igmp	Internet Group Management (multicast control)
ike	Internet Key Exchange - key management for IPsec
imap	Interactive Mail Access Protocol v2 and v4
ipcomp	IP Payload Compression Protocol
ipip-encap	IP-in-IP encapsulation
ipsec-ah	IPsec AH (authenticated only)
ipsec-esp	IPsec ESP (encrypted and authenticated)
ipsec-natt	IPsec NAT-traversal (through udp/4500)
ipsec-suite	The IPsec+IKE suite
l2tp-ctl	Layer Two Tunneling Protocol - control channel
l2tp-encap	Layer Two Tunneling Protocol - encapsulation
l2tp-ipsec	L2TP using IPsec for encryption and authentication
l2tp-raw	L2TP control and transport, unencrypted
ldap	Lightweight Directory Access Protocol
ldaps	Secure LDAP over SSL/TLS
lpr	Line Printer (spooler)
microsoft-ds	Microsoft-DS - SMB without NetBIOS
ms-sql-m	Microsoft-SQL-Monitor
ms-sql-s	Microsoft-SQL-Server
netbios-dgm	NetBIOS Datagram Service
netbios-name	NetBIOS Name Service
netbios-ssn	NetBIOS Session Service - SMB
netcon	Remote Management
nfs-all	NFS (Network File System) server via TCP/UDP
nfs-tcp	NFS (Network File System) server via TCP
nfs-udp	NFS (Network File System) server via UDP
nntp	Network News Transfer Protocol



Service: (None)

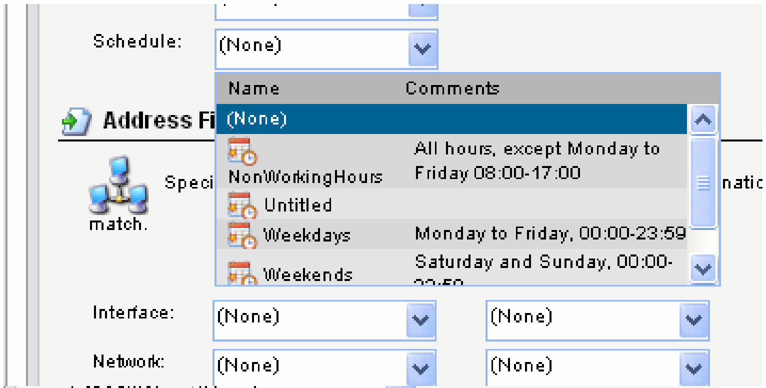
Schedule:

Interface:

Network:

Comments:

Name	Comments
nfs-all	NFS (Network File System) server via TCP/UDP
nfs-tcp	NFS (Network File System) server via TCP
nfs-udp	NFS (Network File System) server via UDP
nntp	Network News Transfer Protocol
ntp	Network Time Protocol
ping-inbound	Inbound ping (does not allow tracerouting)
ping-outbound	Outbound ping (also allows traceroute via ICMP)
pop3	Post Office Protocol - Version 3
pptp-ctl	Point-to-Point Tunneling Protocol - control channel
pptp-suite	PPTP control and transport
radius	Remote Authentication Dial In User Service
radius-acct	RADIUS Accounting
rcmd	Like rexec, but automatic
rdp	Remote Desktop Protocol
rexec	Remote Process Execution
rlogin	Remote login
rsvp	Reservation Protocol
smb-all	All MS Windows networking ports
smtp	Simple Mail Transfer Protocol
smtp-in	Simple Mail Transfer Protocol with SYN flood protection
snmp	Simple Network Management Protocol
snmp-trap	Simple Network Management Protocol traps (alerts)
ssh	Secure shell
ssh-in	Secure shell with SYN flood protection
sun-rpc	Sun/Unix Remote Procedure Call
syslog	Syslog
telnet	Telnet
tftp	Trivial File Transfer Protocol
time	Legacy time service
traceroute-udp	Outbound traceroute via UDP
wins	Windows Internet Naming Service

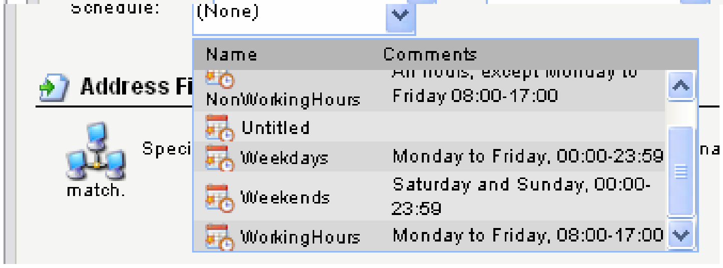


Schedule: (None)

Name	Comments
(None)	
NonWorkingHours	All hours, except Monday to Friday 08:00-17:00
Untitled	
Weekdays	Monday to Friday, 00:00-23:59
Weekends	Saturday and Sunday, 00:00-

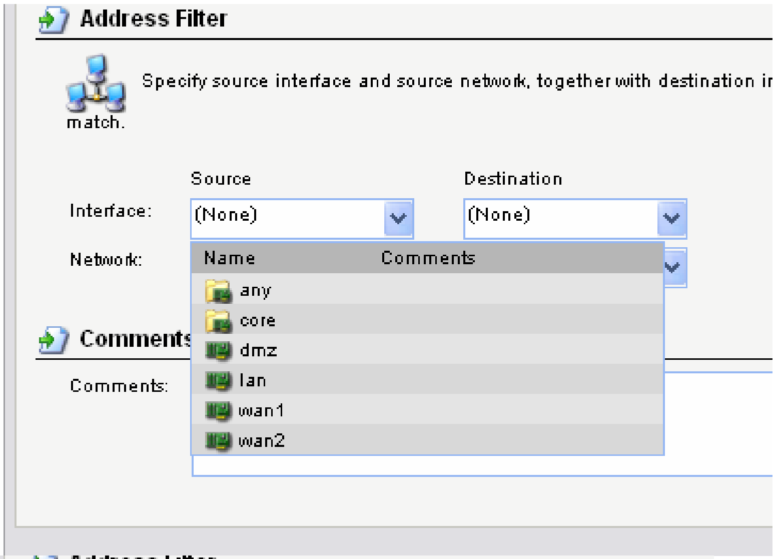
Interface: (None) (None)

Network: (None) (None)



Schedule: (None)

Name	Comments
NonWorkingHours	Friday 08:00-17:00
Untitled	
Weekdays	Monday to Friday, 00:00-23:59
Weekends	Saturday and Sunday, 00:00-23:59
WorkingHours	Monday to Friday, 08:00-17:00



Address Filter

Specify source interface and source network, together with destination ir

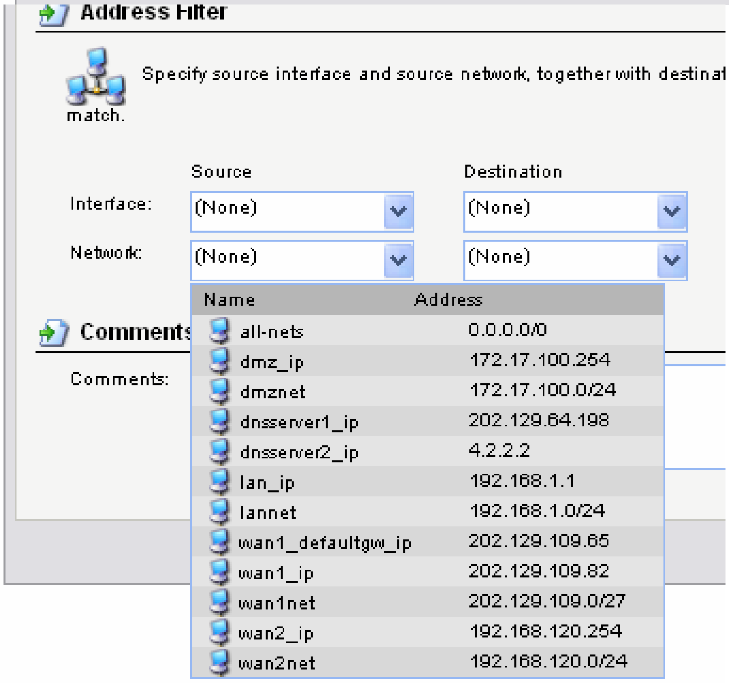
match.

	Source	Destination
Interface:	(None)	(None)
Network:		

Name	Comments
any	
core	
dmz	
lan	
wan1	
wan2	

Comments

Comments:



Address Filter

Specify source interface and source network, together with destinat

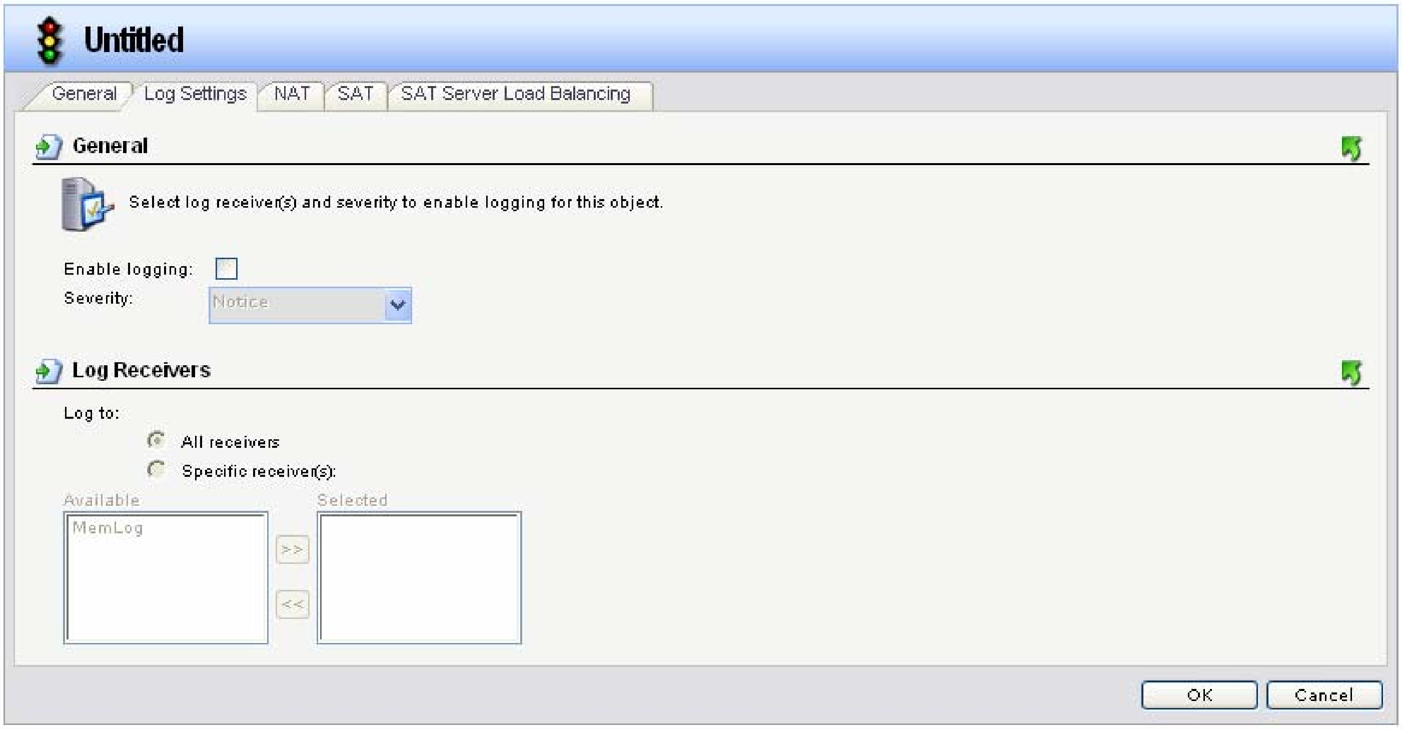
match.

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Name	Address
all-nets	0.0.0.0/0
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
lannet	192.168.1.0/24
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan1net	202.129.109.0/27
wan2_ip	192.168.120.254
wan2net	192.168.120.0/24

Comments

Comments:



General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

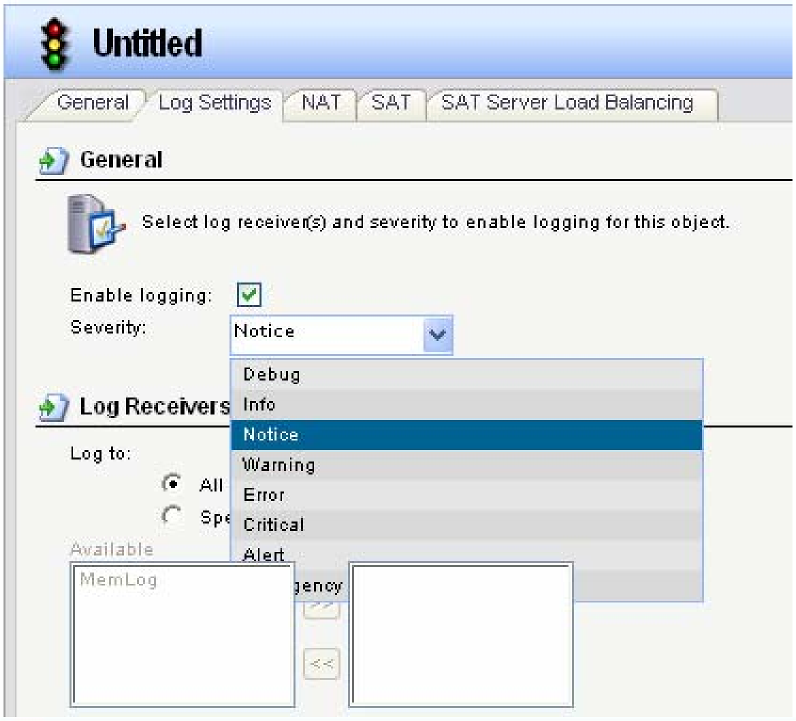
Log Receivers

Log to:

● All receivers

○ Specific receiver(s):

Available	Selected
MemLog	



General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: ☑

Severity: Notice

Log Receivers

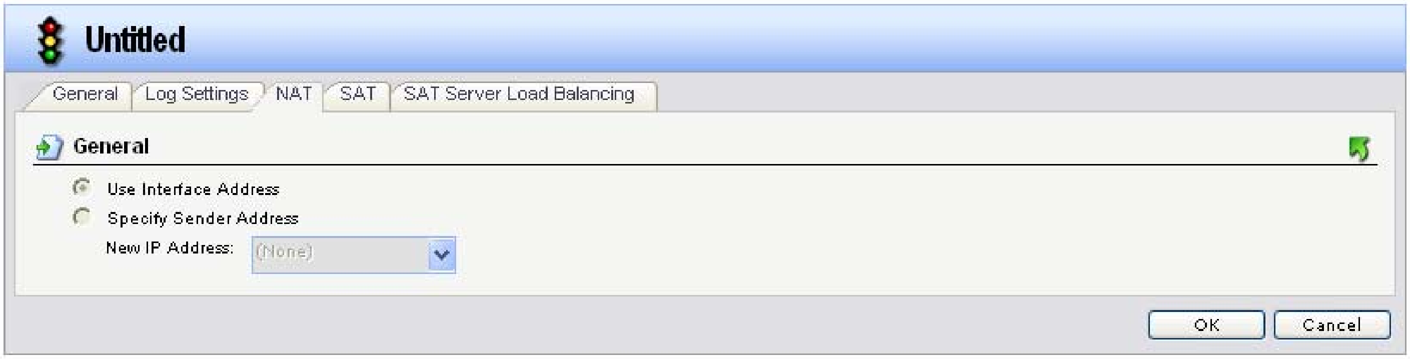
Log to:

● All

○ Spe

Available

MemLog

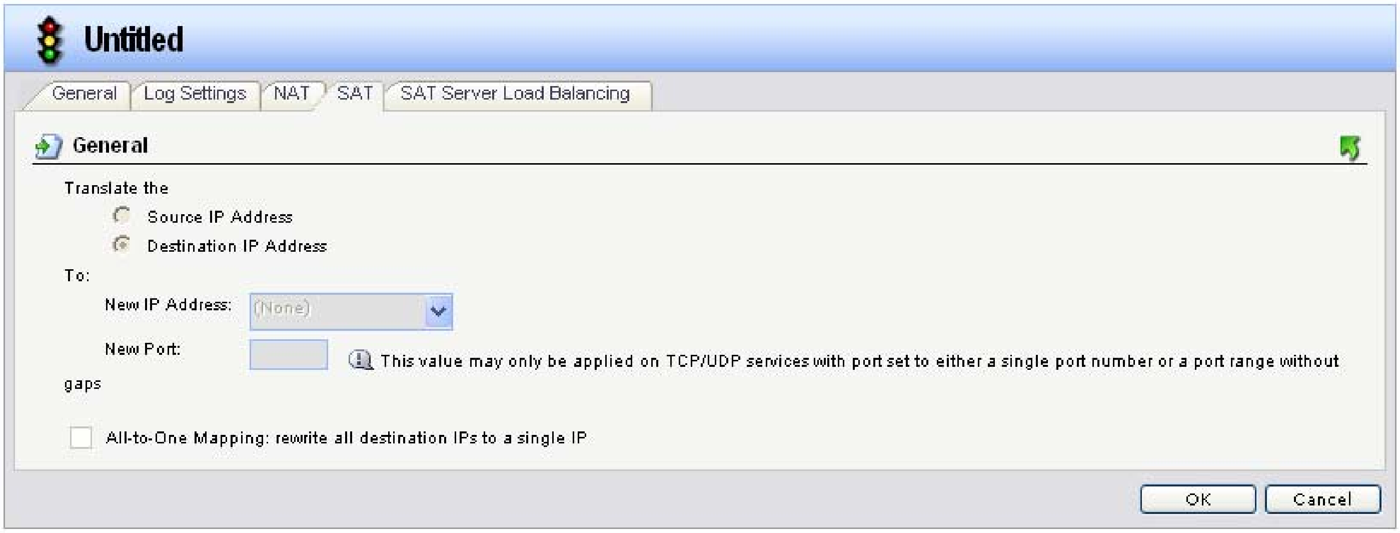


General

● Use Interface Address

○ Specify Sender Address

New IP Address: (None)



General

Translate the

○ Source IP Address

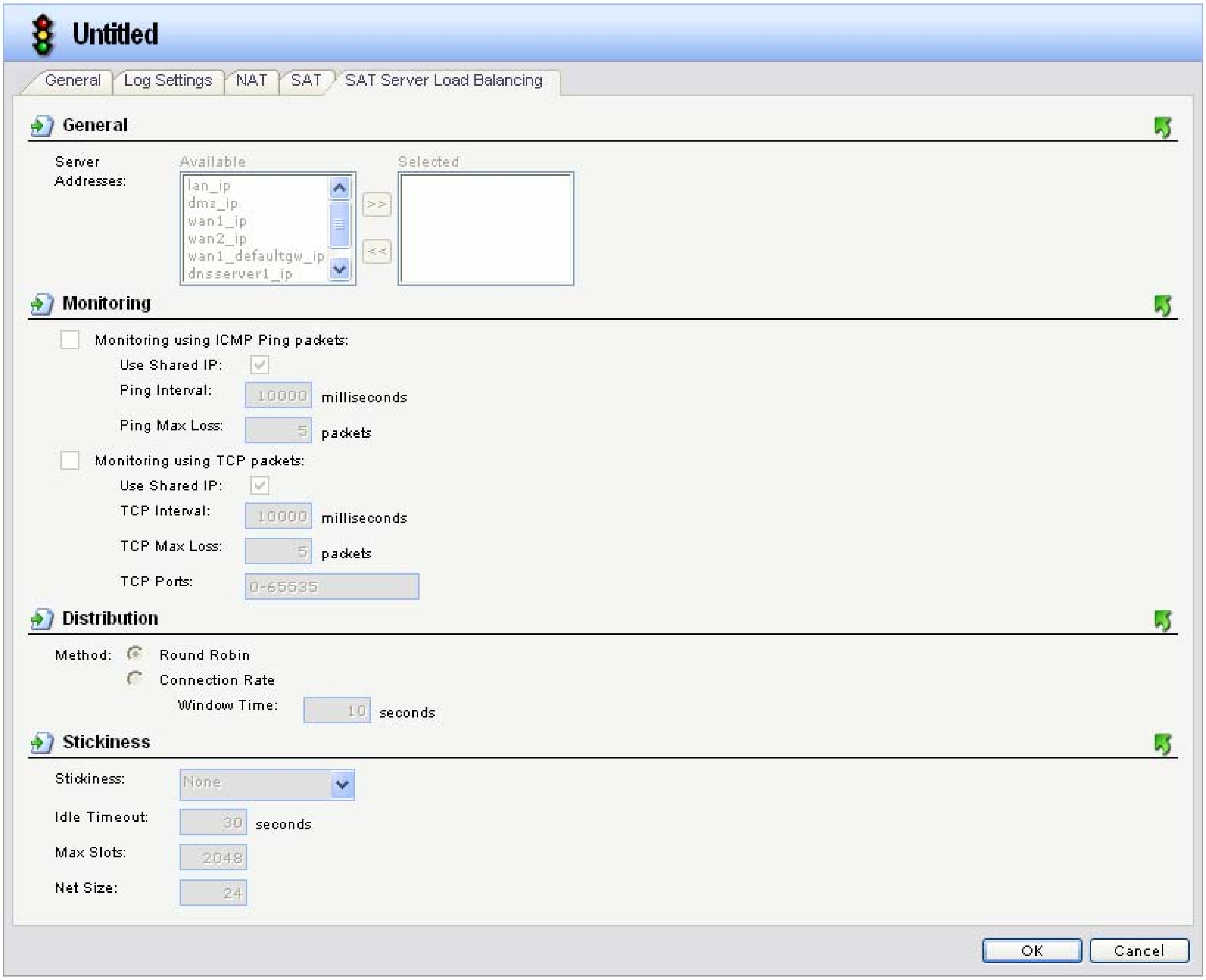
● Destination IP Address

To:

New IP Address: (None)

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



General

Server Addresses:

Available: lan_ip, dmz_ip, wan1_ip, wan2_ip, wan1_defaultgw_ip, dnsserver1_ip

Selected:

Monitoring

□ Monitoring using ICMP Ping packets:

Use Shared IP: ☑

Ping Interval: 10000 milliseconds

Ping Max Loss: 5 packets

□ Monitoring using TCP packets:

Use Shared IP: ☑

TCP Interval: 10000 milliseconds

TCP Max Loss: 5 packets

TCP Ports: 0-65535

Distribution

Method: ● Round Robin

○ Connection Rate

Window Time: 10 seconds

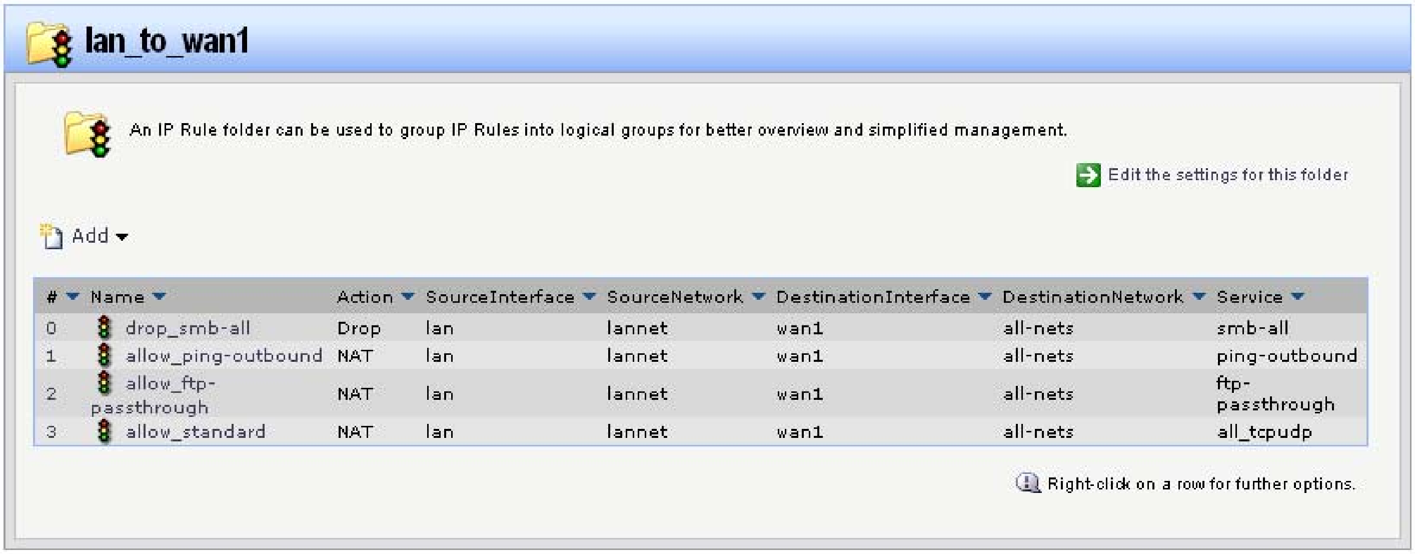
Stickiness

Stickiness: None

Idle Timeout: 30 seconds

Max Slots: 2048

Net Size: 24

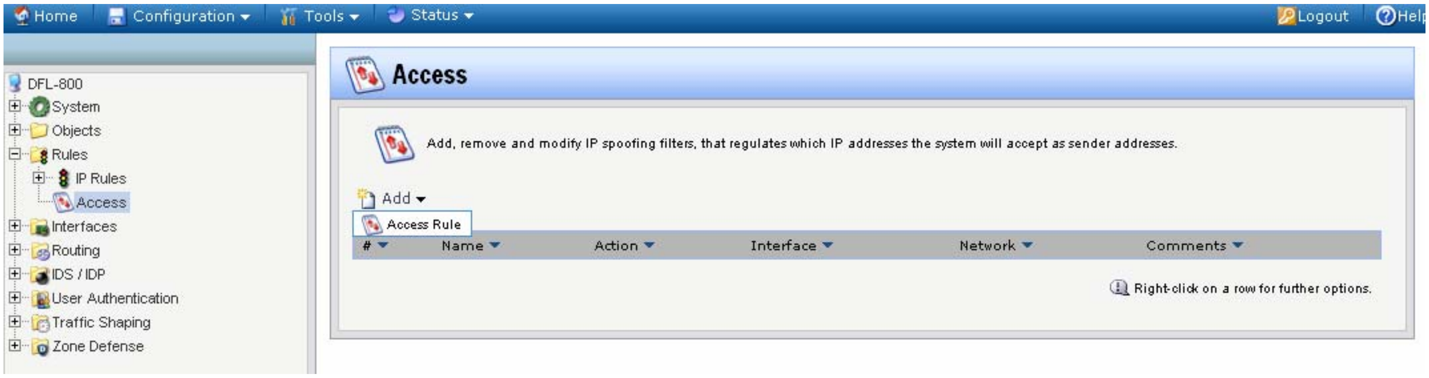


lan_to_wan1

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

#	Name	Action	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service
0	drop_smb-all	Drop	lan	lannet	wan1	all-nets	smb-all
1	allow_ping-outbound	NAT	lan	lannet	wan1	all-nets	ping-outbound
2	allow_ftp-passthrough	NAT	lan	lannet	wan1	all-nets	ftp-passthrough
3	allow_standard	NAT	lan	lannet	wan1	all-nets	all_tcpudp

Right-click on a row for further options.

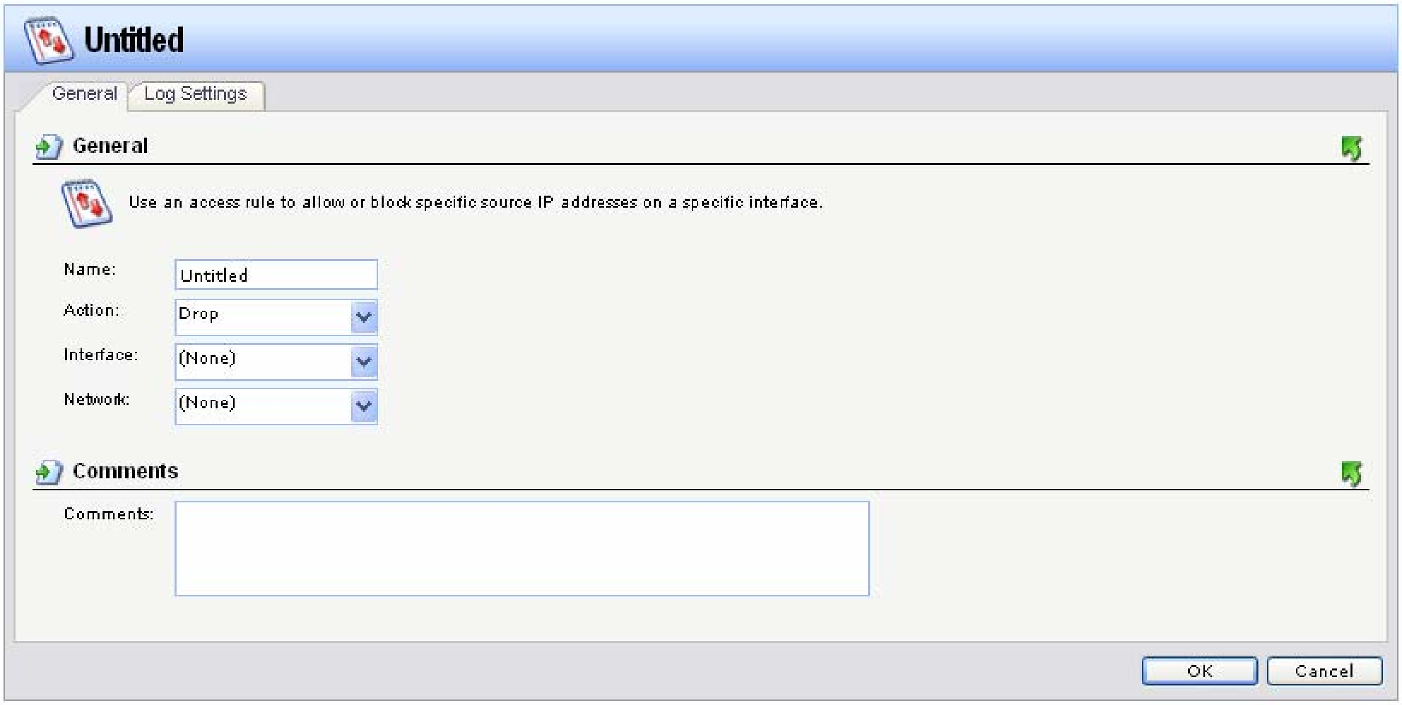


Access

Add, remove and modify IP spoofing filters, that regulates which IP addresses the system will accept as sender addresses.

#	Name	Action	Interface	Network	Comments

Right-click on a row for further options.



Untitled

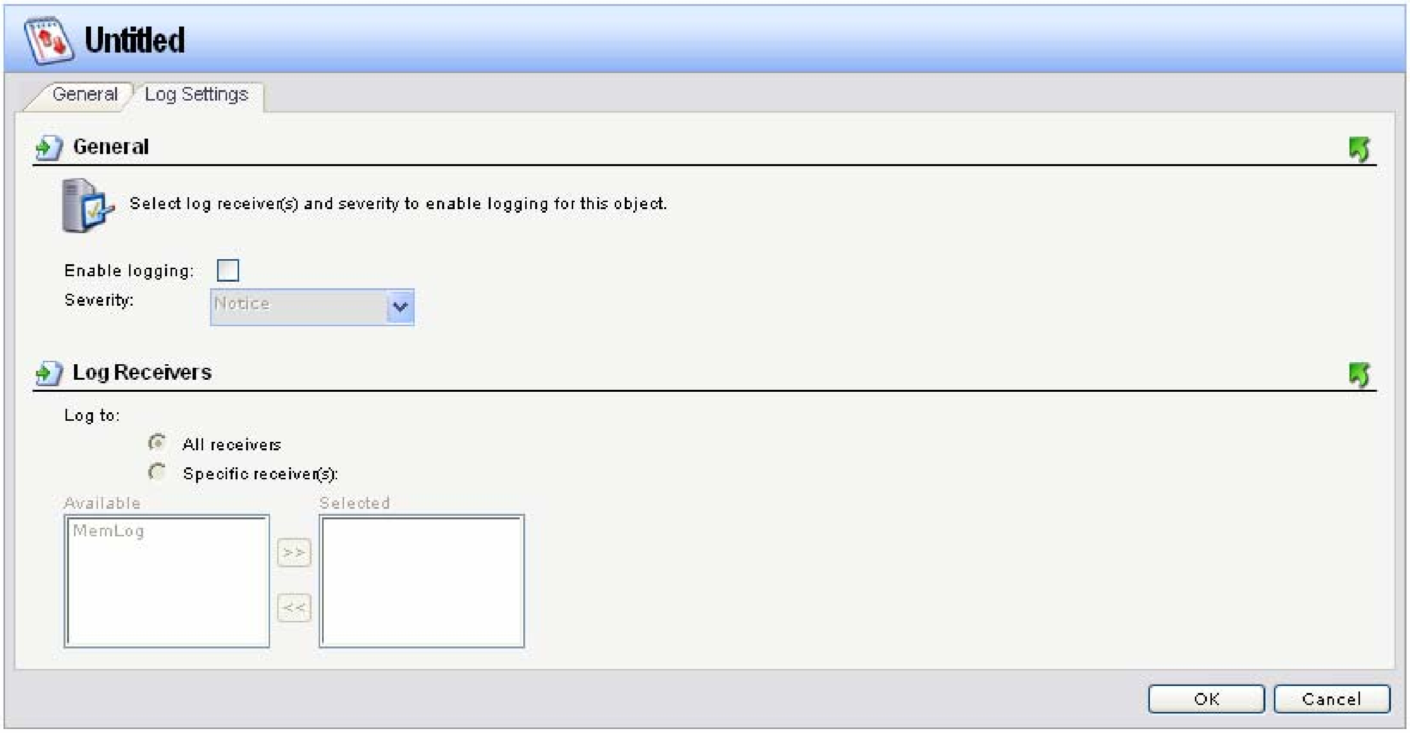
General

Use an access rule to allow or block specific source IP addresses on a specific interface.

Name:	Untitled
Action:	Drop
Interface:	(None)
Network:	(None)

Comments

Comments:



General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

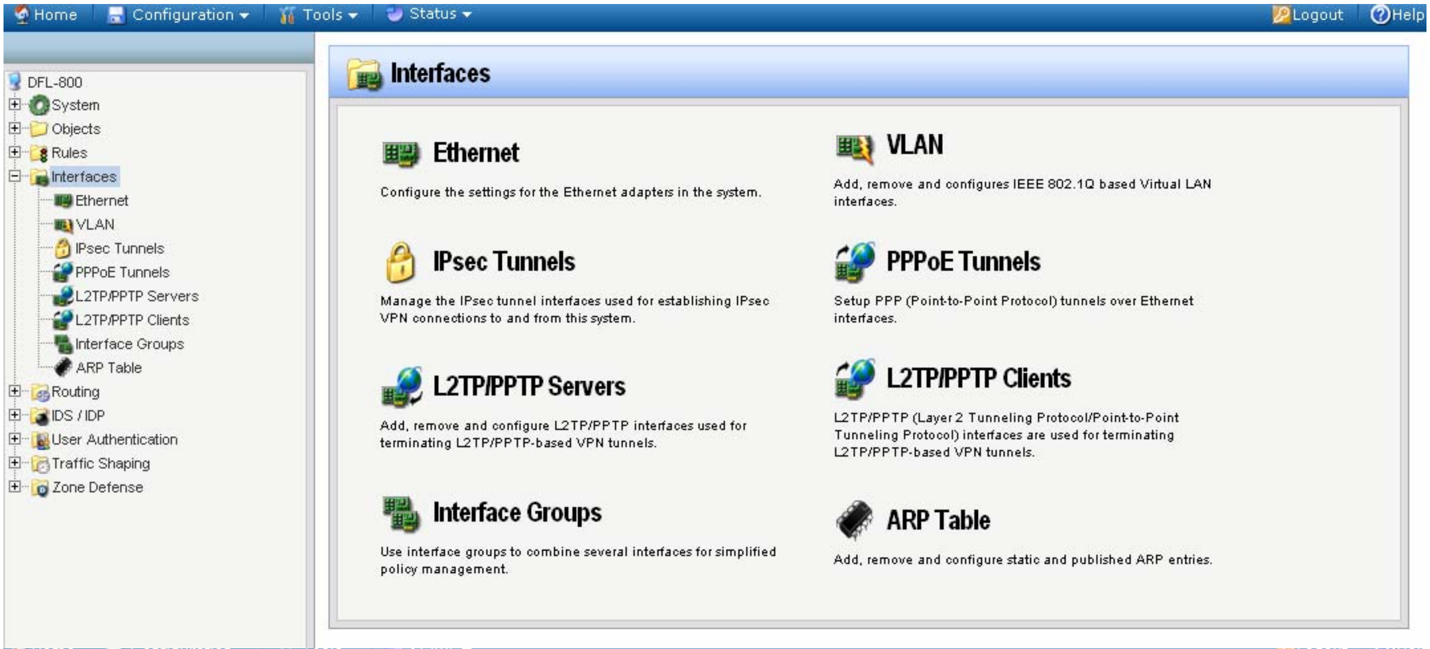
Log Receivers

Log to:

● All receivers

○ Specific receiver(s):

Available	Selected
MemLog	



Interfaces

Ethernet

Configure the settings for the Ethernet adapters in the system.

VLAN

Add, remove and configures IEEE 802.1Q based Virtual LAN interfaces.

IPsec Tunnels

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

PPPoE Tunnels

Setup PPP (Point-to-Point Protocol) tunnels over Ethernet interfaces.

L2TP/PPTP Servers

Add, remove and configure L2TP/PPTP interfaces used for terminating L2TP/PPTP-based VPN tunnels.

L2TP/PPTP Clients

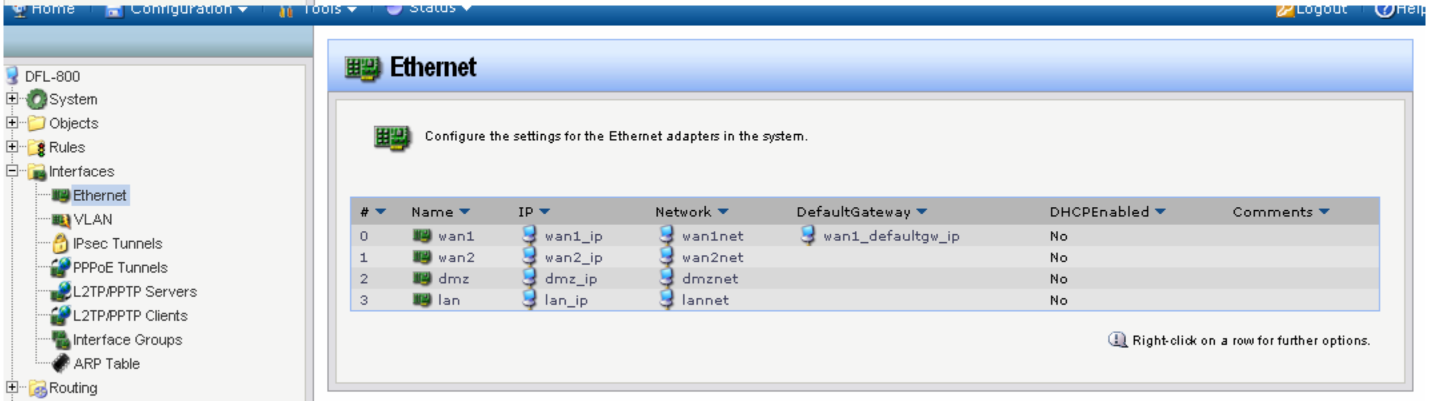
L2TP/PPTP (Layer 2 Tunneling Protocol/Point-to-Point Tunneling Protocol) interfaces are used for terminating L2TP/PPTP-based VPN tunnels.

Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

ARP Table

Add, remove and configure static and published ARP entries.

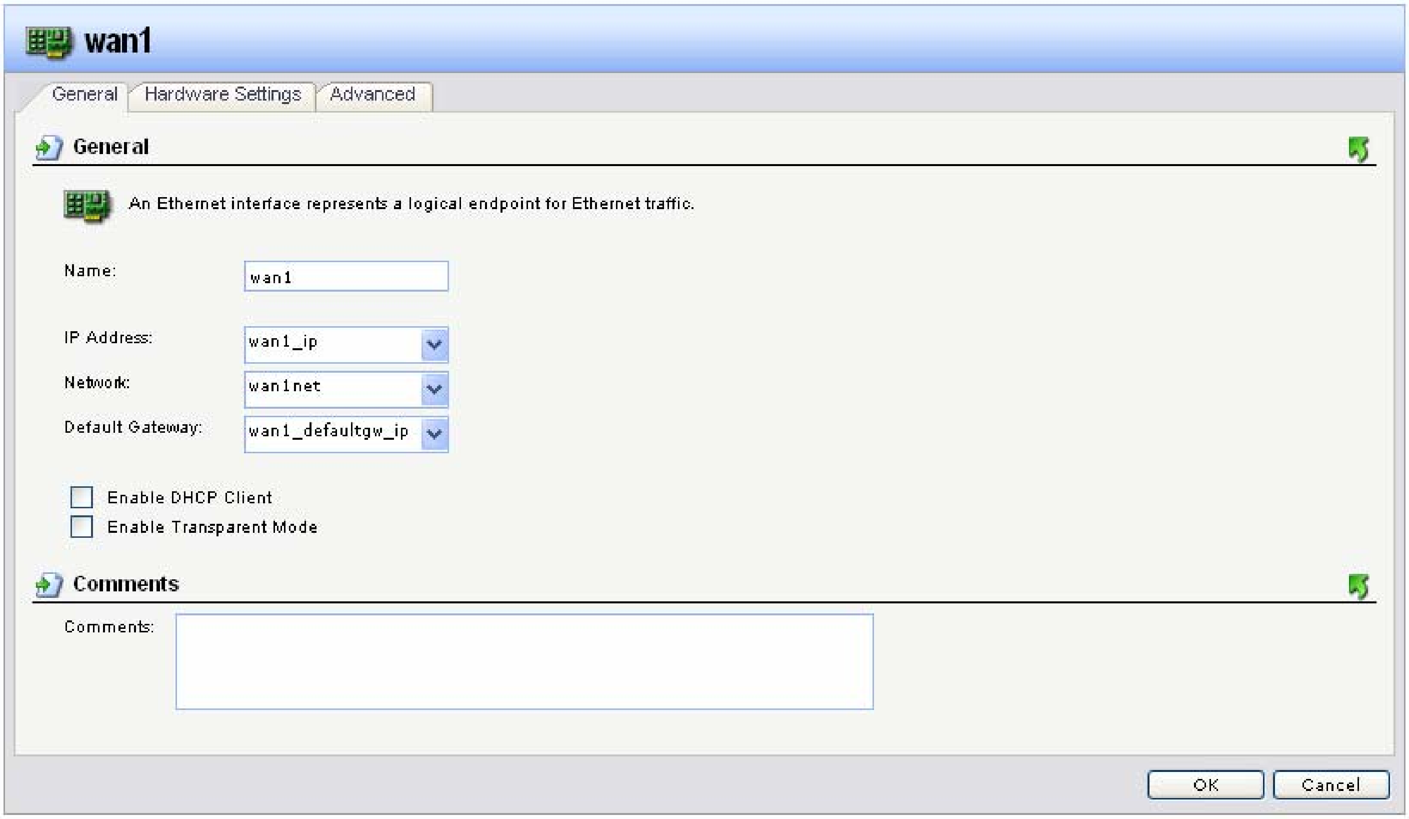


Ethernet

Configure the settings for the Ethernet adapters in the system.

#	Name	IP	Network	DefaultGateway	DHCPEnabled	Comments
0	wan1	wan1_ip	wan1net	wan1_defaultgw_ip	No	
1	wan2	wan2_ip	wan2net		No	
2	dmz	dmz_ip	dmznet		No	
3	lan	lan_ip	lannet		No	

Right-click on a row for further options.



An Ethernet interface represents a logical endpoint for Ethernet traffic.

Name: wan1

IP Address: wan1_ip

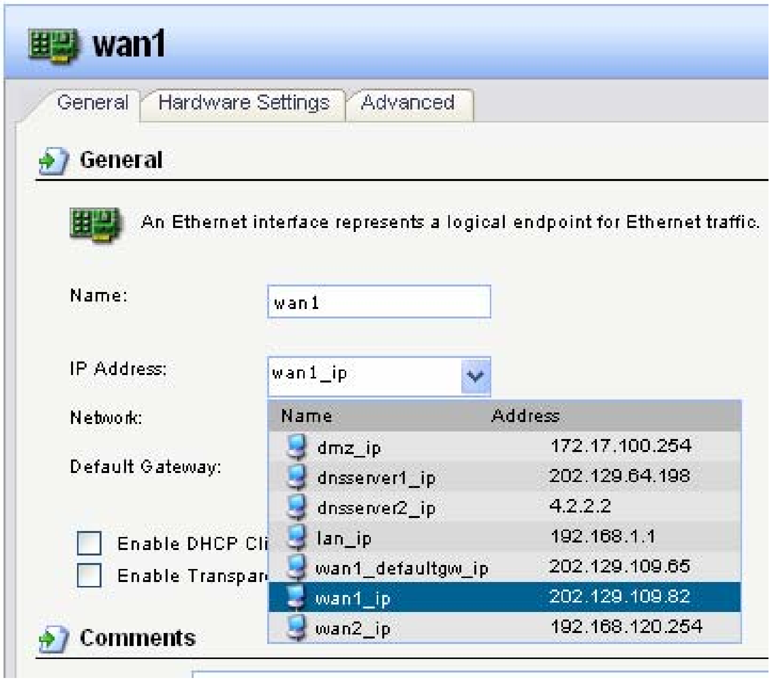
Network: wan1net

Default Gateway: wan1_defaultgw_ip

□ Enable DHCP Client

□ Enable Transparent Mode

Comments:

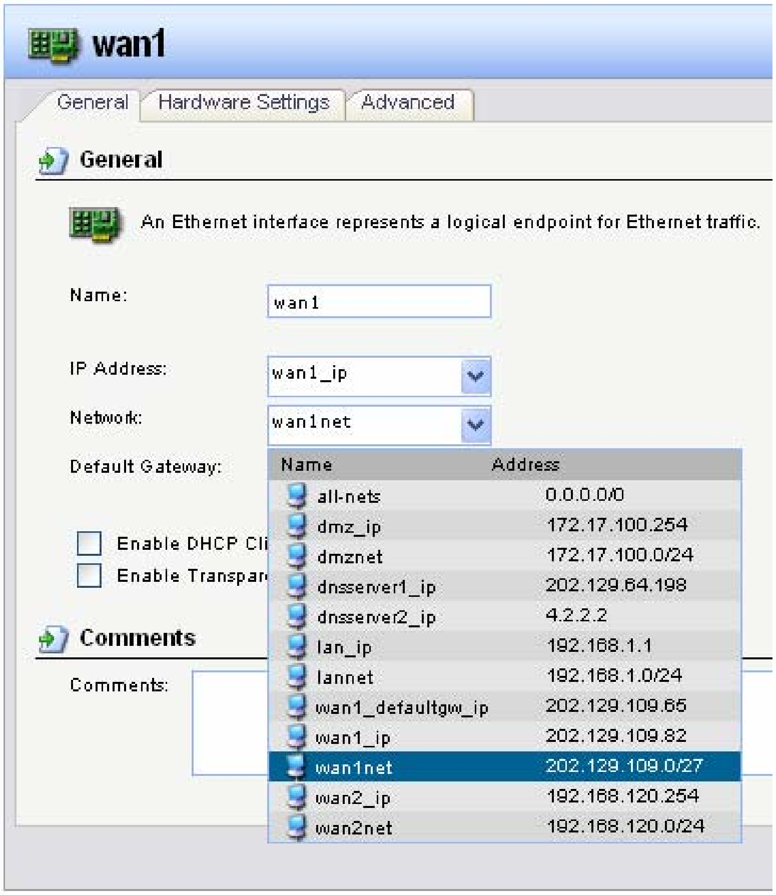


An Ethernet interface represents a logical endpoint for Ethernet traffic.

Name: wan1

IP Address: wan1_ip

Name	Address
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254



wan1

General

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Name: wan1

IP Address: wan1_ip

Network: wan1net

Default Gateway:

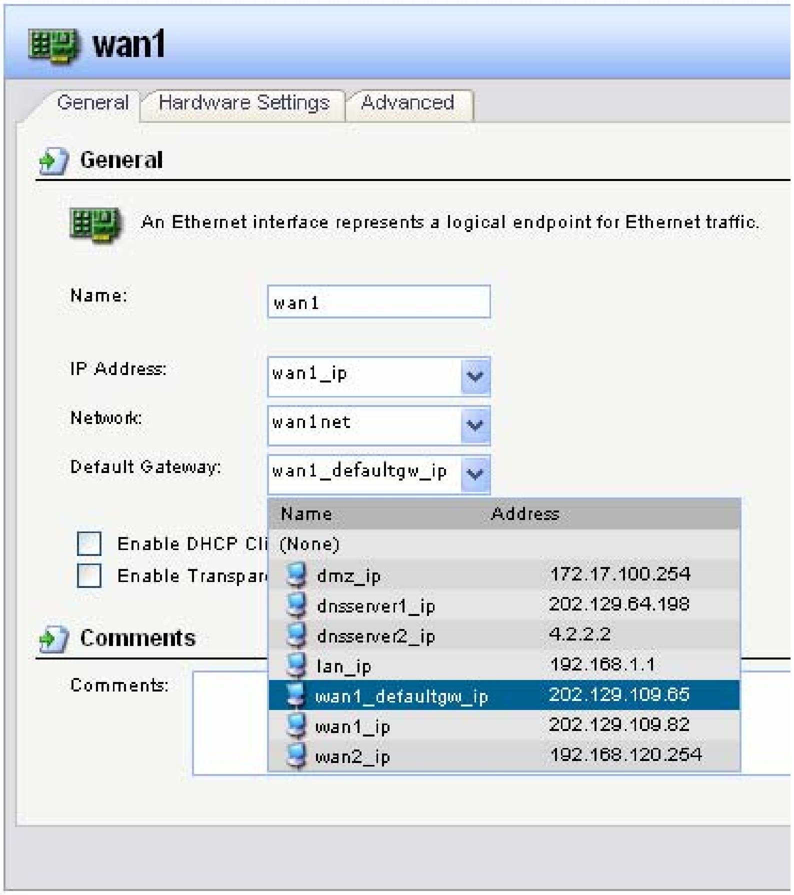
Name	Address
all-nets	0.0.0.0/0
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
lannet	192.168.1.0/24
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan1net	202.129.109.0/27
wan2_ip	192.168.120.254
wan2net	192.168.120.0/24

□ Enable DHCP Cli

□ Enable Transpar

Comments

Comments:



wan1

General

An Ethernet interface represents a logical endpoint for Ethernet traffic.

Name: wan1

IP Address: wan1_ip

Network: wan1net

Default Gateway: wan1_defaultgw_ip

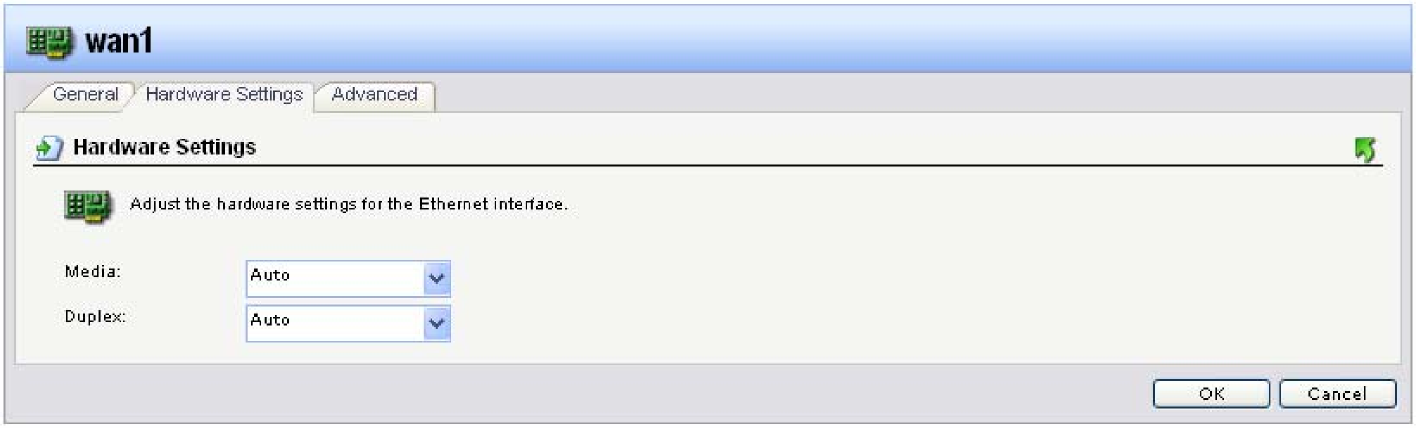
Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254

□ Enable DHCP Cli

□ Enable Transpar

Comments

Comments:



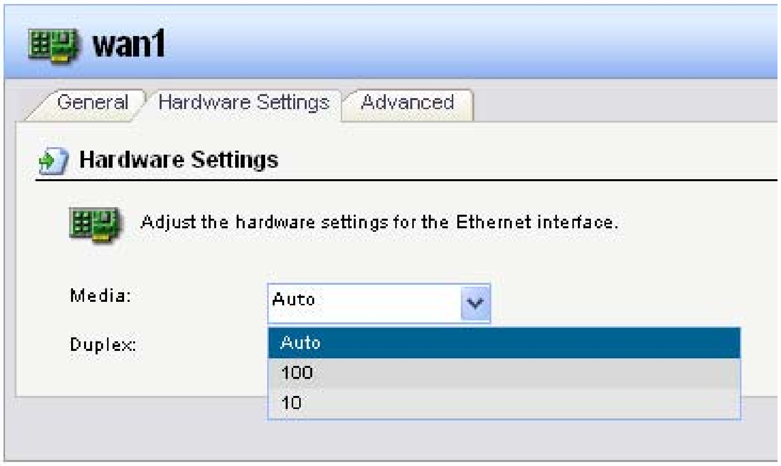
wan1

Hardware Settings

Adjust the hardware settings for the Ethernet interface.

Media: Auto

Duplex: Auto



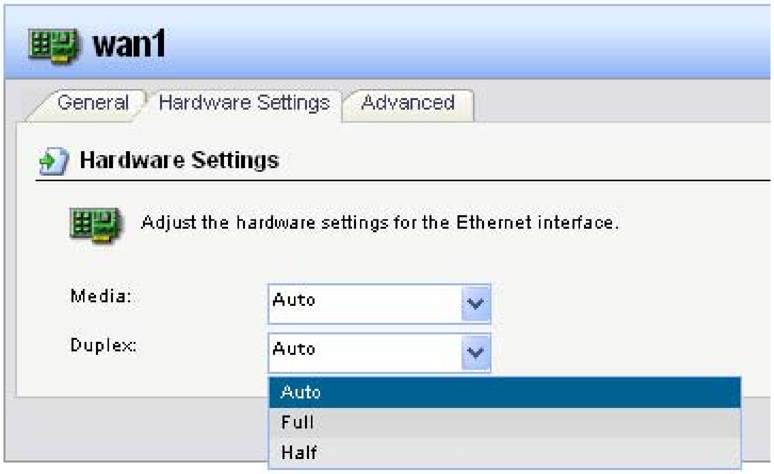
wan1

Hardware Settings

Adjust the hardware settings for the Ethernet interface.

Media: Auto

Duplex:



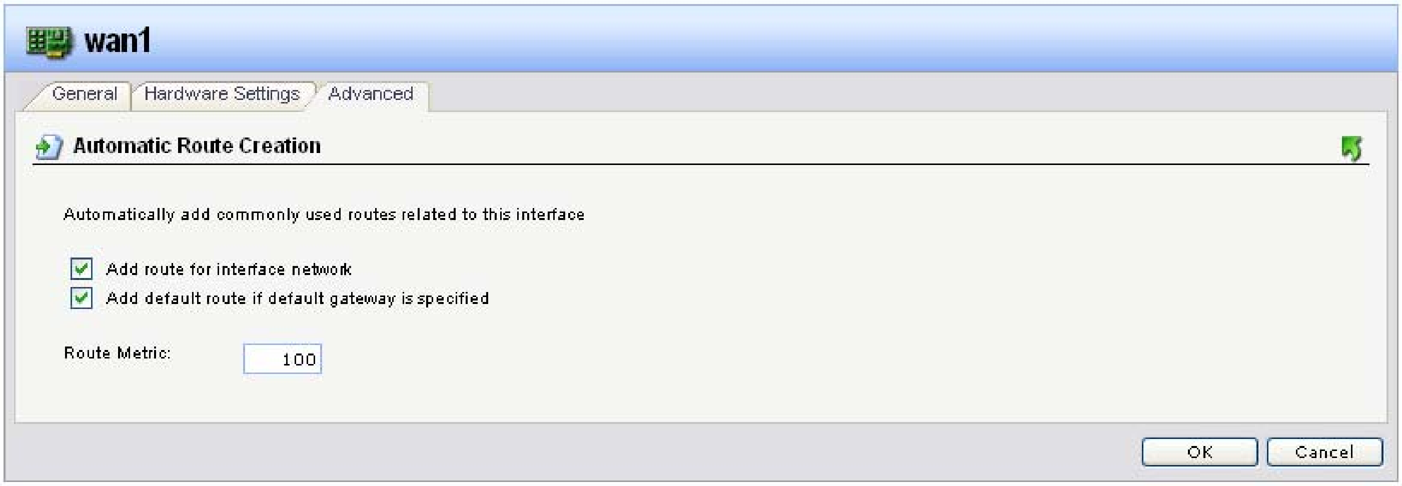
wan1

Hardware Settings

Adjust the hardware settings for the Ethernet interface.

Media: Auto

Duplex: Auto



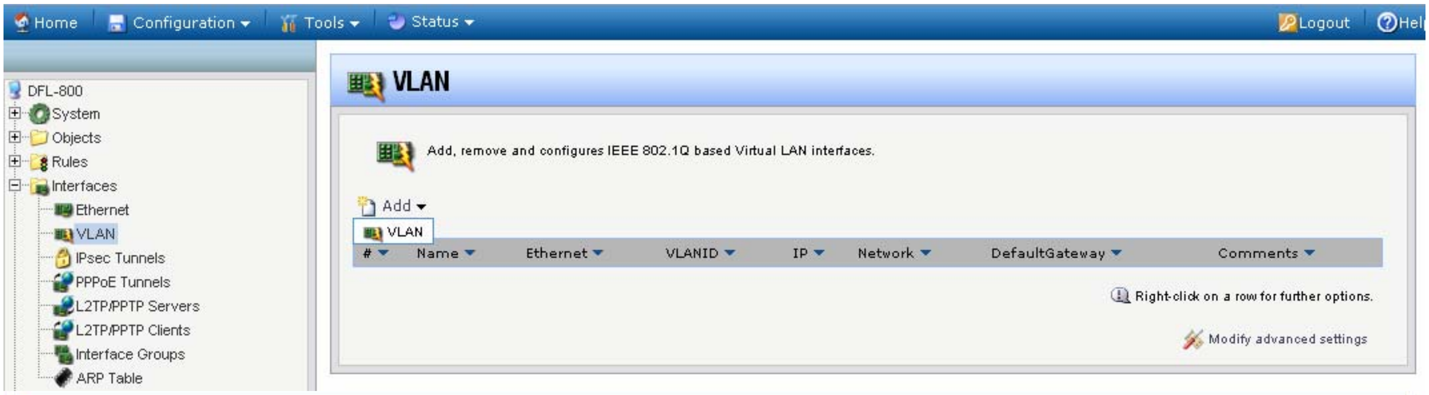
Automatic Route Creation

Automatically add commonly used routes related to this interface

☑ Add route for interface network

☑ Add default route if default gateway is specified

Route Metric: 100

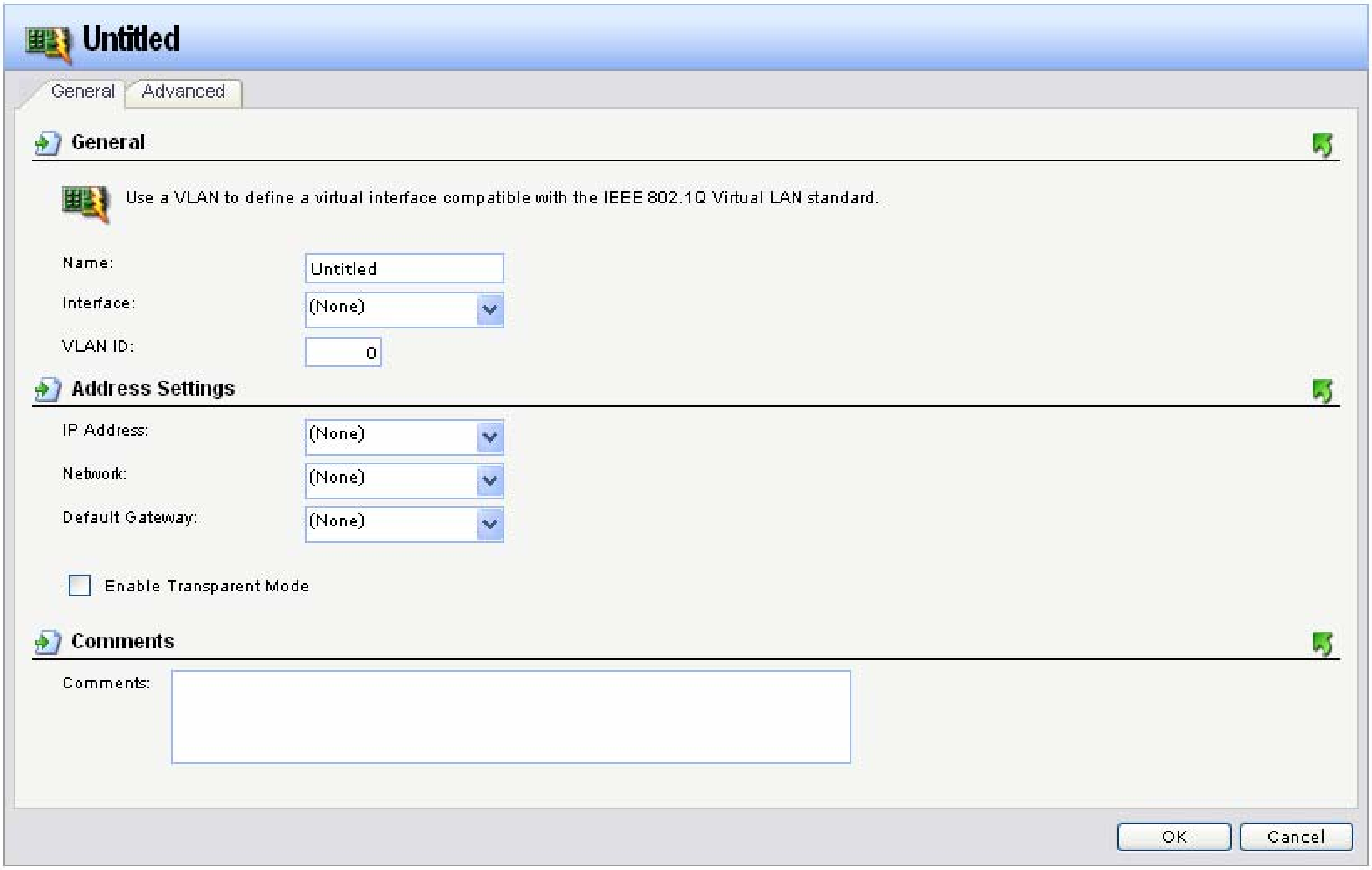


VLAN

Add, remove and configures IEEE 802.1Q based Virtual LAN interfaces.

#	Name	Ethernet	VLANID	IP	Network	DefaultGateway	Comments

Right-click on a row for futher options.



General

Use a VLAN to define a virtual interface compatible with the IEEE 802.1Q Virtual LAN standard.

Name: Untitled

Interface: (None)

VLAN ID: 0

Address Settings

IP Address: (None)

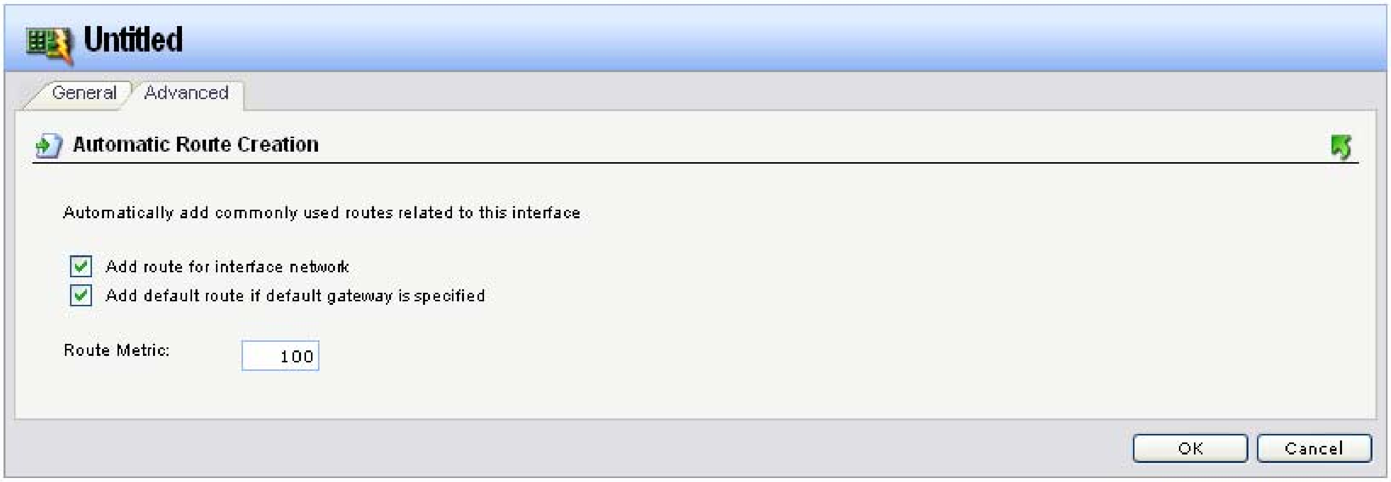
Network: (None)

Default Gateway: (None)

□ Enable Transparent Mode

Comments

Comments:



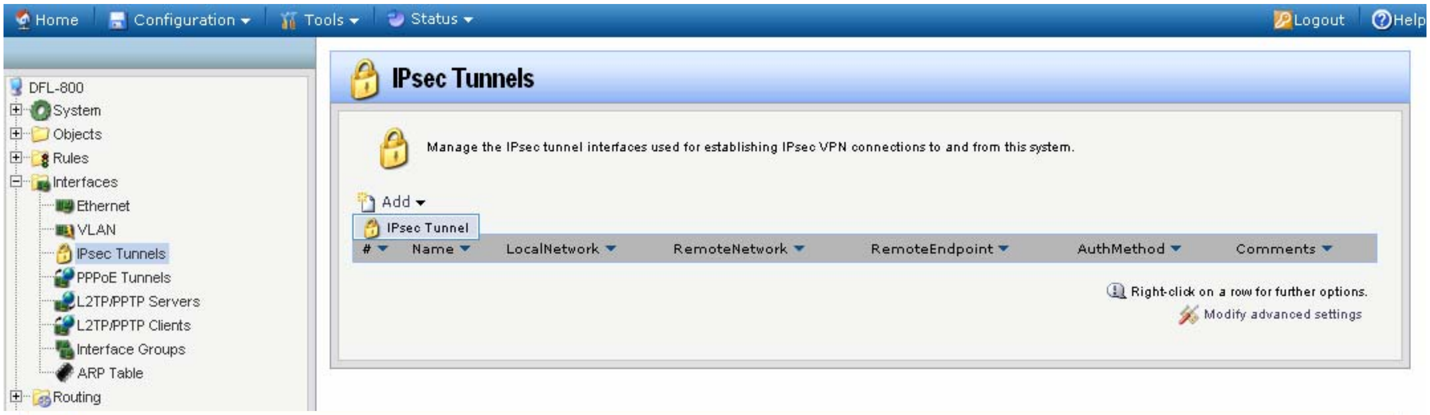
Automatic Route Creation

Automatically add commonly used routes related to this interface

☑ Add route for interface network

☑ Add default route if default gateway is specified

Route Metric: 100



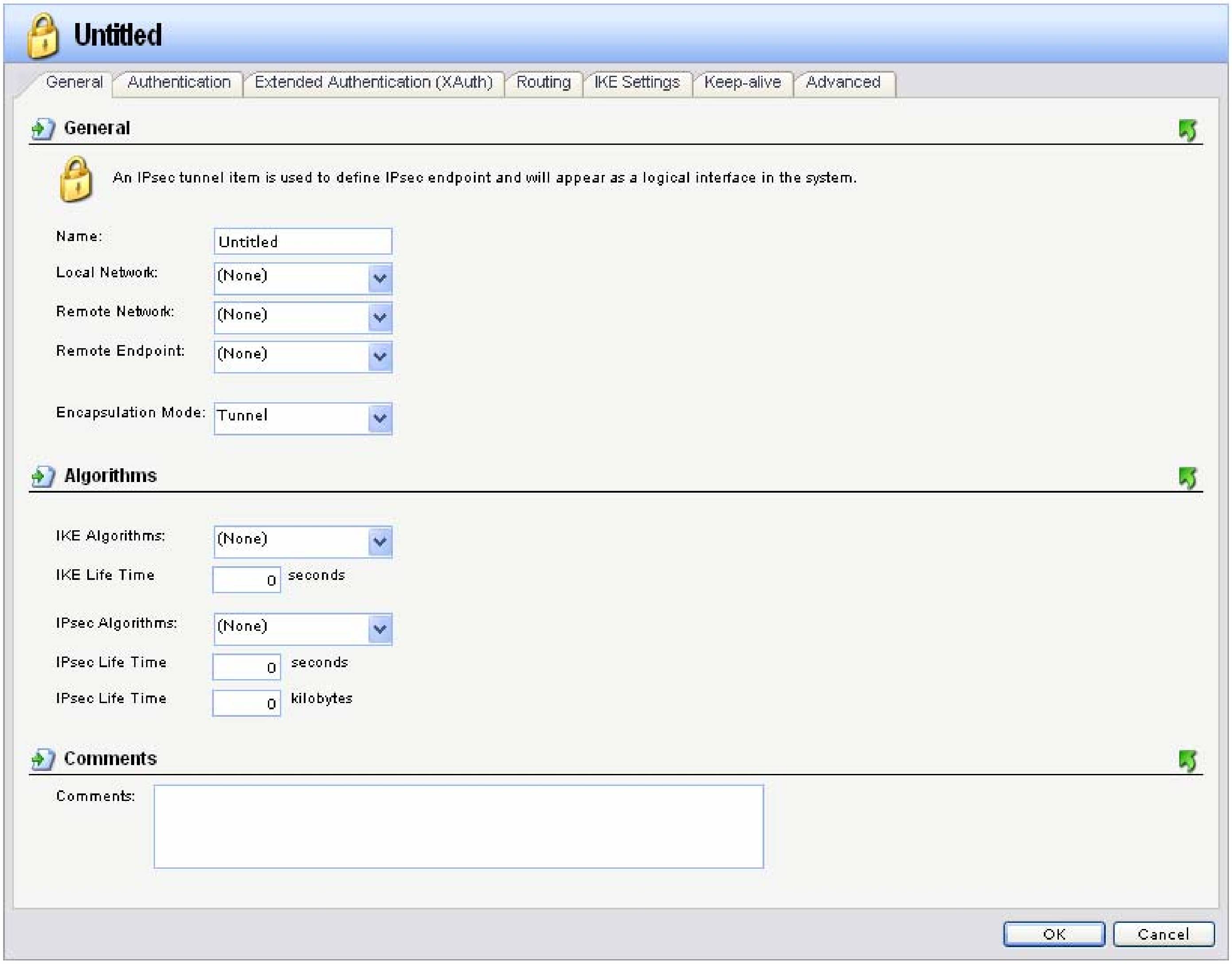
IPsec Tunnels

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	LocalNetwork	RemoteNetwork	RemoteEndpoint	AuthMethod	Comments

Right-click on a row for further options.

Modify advanced settings



General

An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

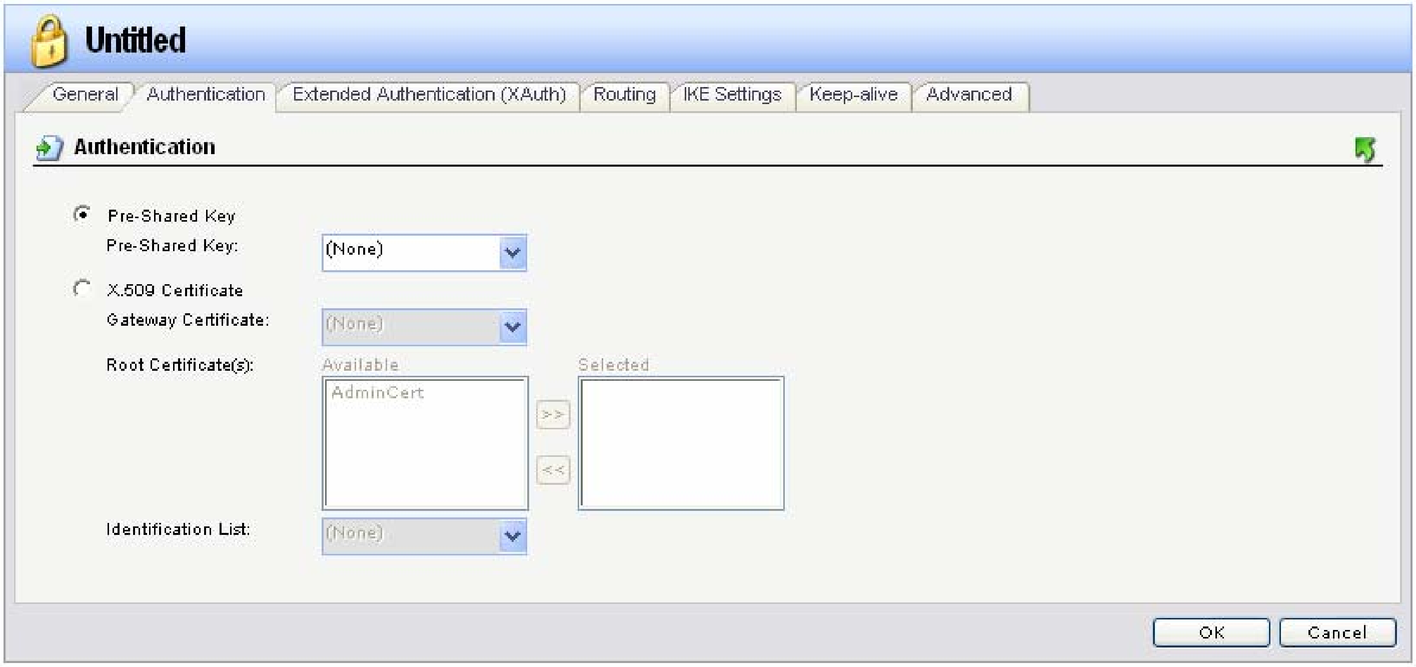
Name:	Untitled
Local Network:	(None)
Remote Network:	(None)
Remote Endpoint:	(None)
Encapsulation Mode:	Tunnel

Algorithms

IKE Algorithms:	(None)
IKE Life Time	0 seconds
IPsec Algorithms:	(None)
IPsec Life Time	0 seconds
IPsec Life Time	0 kilobytes

Comments

Comments:



Authentication

● Pre-Shared Key

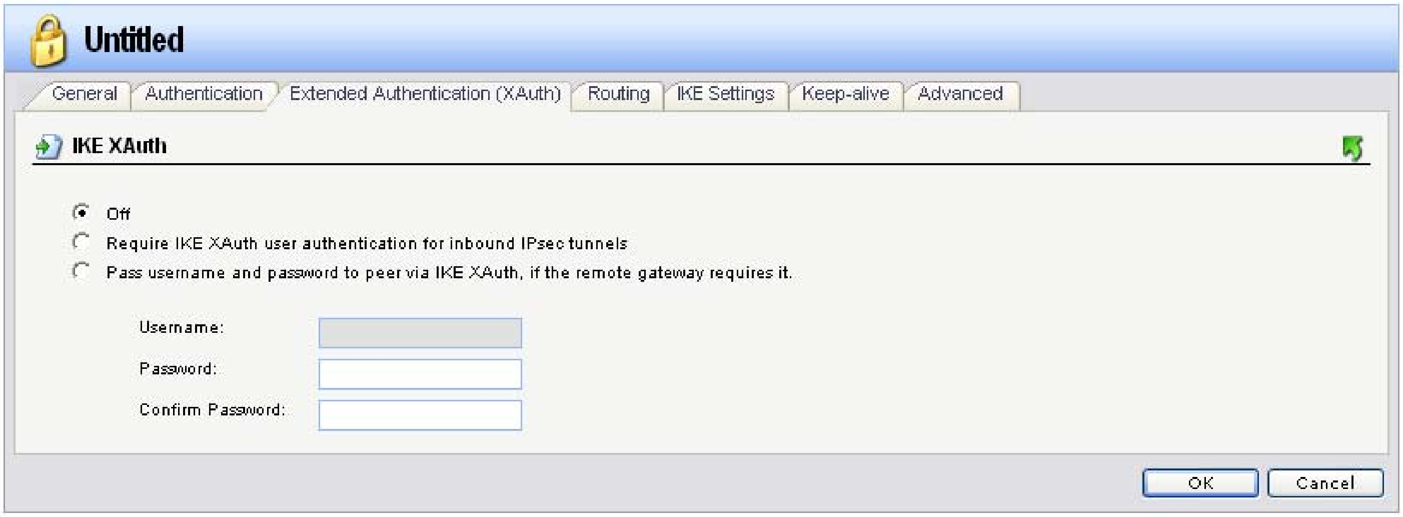
Pre-Shared Key: (None)

○ X.509 Certificate

Gateway Certificate: (None)

Root Certificate(s): Available: AdminCert — Selected:

Identification List: (None)



IKE XAuth

● Off

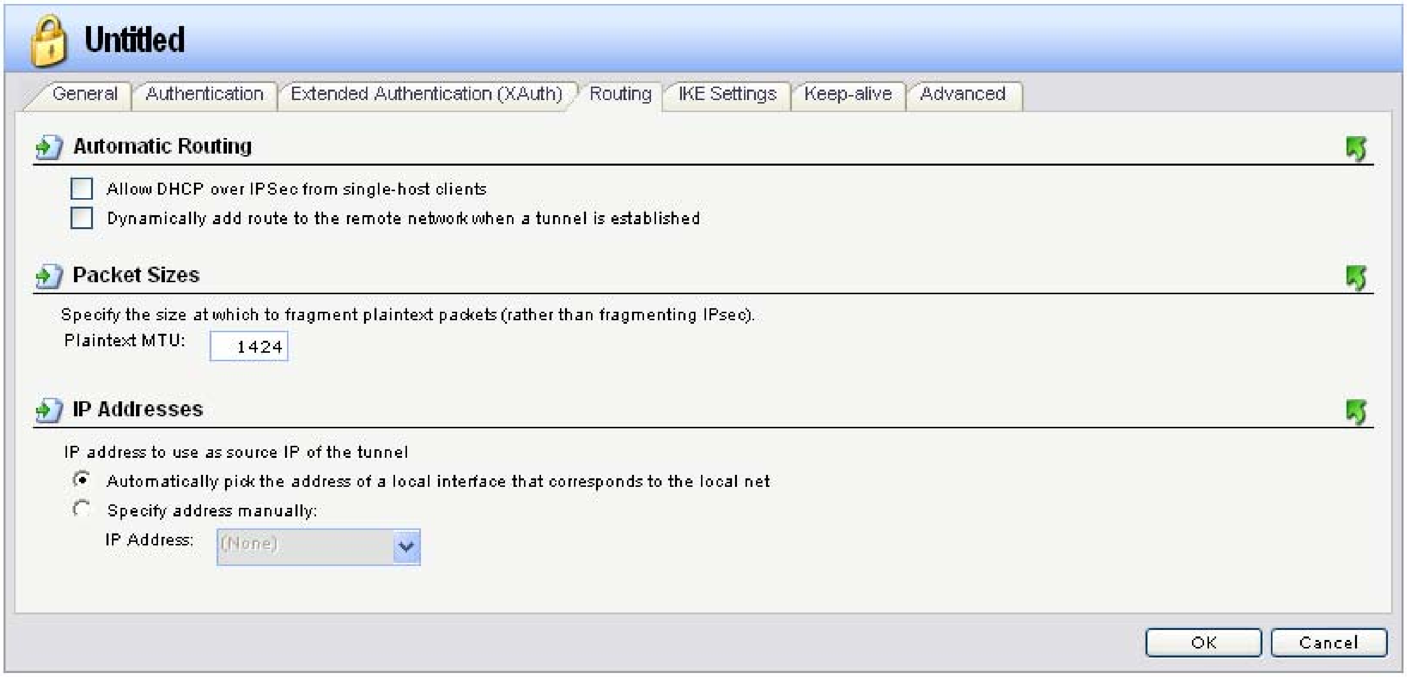
○ Require IKE XAuth user authentication for inbound IPsec tunnels

○ Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

Username:

Password:

Confirm Password:



Automatic Routing

□ Allow DHCP over IPSec from single-host clients

□ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1424

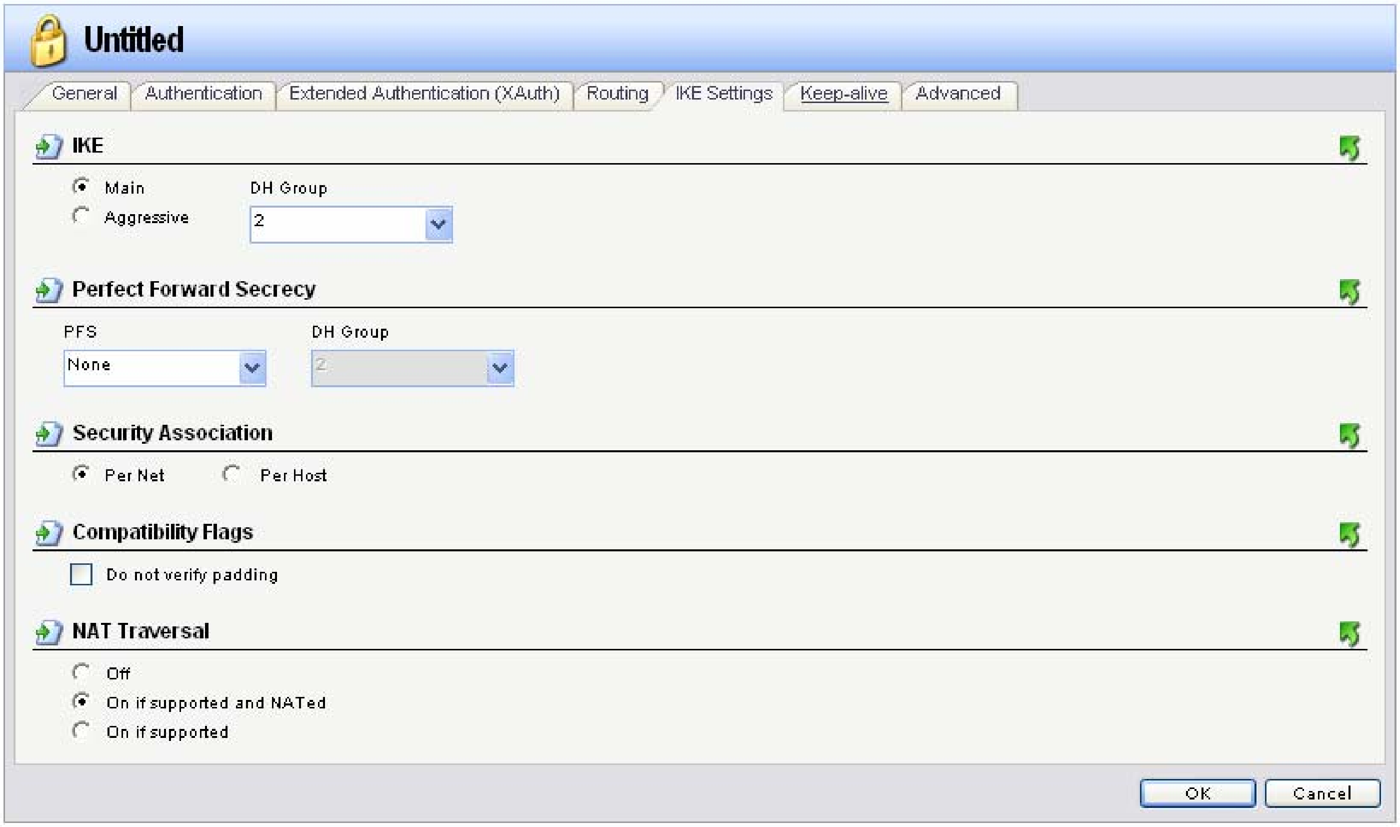
IP Addresses

IP address to use as source IP of the tunnel

● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)



Untitled
General | Authentication | Extended Authentication (XAuth) | Routing | IKE Settings | Keep-alive | Advanced

IKE

● Main ○ Aggressive

DH Group: 2

Perfect Forward Secrecy

PFS: None

DH Group: 2

Security Association

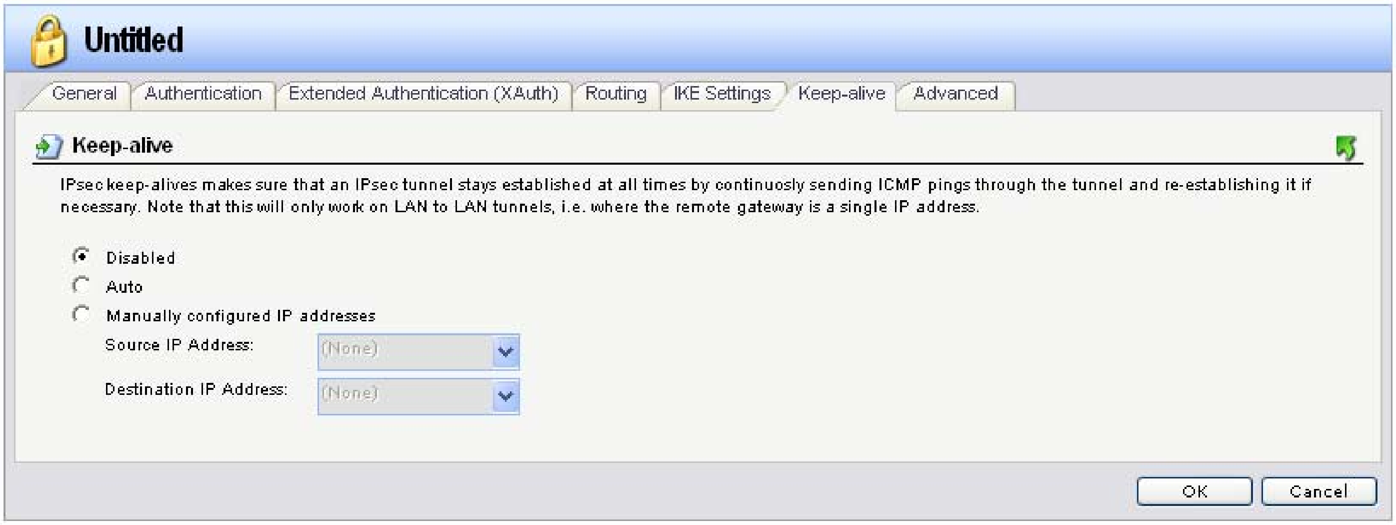
● Per Net ○ Per Host

Compatibility Flags

□ Do not verify padding

NAT Traversal

○ Off
● On if supported and NATed
○ On if supported



Untitled
General | Authentication | Extended Authentication (XAuth) | Routing | IKE Settings | Keep-alive | Advanced

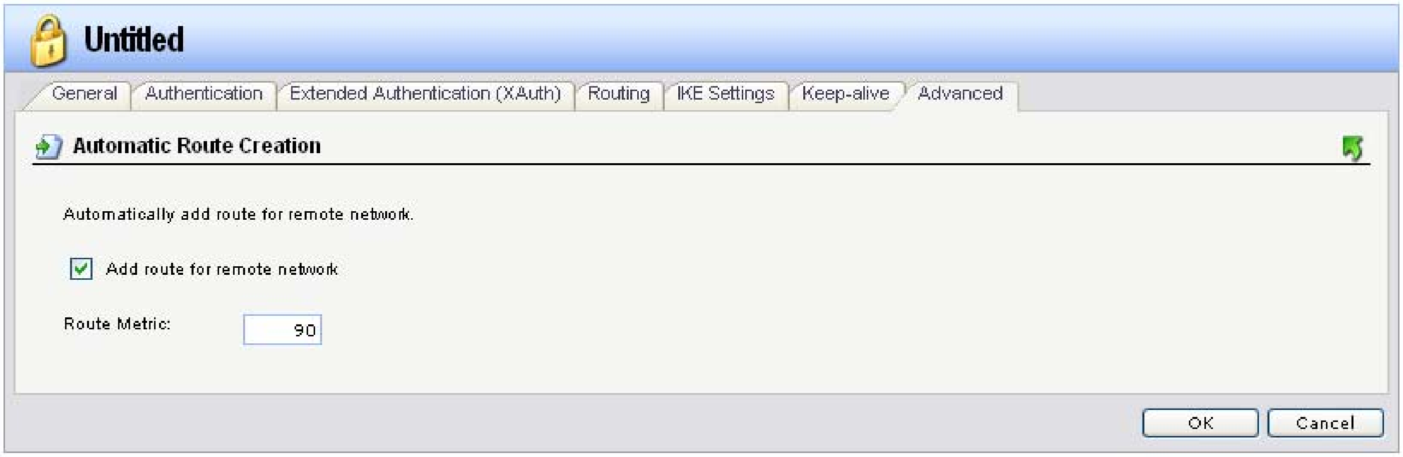
Keep-alive

IPsec keep-alives makes sure that an IPsec tunnel stays established at all times by continuosly sending ICMP pings through the tunnel and re-establishing it if necessary. Note that this will only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP address.

● Disabled
○ Auto
○ Manually configured IP addresses

Source IP Address: (None)

Destination IP Address: (None)



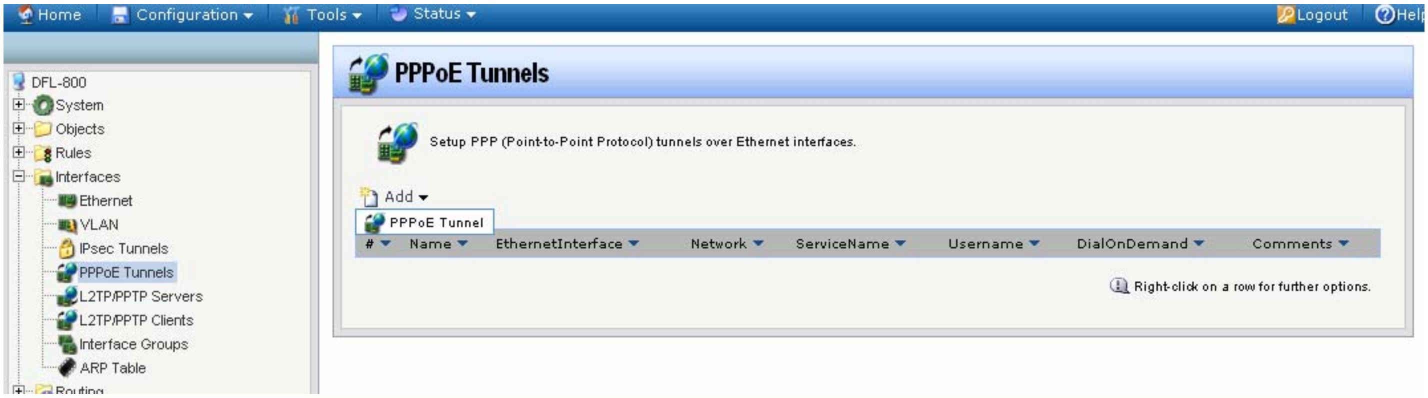
Untitled
General | Authentication | Extended Authentication (XAuth) | Routing | IKE Settings | Keep-alive | Advanced

Automatic Route Creation

Automatically add route for remote network.

☑ Add route for remote network

Route Metric: 90

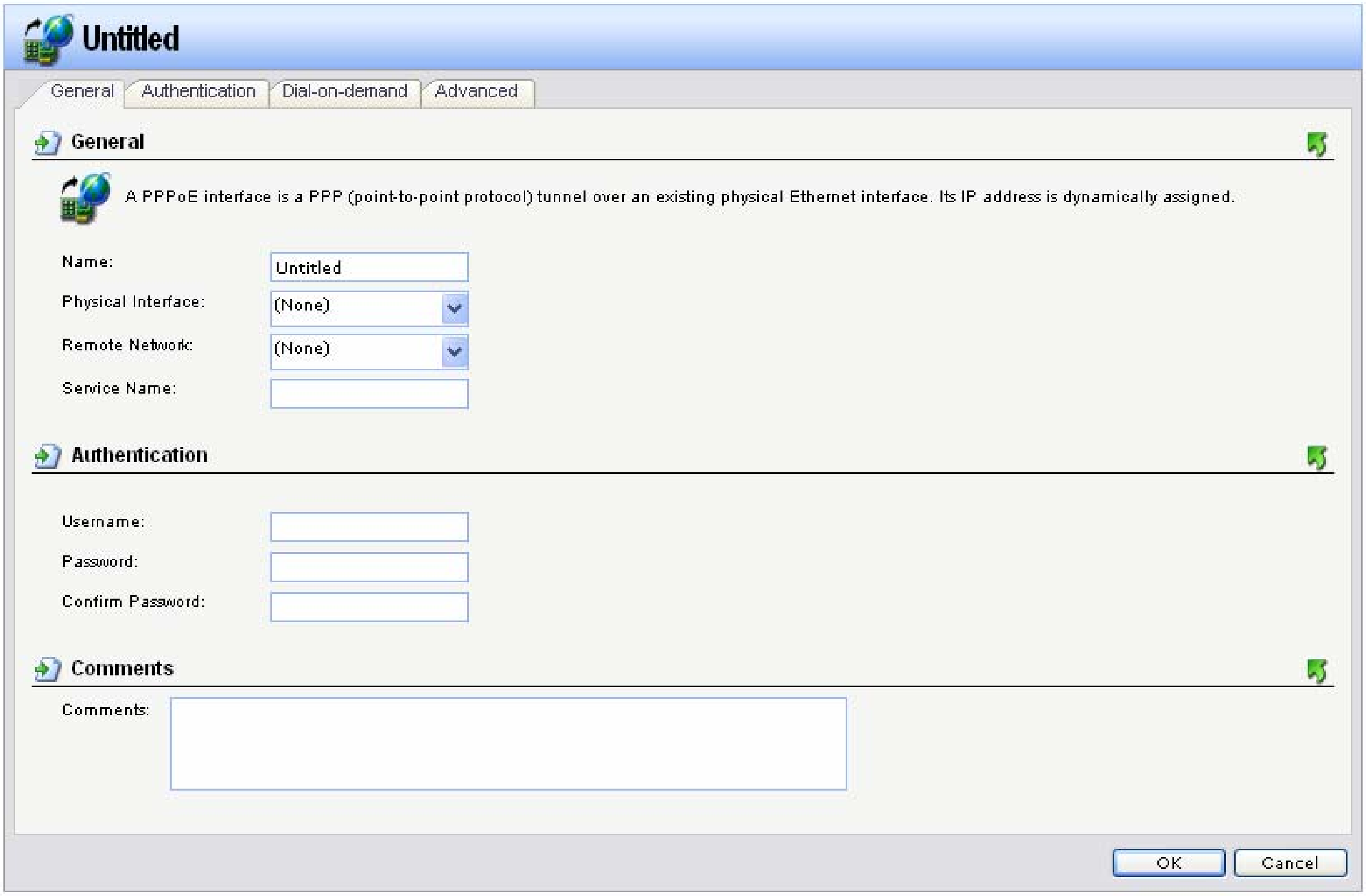


PPPoE Tunnels

Setup PPP (Point-to-Point Protocol) tunnels over Ethernet interfaces.

#	Name	EthernetInterface	Network	ServiceName	Username	DialOnDemand	Comments

Right-click on a row for further options.



Untitled

General

A PPPoE interface is a PPP (point-to-point protocol) tunnel over an existing physical Ethernet interface. Its IP address is dynamically assigned.

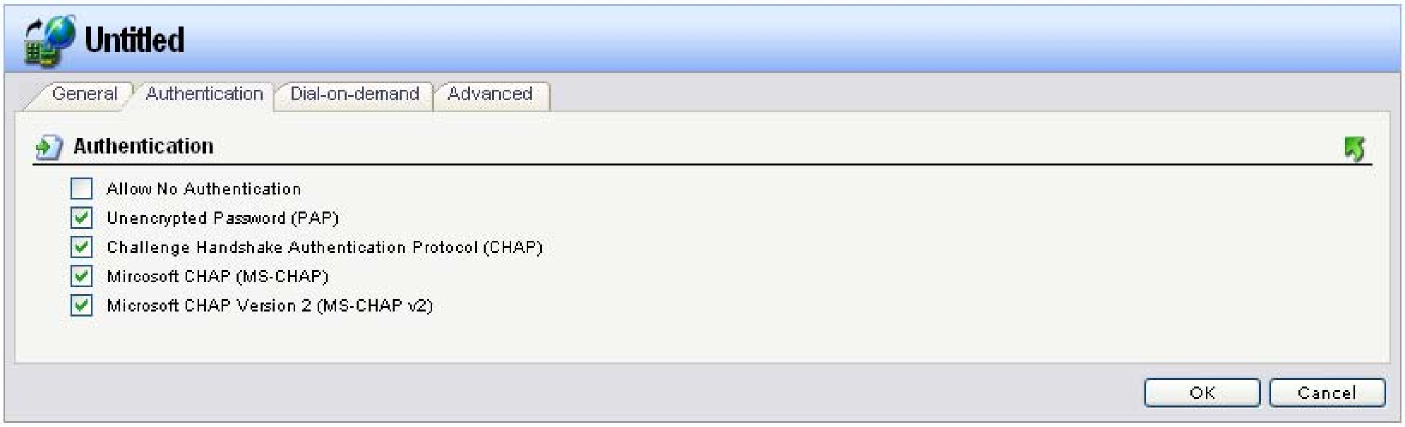
Name:	Untitled
Physical Interface:	(None)
Remote Network:	(None)
Service Name:	

Authentication

Username:	
Password:	
Confirm Password:	

Comments

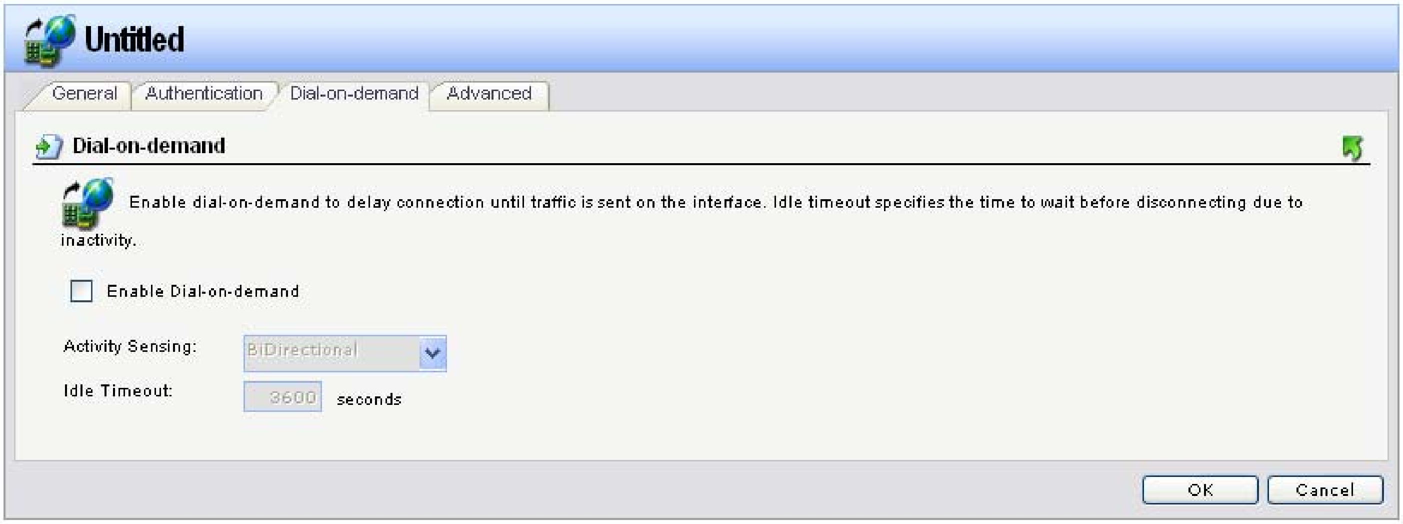
Comments:



Untitled

Authentication

- ☐ Allow No Authentication
- ☑ Unencrypted Password (PAP)
- ☑ Challenge Handshake Authentication Protocol (CHAP)
- ☑ Mircosoft CHAP (MS-CHAP)
- ☑ Microsoft CHAP Version 2 (MS-CHAP v2)



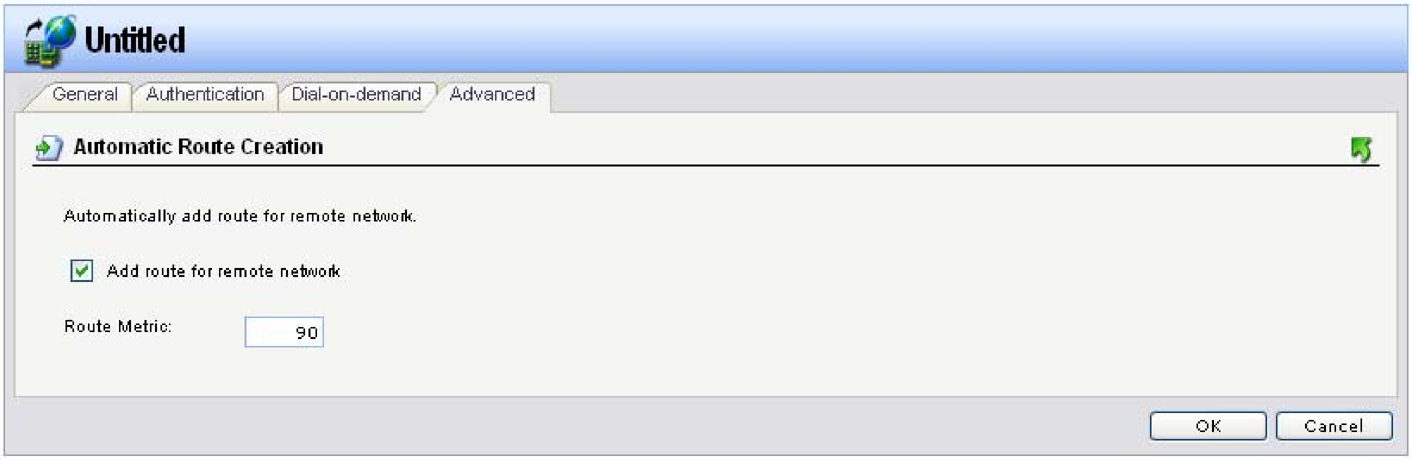
Dial-on-demand

Enable dial-on-demand to delay connection until traffic is sent on the interface. Idle timeout specifies the time to wait before disconnecting due to inactivity.

□ Enable Dial-on-demand

Activity Sensing: BiDirectional

Idle Timeout: 3600 seconds

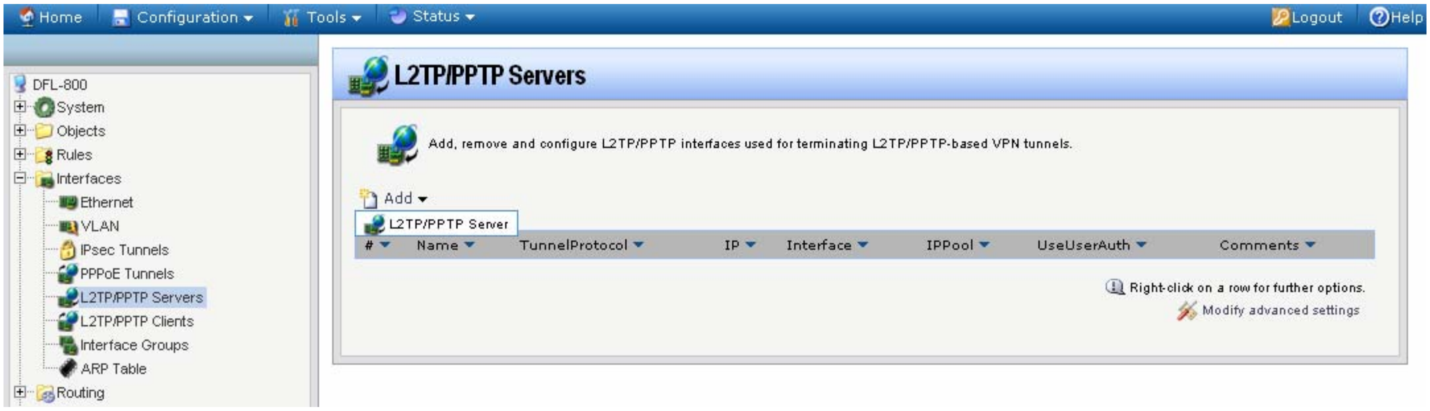


Automatic Route Creation

Automatically add route for remote network.

☑ Add route for remote network

Route Metric: 90



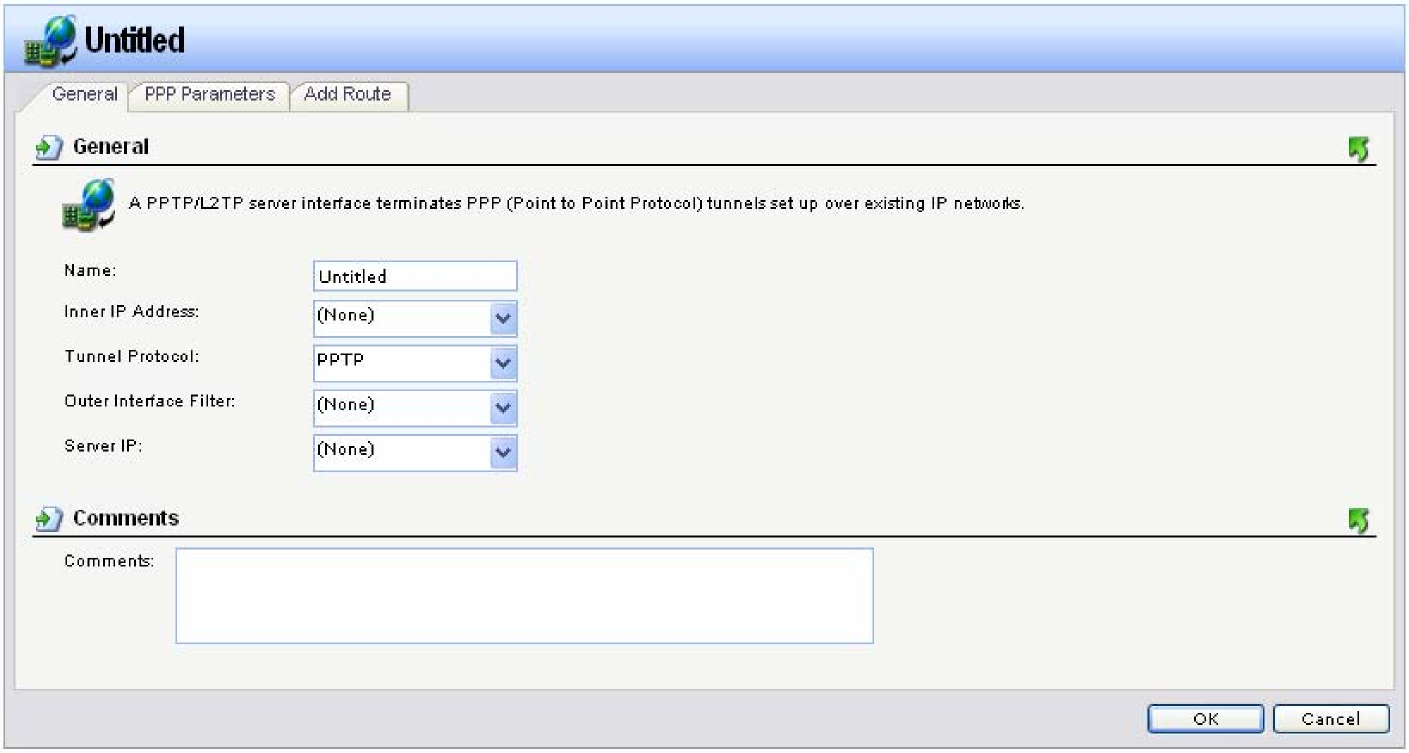
L2TP/PPTP Servers

Add, remove and configure L2TP/PPTP interfaces used for terminating L2TP/PPTP-based VPN tunnels.

#	Name	TunnelProtocol	IP	Interface	IPPool	UseUserAuth	Comments

Right-click on a row for further options.

Modify advanced settings



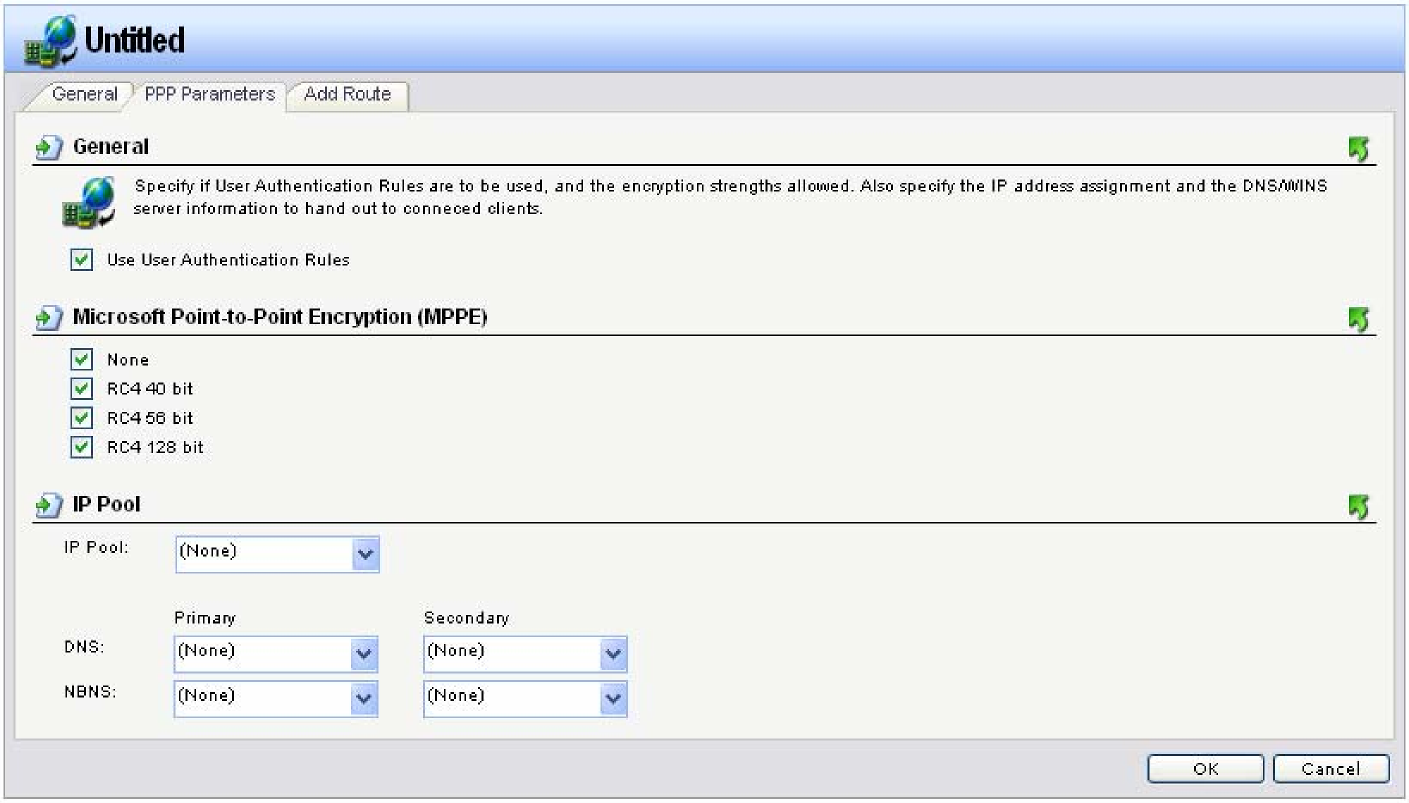
General

A PPTP/L2TP server interface terminates PPP (Point to Point Protocol) tunnels set up over existing IP networks.

Name:	Untitled
Inner IP Address:	(None)
Tunnel Protocol:	PPTP
Outer Interface Filter:	(None)
Server IP:	(None)

Comments

Comments:



General

Specify if User Authentication Rules are to be used, and the encryption strengths allowed. Also specify the IP address assignment and the DNS/WINS server information to hand out to conneced clients.

☑ Use User Authentication Rules

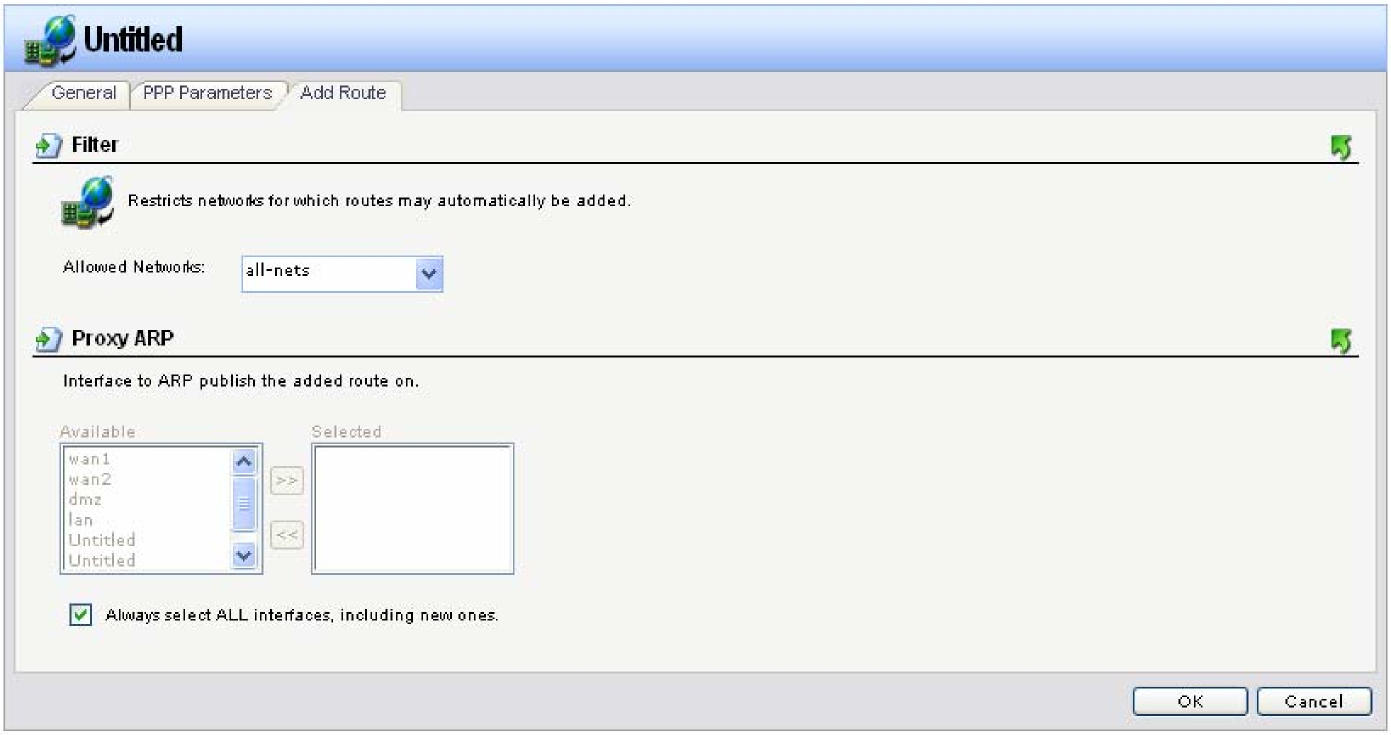
Microsoft Point-to-Point Encryption (MPPE)

☑ None
☑ RC4 40 bit
☑ RC4 56 bit
☑ RC4 128 bit

IP Pool

IP Pool: (None)

	Primary	Secondary
DNS:	(None)	(None)
NBNS:	(None)	(None)



Untitled

Filter

Restricts networks for which routes may automatically be added.

Allowed Networks: all-nets

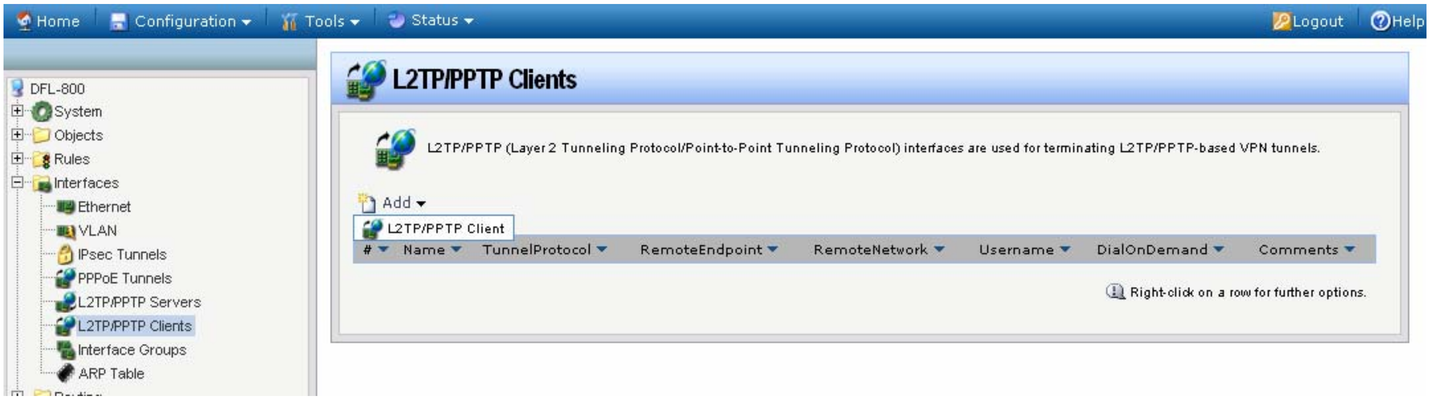
Proxy ARP

Interface to ARP publish the added route on.

Available: wan1, wan2, dmz, lan, Untitled, Untitled

Selected:

☑ Always select ALL interfaces, including new ones.

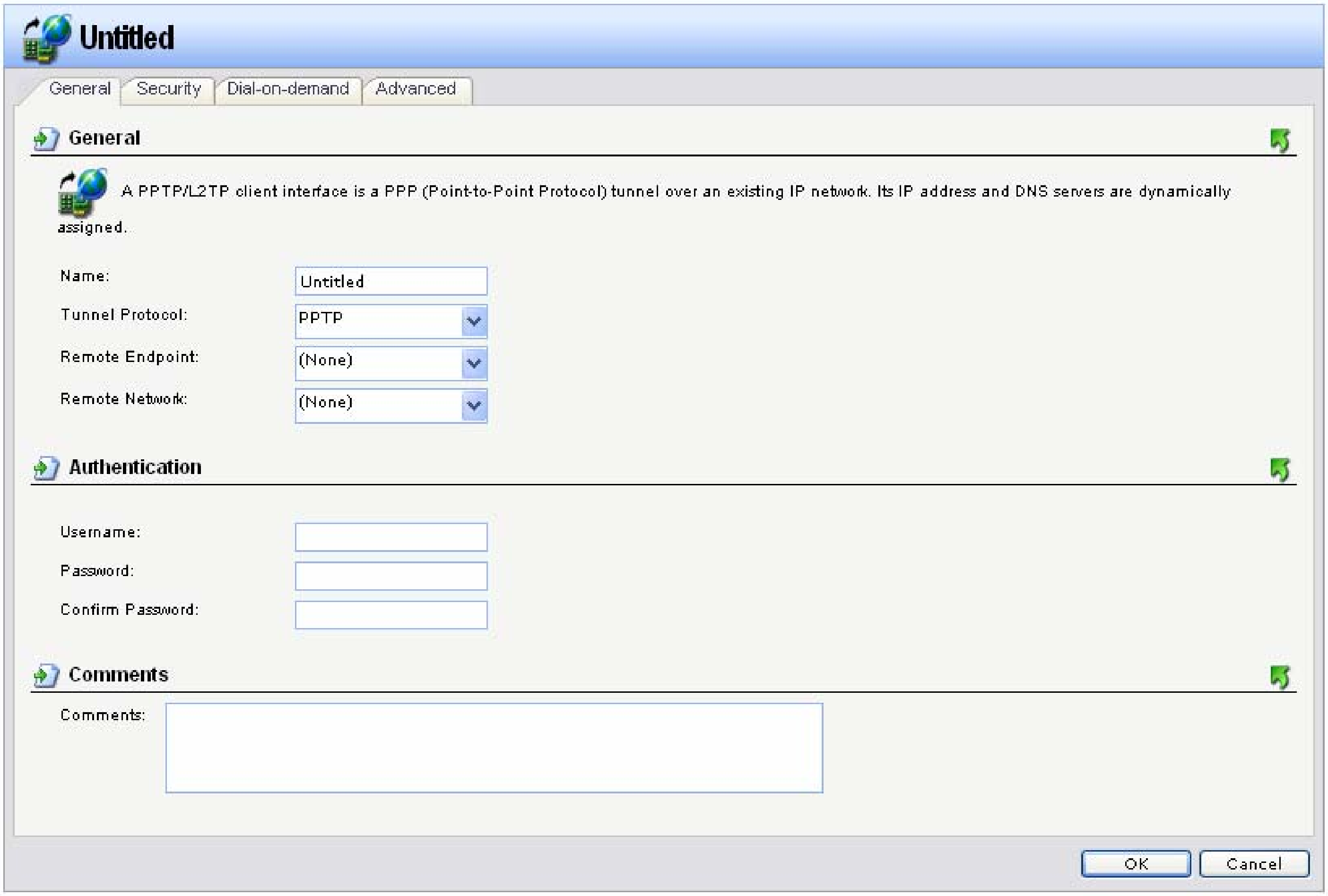


L2TP/PPTP Clients

L2TP/PPTP (Layer 2 Tunneling Protocol/Point-to-Point Tunneling Protocol) interfaces are used for terminating L2TP/PPTP-based VPN tunnels.

#	Name	TunnelProtocol	RemoteEndpoint	RemoteNetwork	Username	DialOnDemand	Comments

Right-click on a row for further options.



General

A PPTP/L2TP client interface is a PPP (Point-to-Point Protocol) tunnel over an existing IP network. Its IP address and DNS servers are dynamically assigned.

Name:	Untitled
Tunnel Protocol:	PPTP
Remote Endpoint:	(None)
Remote Network:	(None)

Authentication

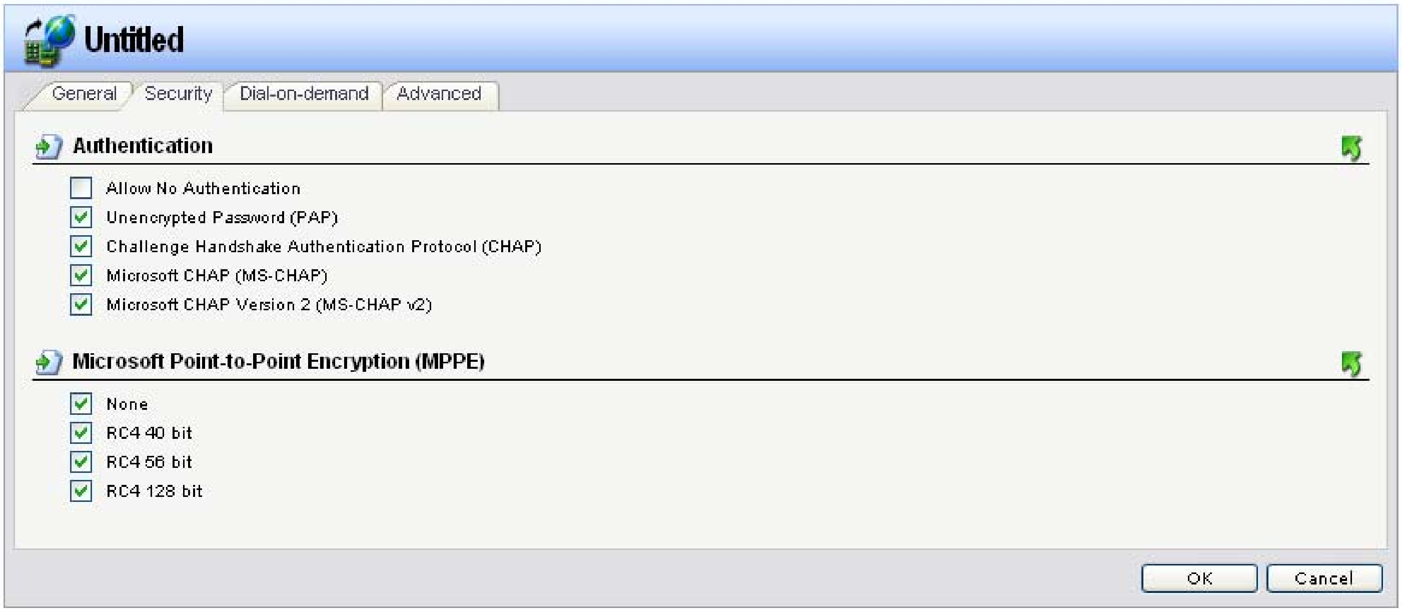
Username:

Password:

Confirm Password:

Comments

Comments:

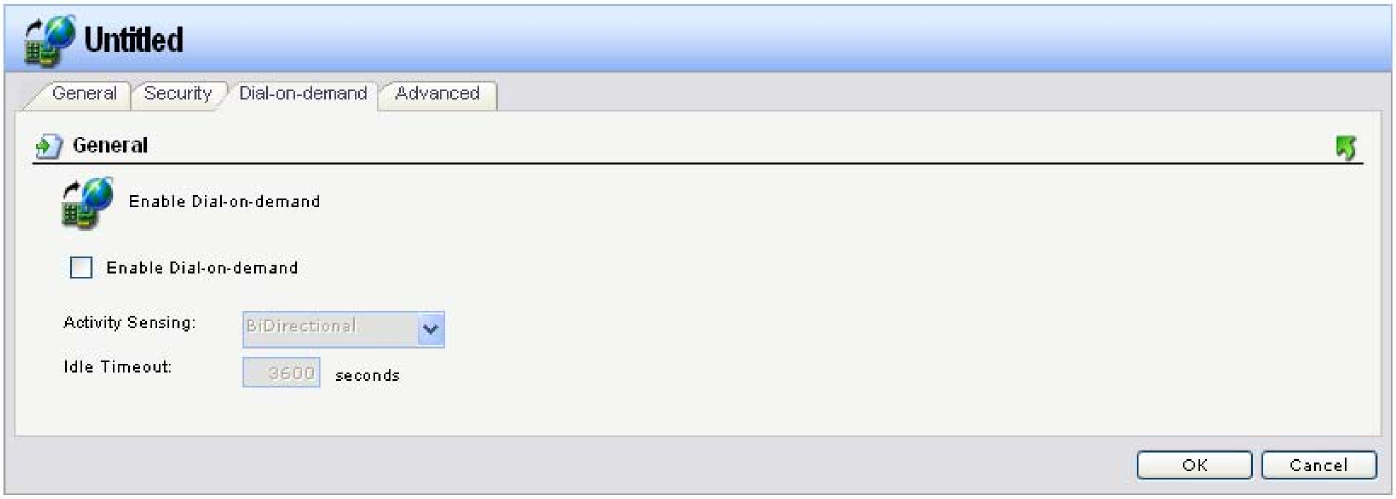


Authentication

- □ Allow No Authentication
- ☑ Unencrypted Password (PAP)
- ☑ Challenge Handshake Authentication Protocol (CHAP)
- ☑ Microsoft CHAP (MS-CHAP)
- ☑ Microsoft CHAP Version 2 (MS-CHAP v2)

Microsoft Point-to-Point Encryption (MPPE)

- ☑ None
- ☑ RC4 40 bit
- ☑ RC4 56 bit
- ☑ RC4 128 bit



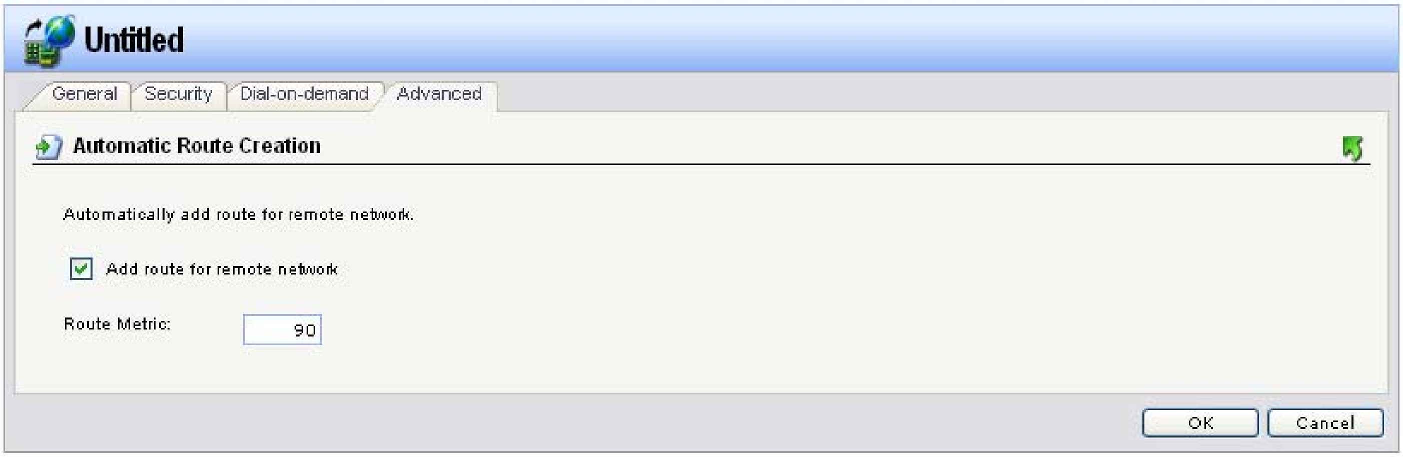
General

Enable Dial-on-demand

□ Enable Dial-on-demand

Activity Sensing: BiDirectional

Idle Timeout: 3600 seconds

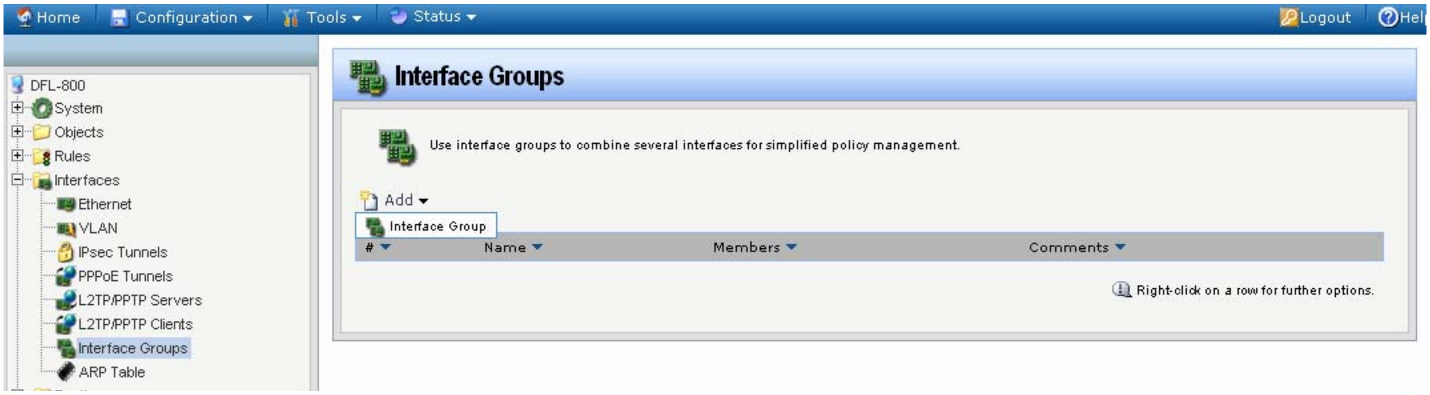


Automatic Route Creation

Automatically add route for remote network.

☑ Add route for remote network

Route Metric: 90

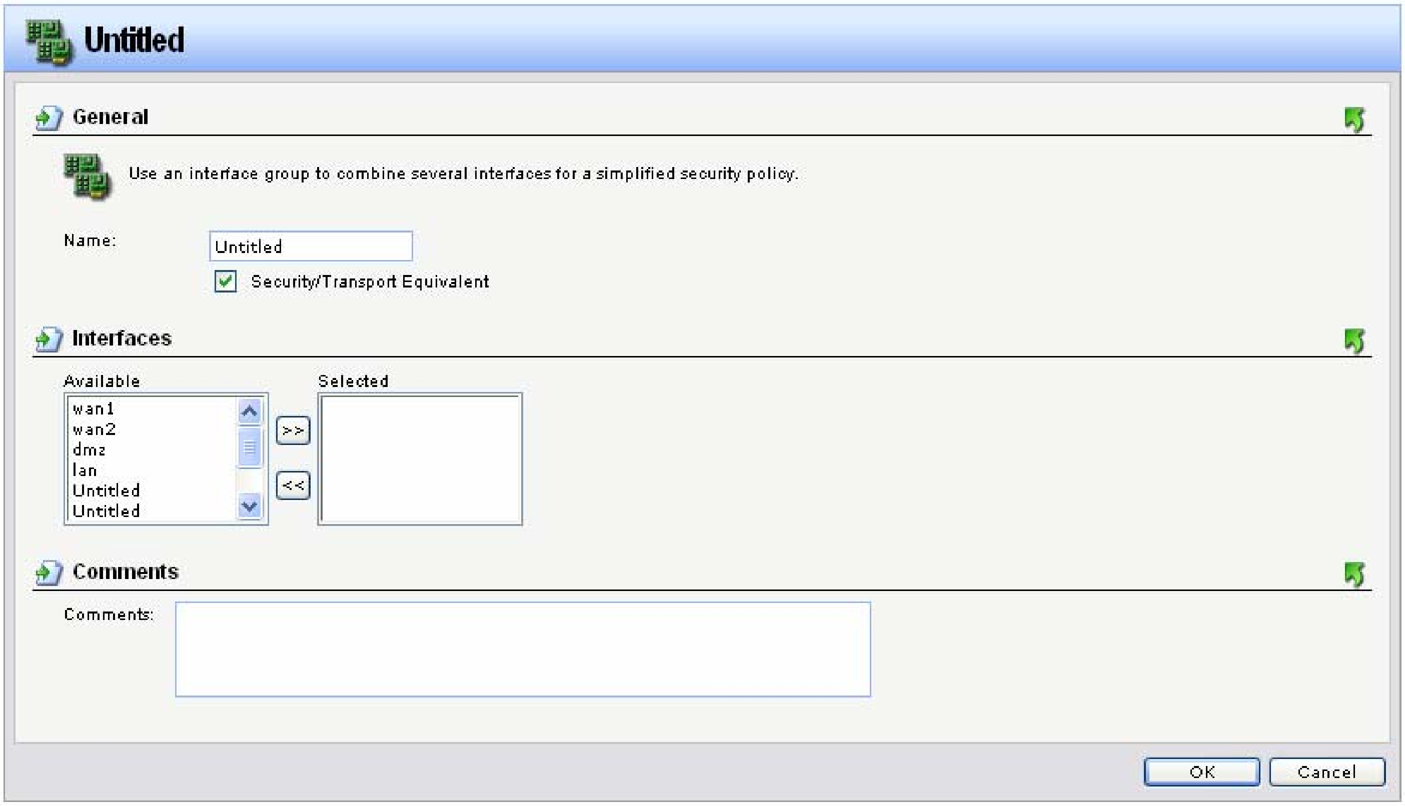


Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

#	Name	Members	Comments

Right-click on a row for further options.



Untitled

General

Use an interface group to combine several interfaces for a simplified security policy.

Name: Untitled

☑ Security/Transport Equivalent

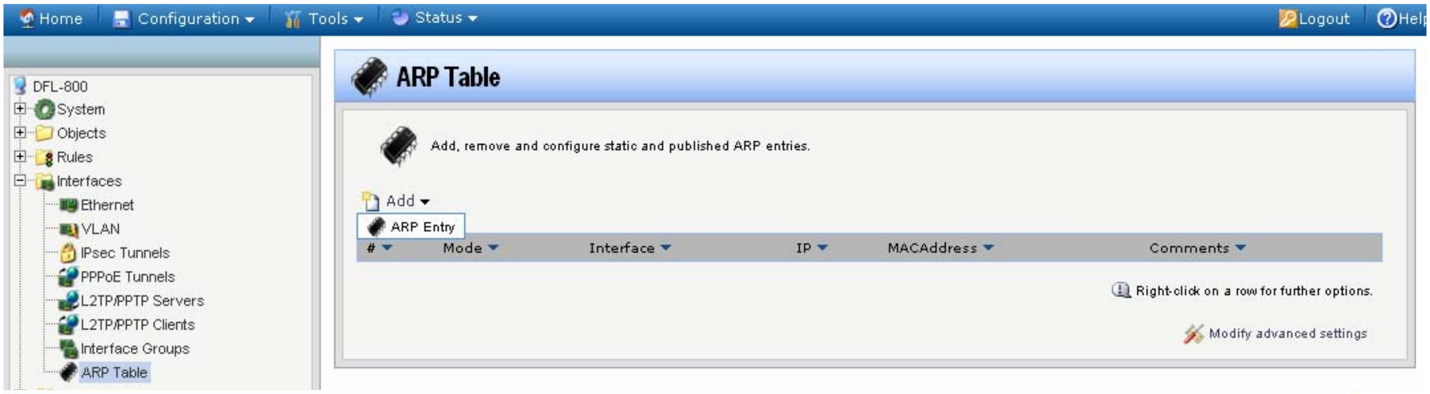
Interfaces

Available: wan1, wan2, dmz, lan, Untitled, Untitled

Selected:

Comments

Comments:

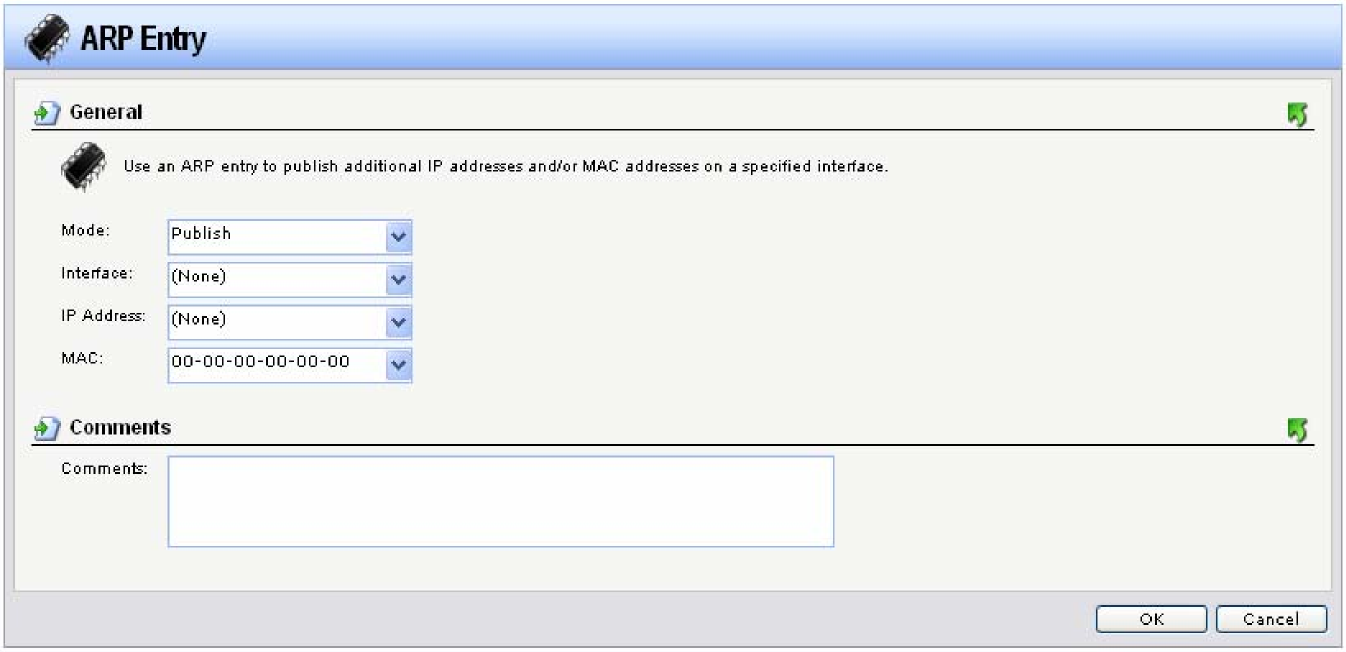


ARP Table

Add, remove and configure static and published ARP entries.

#	Mode	Interface	IP	MACAddress	Comments

Right-click on a row for further options.



ARP Entry

General

Use an ARP entry to publish additional IP addresses and/or MAC addresses on a specified interface.

Mode: Publish

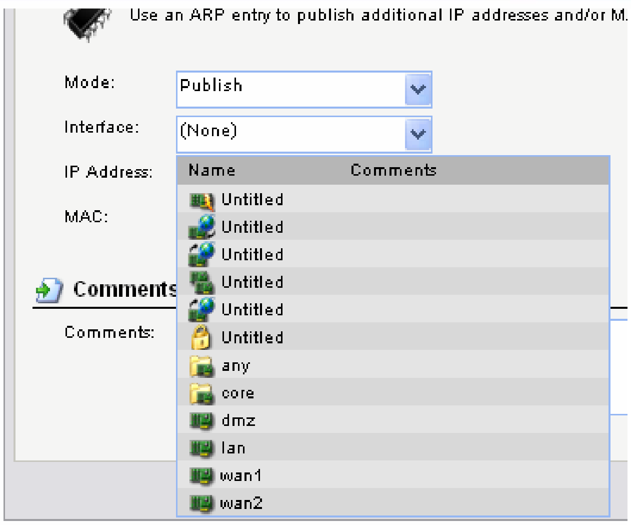
Interface: (None)

IP Address: (None)

MAC: 00-00-00-00-00-00

Comments

Comments:



Use an ARP entry to publish additional IP addresses and/or M

Mode: Publish

Interface: (None)

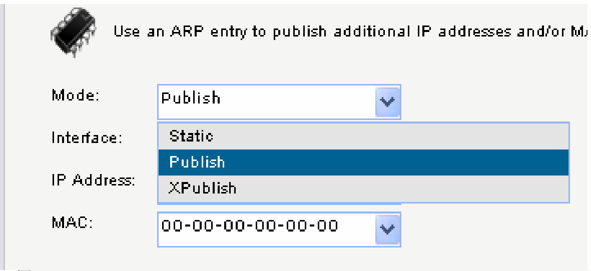
IP Address:

MAC:

Name	Comments
Untitled	
Untitled	
Untitled	
Untitled	
Untitled	
Untitled	
any	
core	
dmz	
lan	
wan1	
wan2	

Comments

Comments:



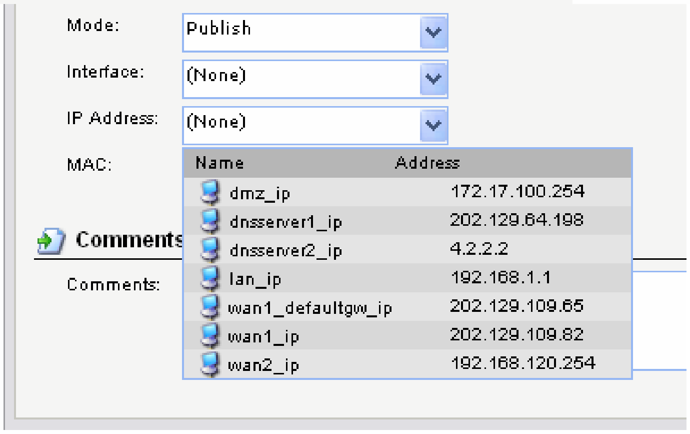
Use an ARP entry to publish additional IP addresses and/or M

Mode: Publish

Interface:

IP Address:

MAC: 00-00-00-00-00-00



Mode: Publish

Interface: (None)

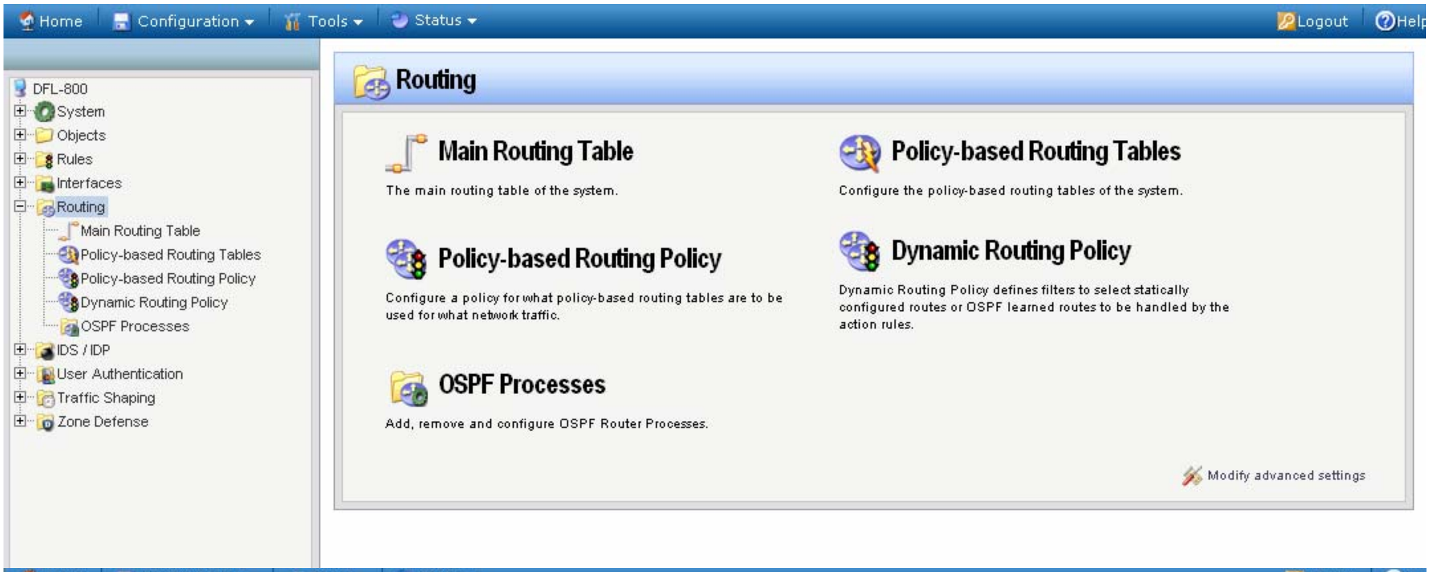
IP Address: (None)

MAC:

Name	Address
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254

Comments

Comments:



Routing

Main Routing Table

The main routing table of the system.

Policy-based Routing Tables

Configure the policy-based routing tables of the system.

Policy-based Routing Policy

Configure a policy for what policy-based routing tables are to be used for what network traffic.

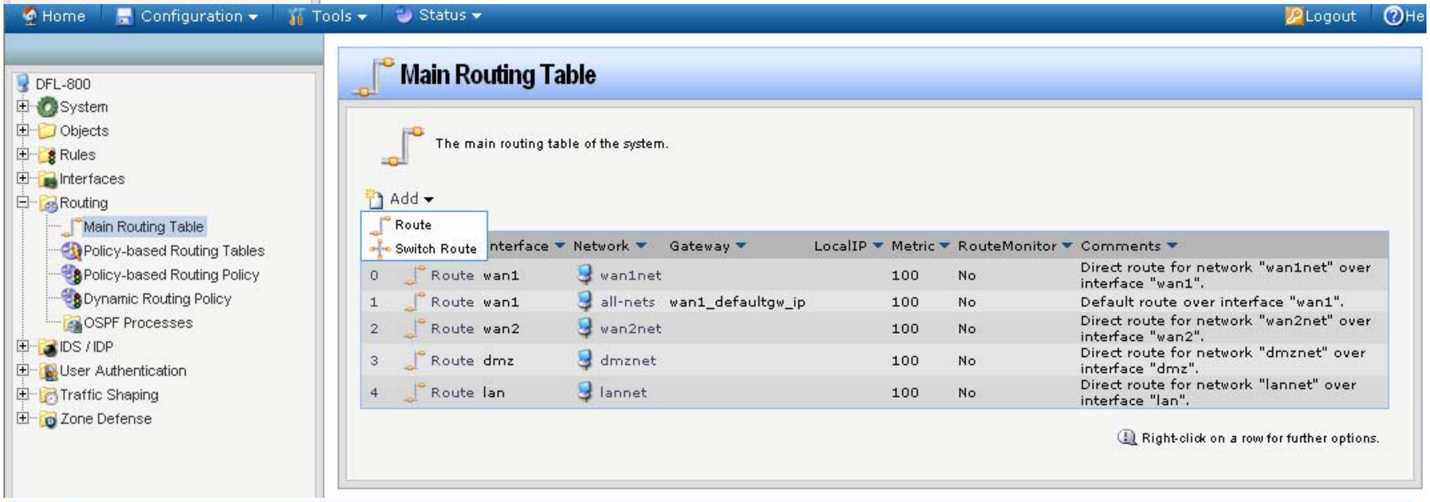
Dynamic Routing Policy

Dynamic Routing Policy defines filters to select statically configured routes or OSPF learned routes to be handled by the action rules.

OSPF Processes

Add, remove and configure OSPF Router Processes.

Modify advanced settings

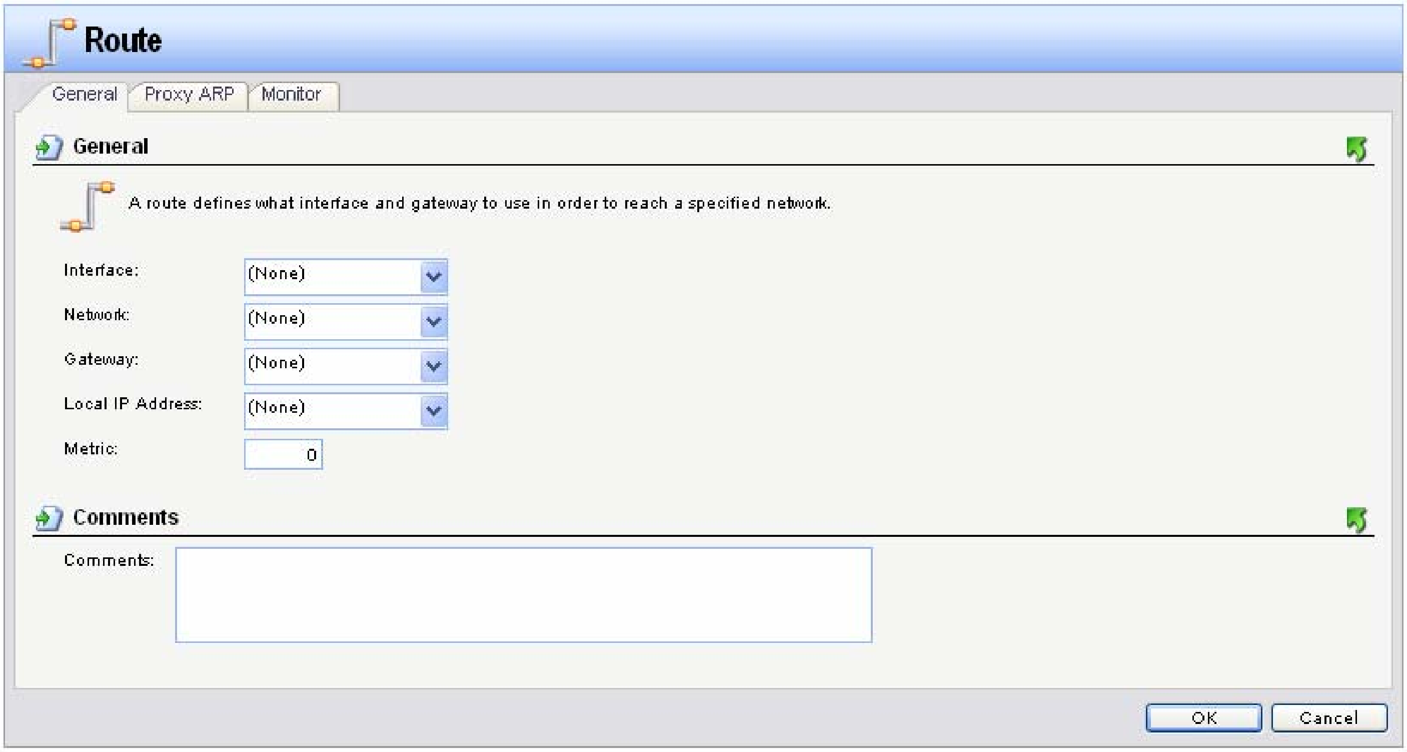


Main Routing Table

The main routing table of the system.

		nterface	Network	Gateway	LocalIP	Metric	RouteMonitor	Comments
0	Route	wan1	wan1net			100	No	Direct route for network "wan1net" over interface "wan1".
1	Route	wan1	all-nets	wan1_defaultgw_ip		100	No	Default route over interface "wan1".
2	Route	wan2	wan2net			100	No	Direct route for network "wan2net" over interface "wan2".
3	Route	dmz	dmznet			100	No	Direct route for network "dmznet" over interface "dmz".
4	Route	lan	lannet			100	No	Direct route for network "lannet" over interface "lan".

Right-click on a row for further options.



Route

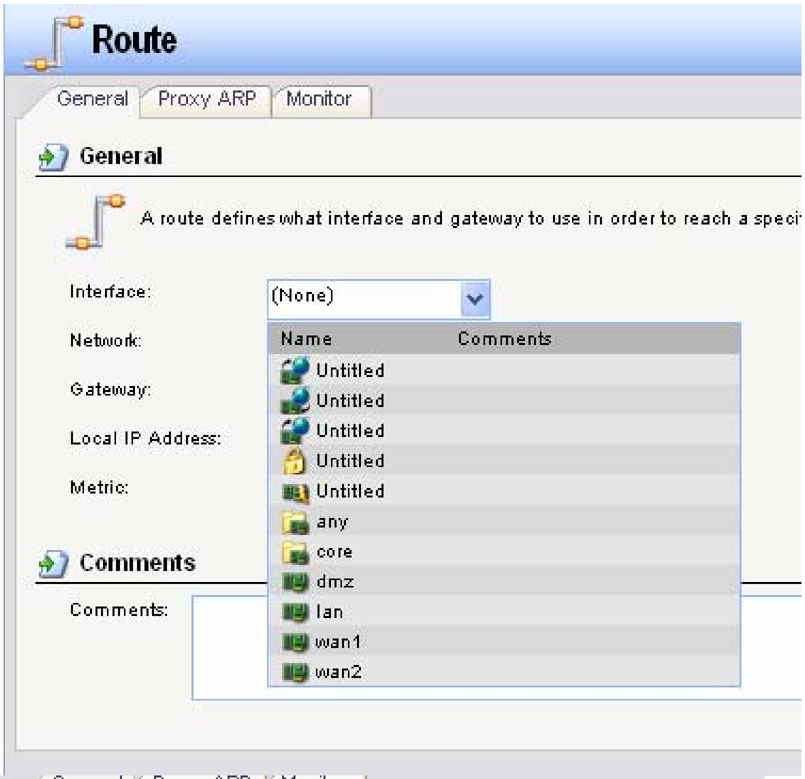
General

A route defines what interface and gateway to use in order to reach a specified network.

Interface:	(None)
Network:	(None)
Gateway:	(None)
Local IP Address:	(None)
Metric:	0

Comments

Comments:



Route

General

A route defines what interface and gateway to use in order to reach a speci

Interface: (None)

Network:

Gateway:

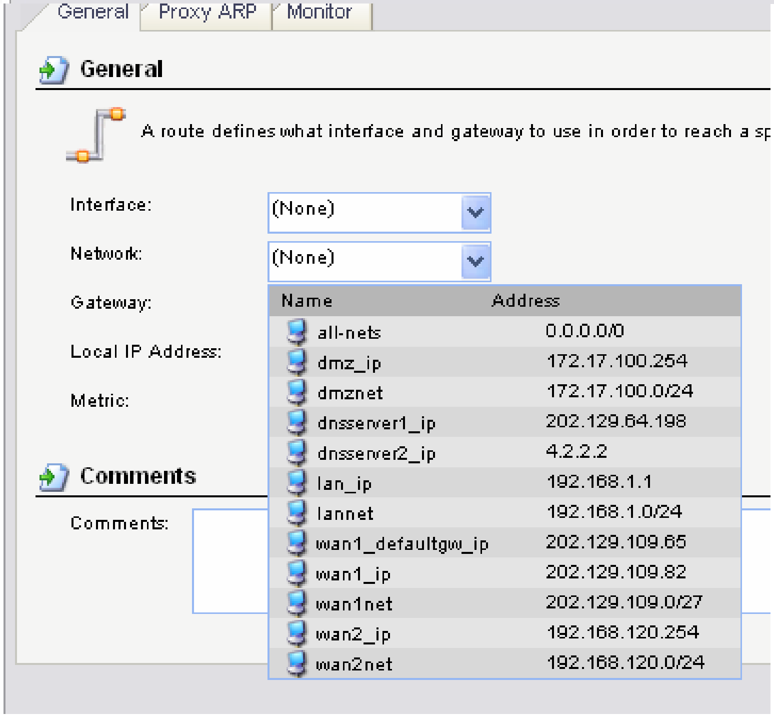
Local IP Address:

Metric:

Name	Comments
Untitled	
Untitled	
Untitled	
Untitled	
Untitled	
any	
core	
dmz	
lan	
wan1	
wan2	

Comments

Comments:



General

A route defines what interface and gateway to use in order to reach a sp

Interface: (None)

Network: (None)

Gateway:

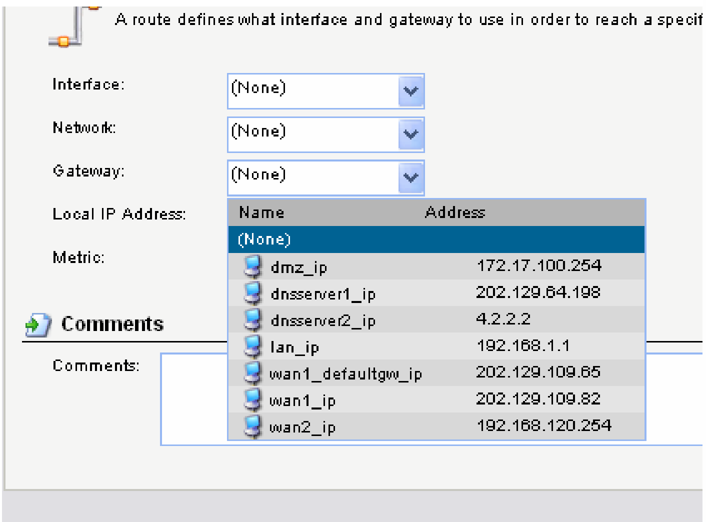
Local IP Address:

Metric:

Name	Address
all-nets	0.0.0.0/0
dmz_ip	172.17.100.254
dmznet	172.17.100.0/24
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
lannet	192.168.1.0/24
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan1net	202.129.109.0/27
wan2_ip	192.168.120.254
wan2net	192.168.120.0/24

Comments

Comments:



A route defines what interface and gateway to use in order to reach a specif

Interface: (None)

Network: (None)

Gateway: (None)

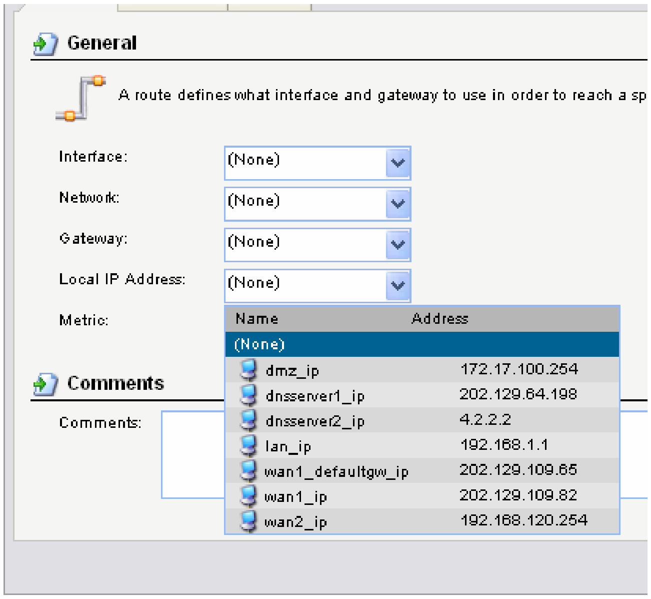
Local IP Address:

Metric:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254

Comments

Comments:



General

A route defines what interface and gateway to use in order to reach a sp

Interface: (None)

Network: (None)

Gateway: (None)

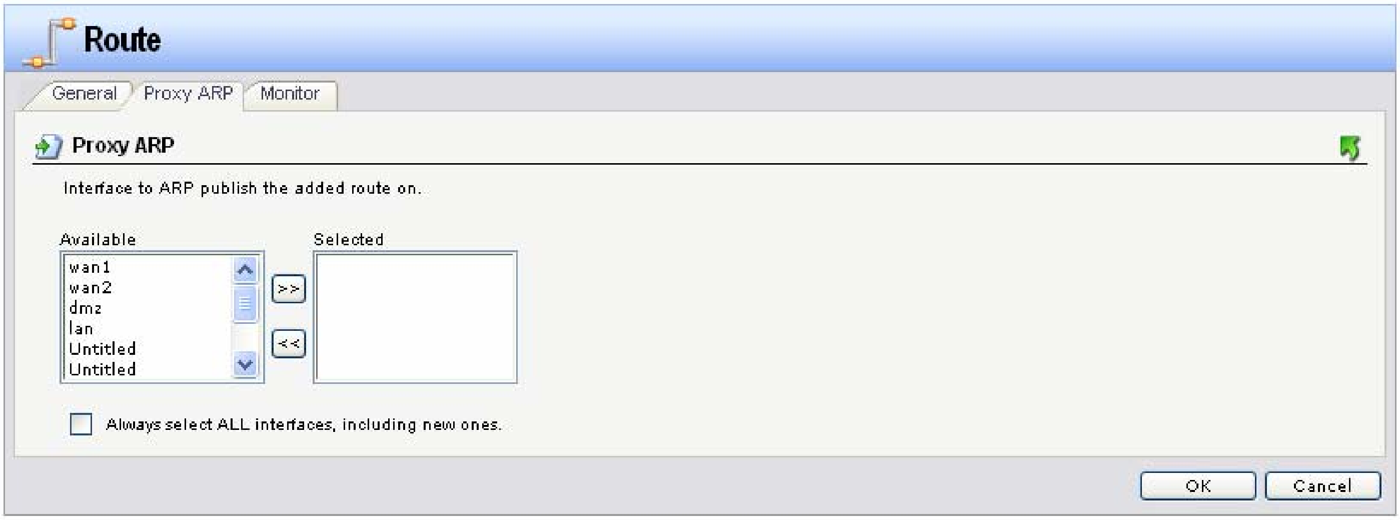
Local IP Address: (None)

Metric:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254

Comments

Comments:



Route

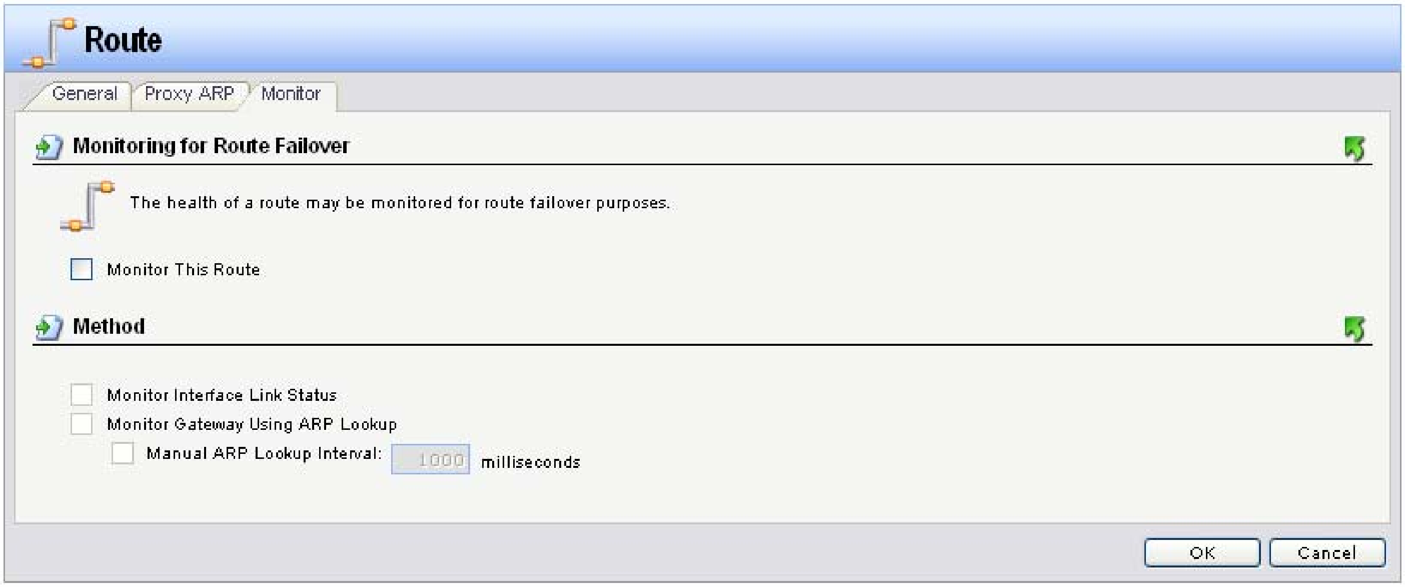
Proxy ARP

Interface to ARP publish the added route on.

Available: wan1, wan2, dmz, lan, Untitled, Untitled

Selected:

□ Always select ALL interfaces, including new ones.



Route

Monitoring for Route Failover

The health of a route may be monitored for route failover purposes.

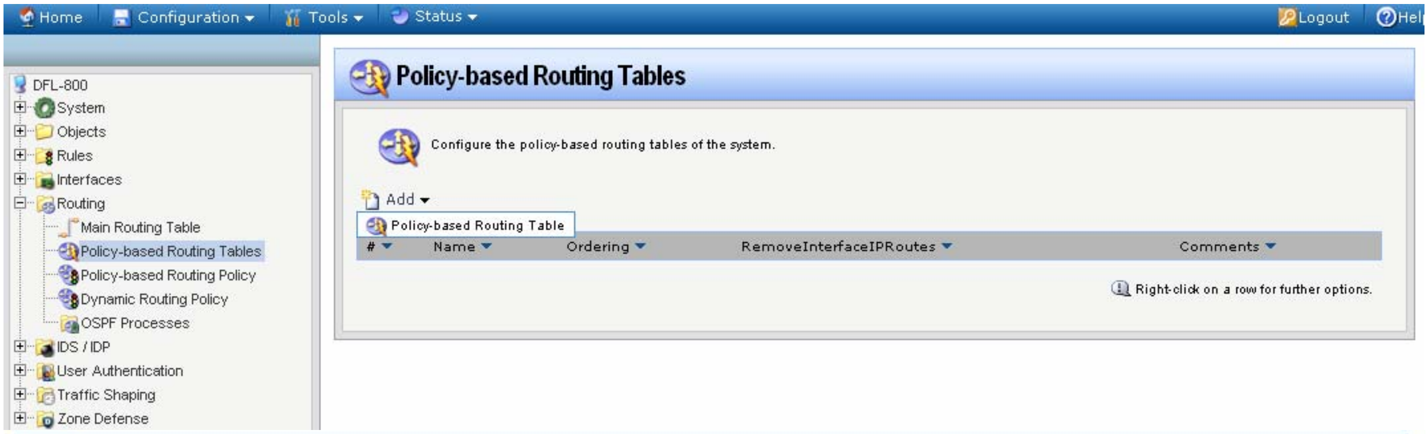
□ Monitor This Route

Method

□ Monitor Interface Link Status

□ Monitor Gateway Using ARP Lookup

□ Manual ARP Lookup Interval: 1000 milliseconds

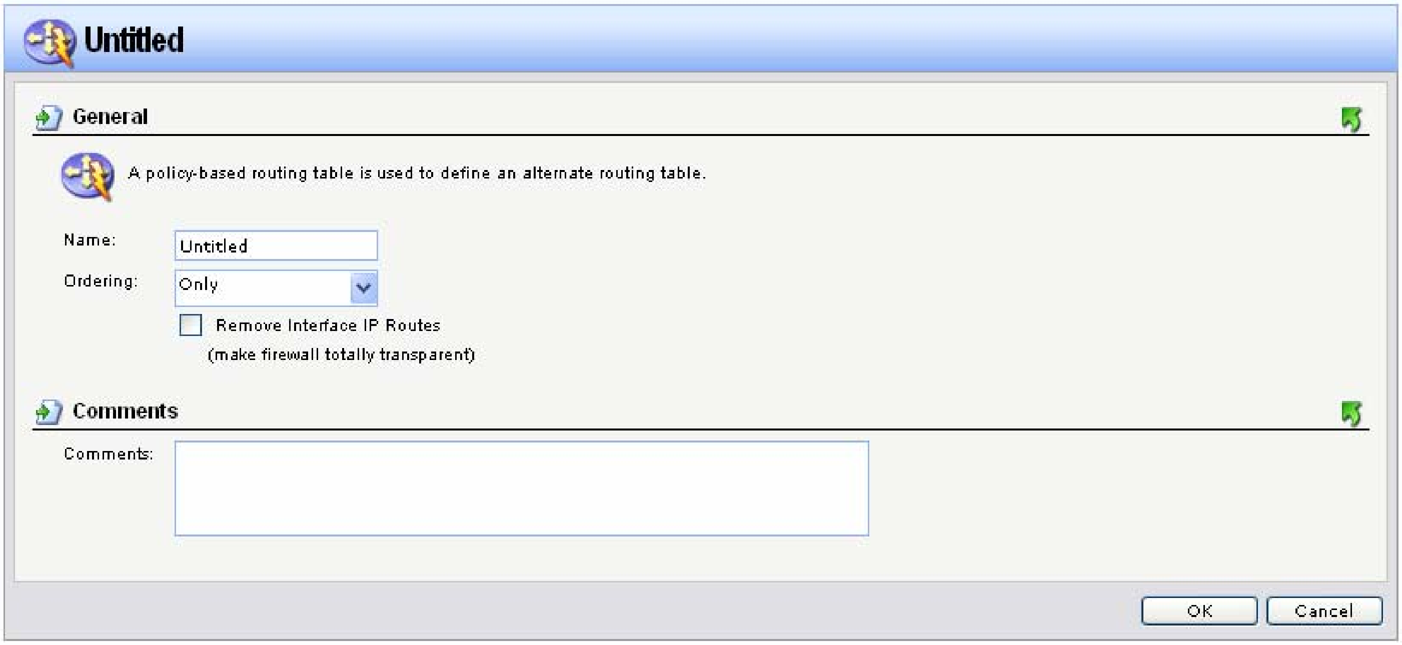


Policy-based Routing Tables

Configure the policy-based routing tables of the system.

#	Name	Ordering	RemoveInterfaceIPRoutes	Comments

Right-click on a row for further options.



Untitled

General

A policy-based routing table is used to define an alternate routing table.

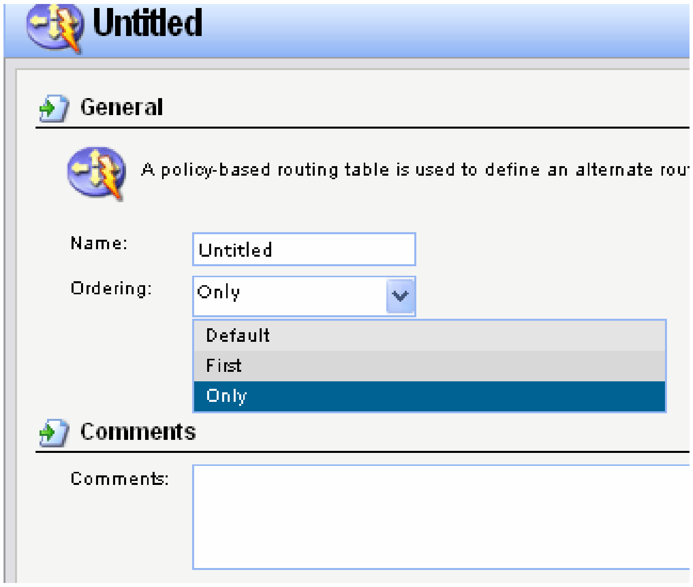
Name: Untitled

Ordering: Only

□ Remove Interface IP Routes (make firewall totally transparent)

Comments

Comments:



Untitled

General

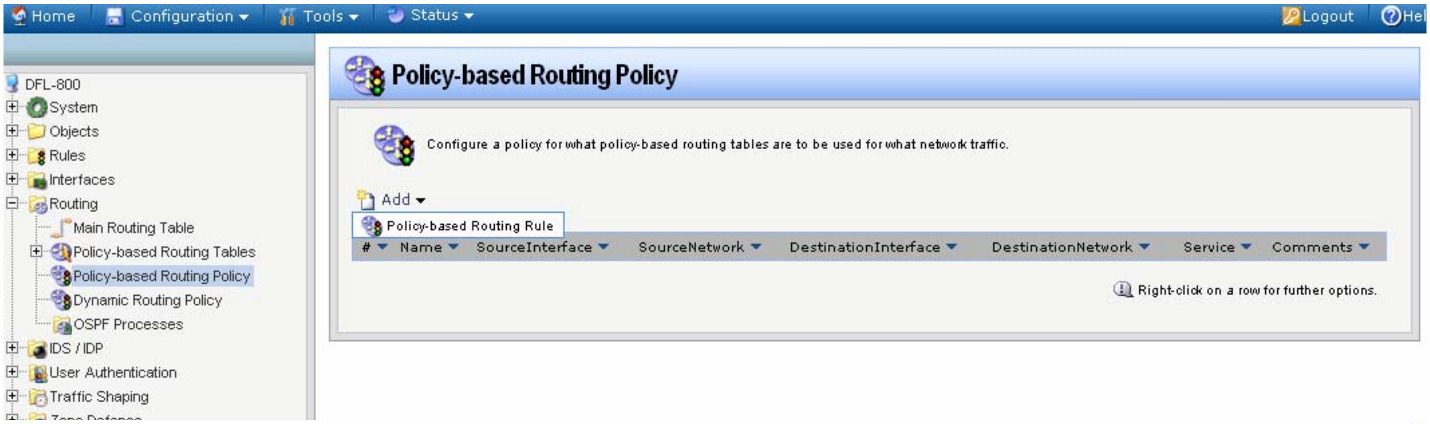
A policy-based routing table is used to define an alternate rou

Name: Untitled

Ordering: Only

Comments

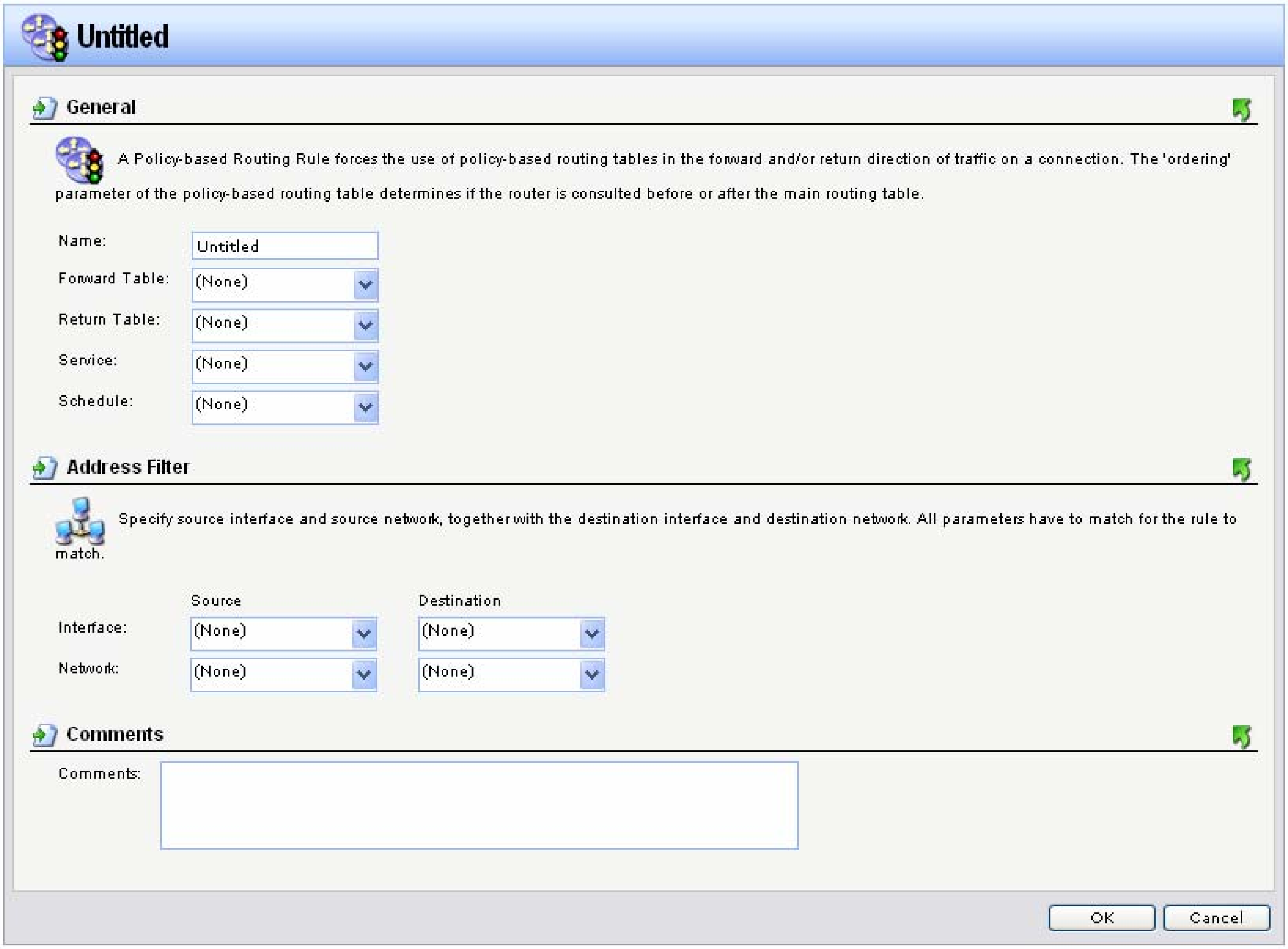
Comments:



Policy-based Routing Policy

Configure a policy for what policy-based routing tables are to be used for what network traffic.

Right-click on a row for further options.



Untitled

General

A Policy-based Routing Rule forces the use of policy-based routing tables in the forward and/or return direction of traffic on a connection. The 'ordering' parameter of the policy-based routing table determines if the router is consulted before or after the main routing table.

Name:	Untitled
Forward Table:	(None)
Return Table:	(None)
Service:	(None)
Schedule:	(None)

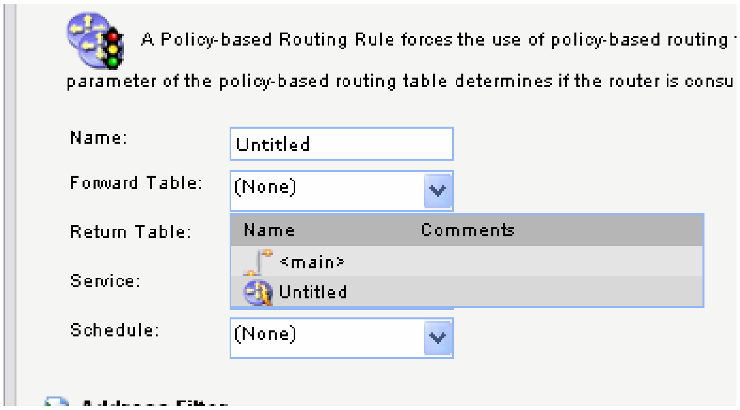
Address Filter

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

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:

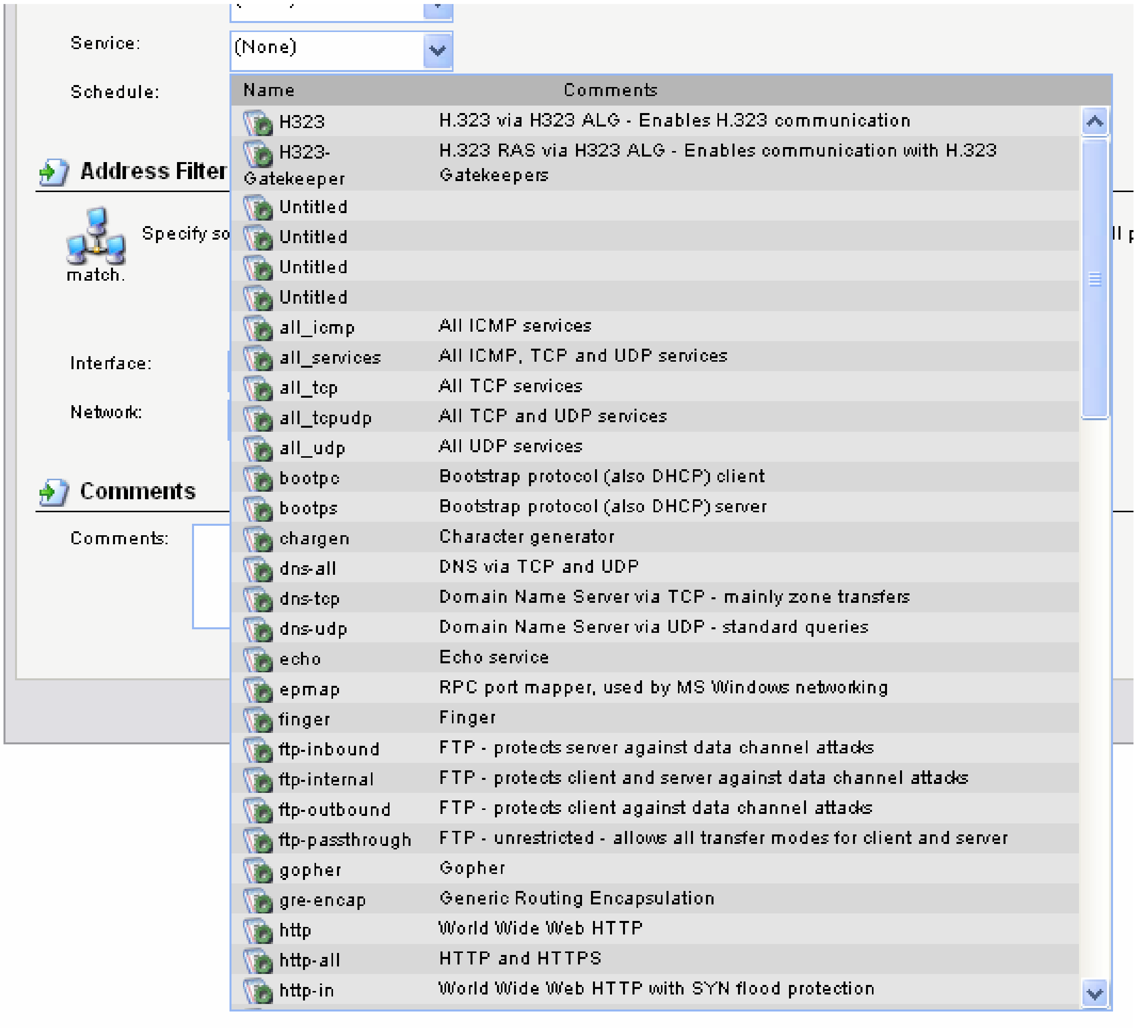


A Policy-based Routing Rule forces the use of policy-based routing t

parameter of the policy-based routing table determines if the router is consu

Name:	Untitled
Forward Table:	(None)
Return Table:	
Service:	
Schedule:	(None)

Name	Comments
<main>	
Untitled	



Service: (None)

Schedule:

Address Filter

Specify so

match.

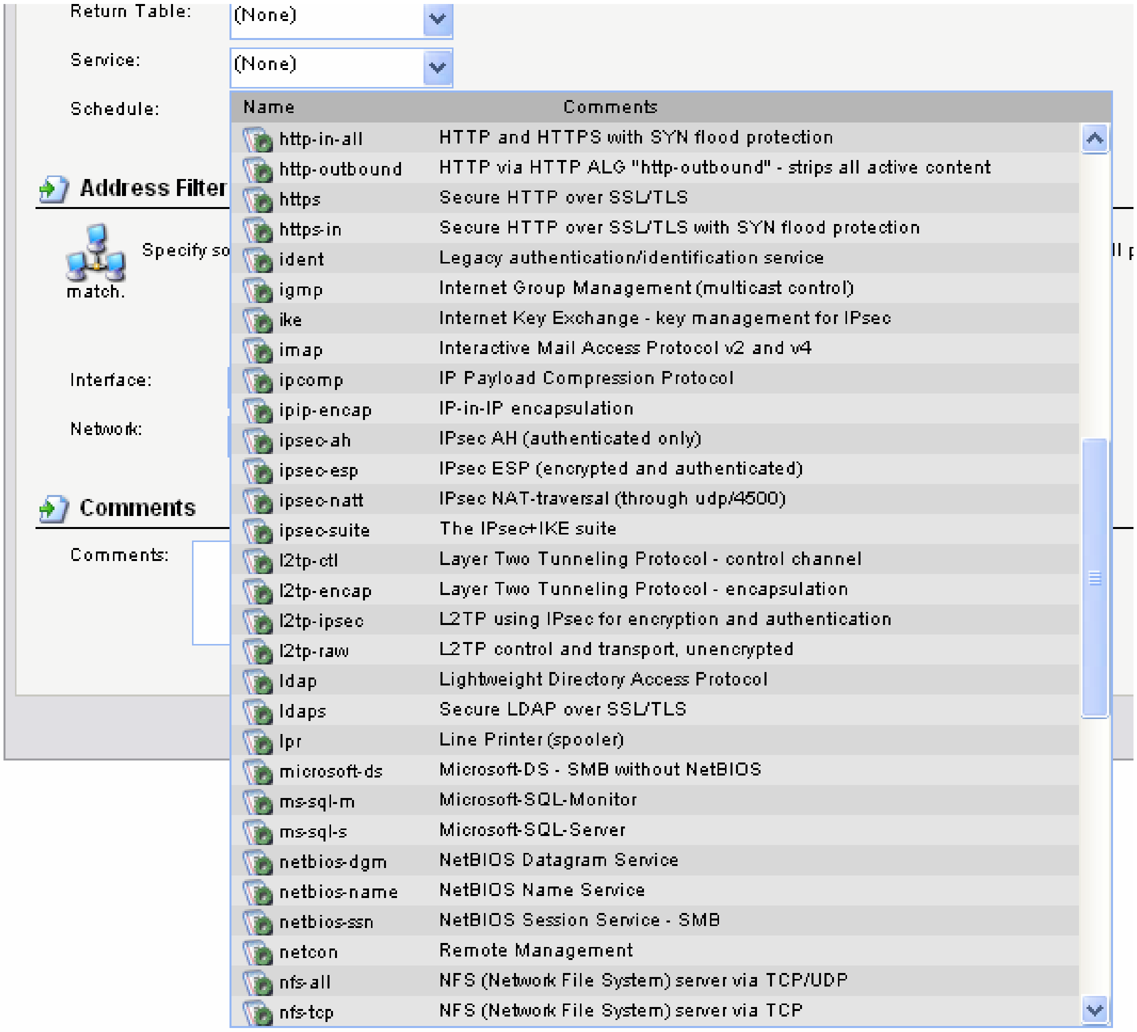
Interface:

Network:

Comments

Comments:

Name	Comments
H323	H.323 via H323 ALG - Enables H.323 communication
H323-Gatekeeper	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers
Untitled	
Untitled	
Untitled	
Untitled	
all_icmp	All ICMP services
all_services	All ICMP, TCP and UDP services
all_tcp	All TCP services
all_tcpudp	All TCP and UDP services
all_udp	All UDP services
bootpc	Bootstrap protocol (also DHCP) client
bootps	Bootstrap protocol (also DHCP) server
chargen	Character generator
dns-all	DNS via TCP and UDP
dns-tcp	Domain Name Server via TCP - mainly zone transfers
dns-udp	Domain Name Server via UDP - standard queries
echo	Echo service
epmap	RPC port mapper, used by MS Windows networking
finger	Finger
ftp-inbound	FTP - protects server against data channel attacks
ftp-internal	FTP - protects client and server against data channel attacks
ftp-outbound	FTP - protects client against data channel attacks
ftp-passthrough	FTP - unrestricted - allows all transfer modes for client and server
gopher	Gopher
gre-encap	Generic Routing Encapsulation
http	World Wide Web HTTP
http-all	HTTP and HTTPS
http-in	World Wide Web HTTP with SYN flood protection



Return Table: (None)

Service: (None)

Schedule:

Name	Comments
http-in-all	HTTP and HTTPS with SYN flood protection
http-outbound	HTTP via HTTP ALG "http-outbound" - strips all active content
https	Secure HTTP over SSL/TLS
https-in	Secure HTTP over SSL/TLS with SYN flood protection
ident	Legacy authentication/identification service
igmp	Internet Group Management (multicast control)
ike	Internet Key Exchange - key management for IPsec
imap	Interactive Mail Access Protocol v2 and v4
ipcomp	IP Payload Compression Protocol
ipip-encap	IP-in-IP encapsulation
ipsec-ah	IPsec AH (authenticated only)
ipsec-esp	IPsec ESP (encrypted and authenticated)
ipsec-natt	IPsec NAT-traversal (through udp/4500)
ipsec-suite	The IPsec+IKE suite
l2tp-ctl	Layer Two Tunneling Protocol - control channel
l2tp-encap	Layer Two Tunneling Protocol - encapsulation
l2tp-ipsec	L2TP using IPsec for encryption and authentication
l2tp-raw	L2TP control and transport, unencrypted
ldap	Lightweight Directory Access Protocol
ldaps	Secure LDAP over SSL/TLS
lpr	Line Printer (spooler)
microsoft-ds	Microsoft-DS - SMB without NetBIOS
ms-sql-m	Microsoft-SQL-Monitor
ms-sql-s	Microsoft-SQL-Server
netbios-dgm	NetBIOS Datagram Service
netbios-name	NetBIOS Name Service
netbios-ssn	NetBIOS Session Service - SMB
netcon	Remote Management
nfs-all	NFS (Network File System) server via TCP/UDP
nfs-tcp	NFS (Network File System) server via TCP

Address Filter

Specify so

ll p

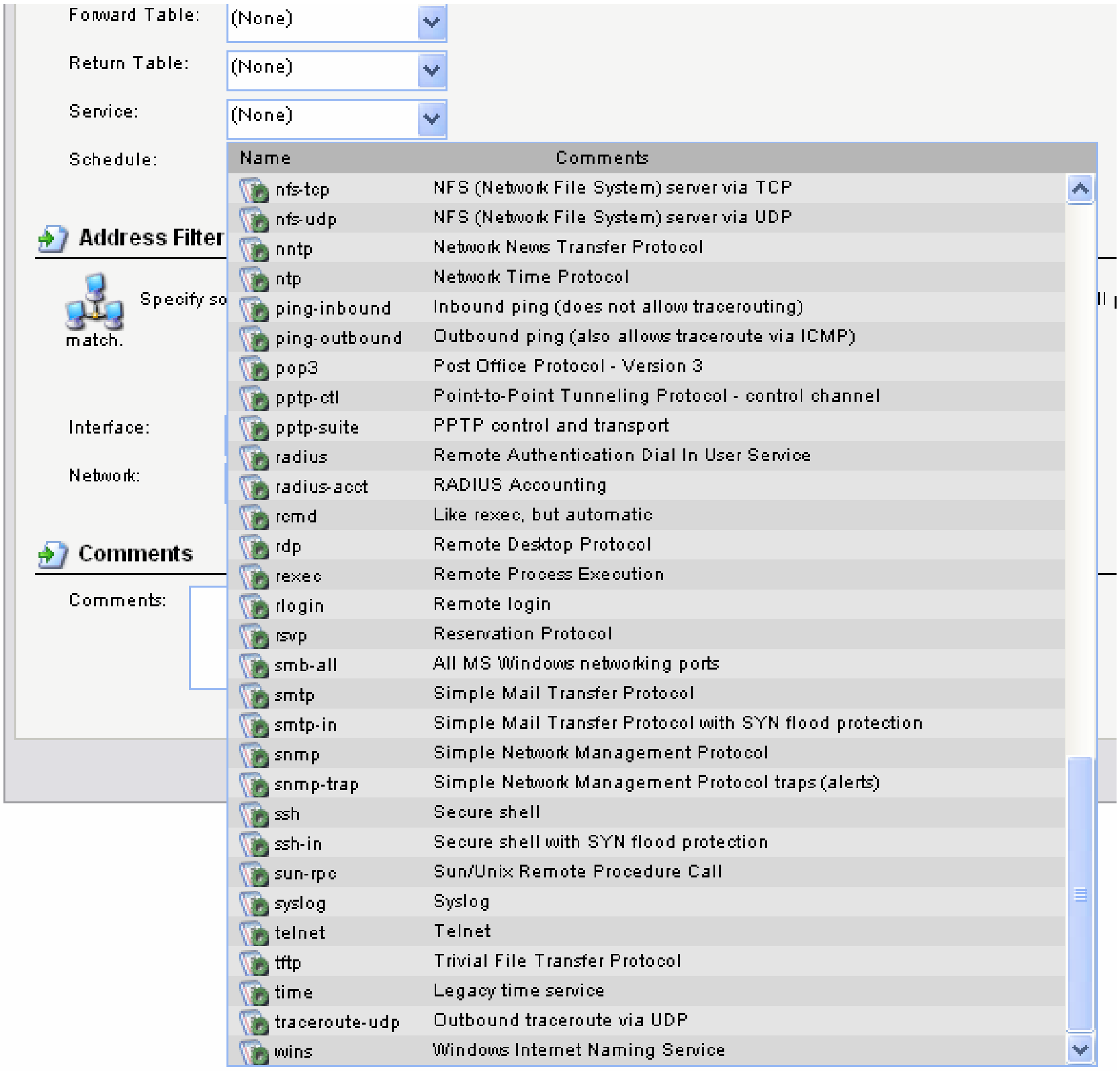
match.

Interface:

Network:

Comments

Comments:



Forward Table:	(None)
Return Table:	(None)
Service:	(None)
Schedule:	

Name	Comments
nfs-tcp	NFS (Network File System) server via TCP
nfs-udp	NFS (Network File System) server via UDP
nntp	Network News Transfer Protocol
ntp	Network Time Protocol
ping-inbound	Inbound ping (does not allow tracerouting)
ping-outbound	Outbound ping (also allows traceroute via ICMP)
pop3	Post Office Protocol - Version 3
pptp-ctl	Point-to-Point Tunneling Protocol - control channel
pptp-suite	PPTP control and transport
radius	Remote Authentication Dial In User Service
radius-acct	RADIUS Accounting
rcmd	Like rexec, but automatic
rdp	Remote Desktop Protocol
rexec	Remote Process Execution
rlogin	Remote login
rsvp	Reservation Protocol
smb-all	All MS Windows networking ports
smtp	Simple Mail Transfer Protocol
smtp-in	Simple Mail Transfer Protocol with SYN flood protection
snmp	Simple Network Management Protocol
snmp-trap	Simple Network Management Protocol traps (alerts)
ssh	Secure shell
ssh-in	Secure shell with SYN flood protection
sun-rpc	Sun/Unix Remote Procedure Call
syslog	Syslog
telnet	Telnet
tftp	Trivial File Transfer Protocol
time	Legacy time service
traceroute-udp	Outbound traceroute via UDP
wins	Windows Internet Naming Service

Address Filter

Specify so

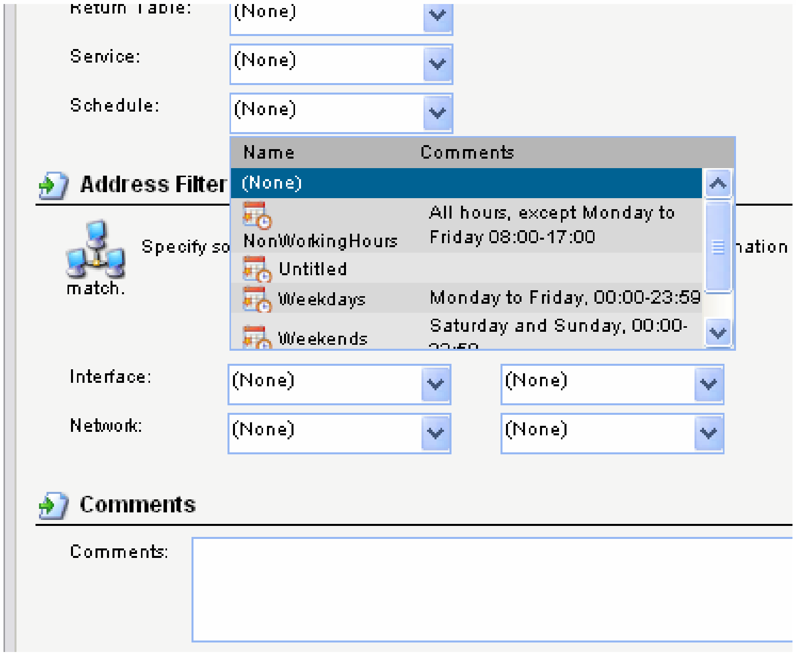
match.

Interface:

Network:

Comments

Comments:



Return Table:	(None)
Service:	(None)
Schedule:	(None)

Name	Comments
(None)	
NonWorkingHours	All hours, except Monday to Friday 08:00-17:00
Untitled	
Weekdays	Monday to Friday, 00:00-23:59
Weekends	Saturday and Sunday, 00:00-23:59

Address Filter

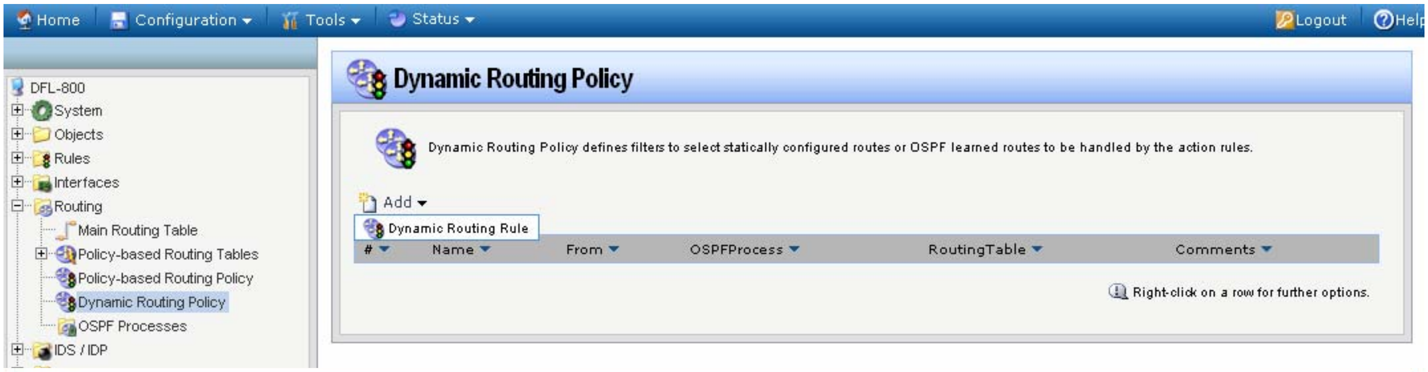
Specify so ... nation

match.

Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:

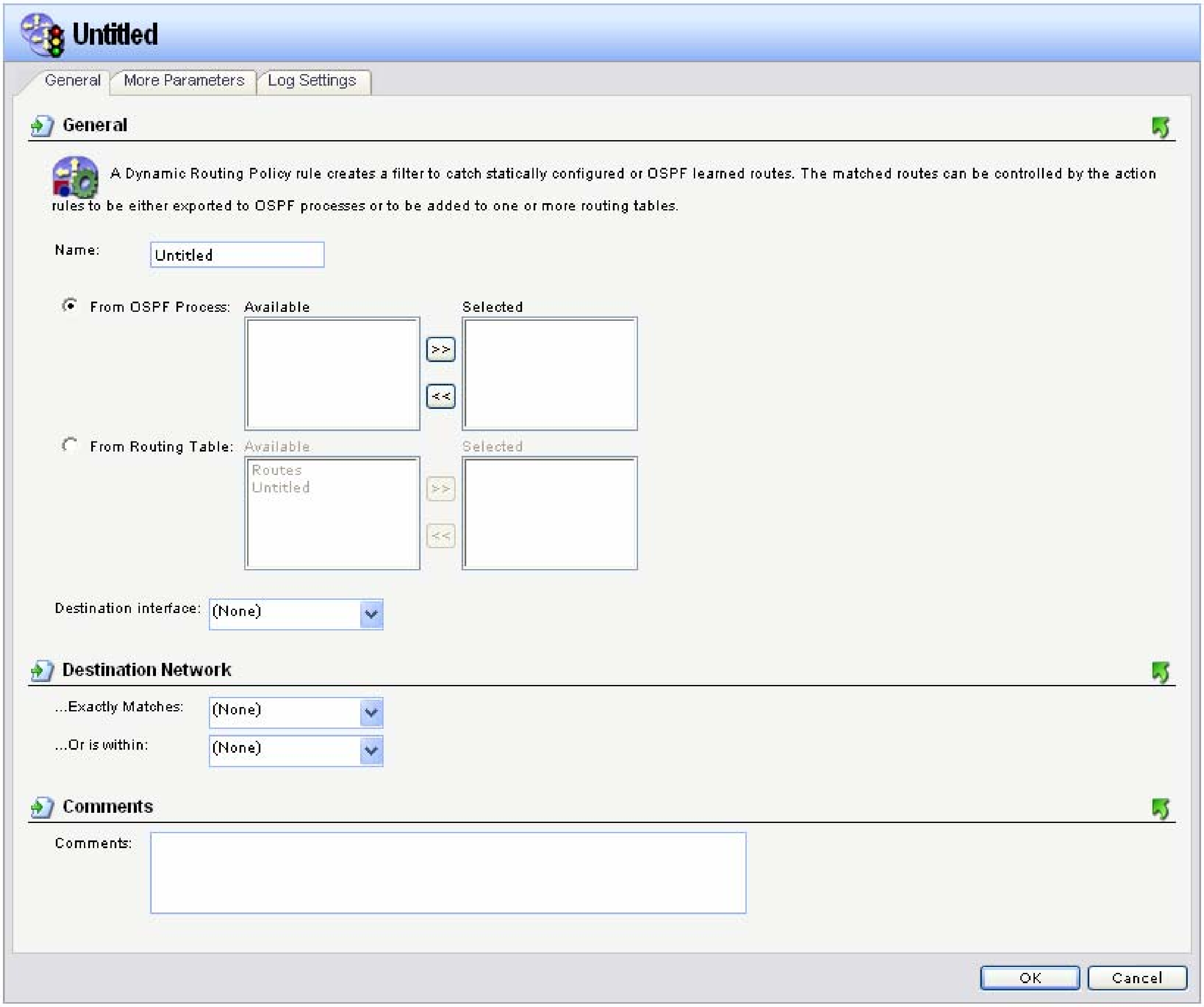


Dynamic Routing Policy

Dynamic Routing Policy defines filters to select statically configured routes or OSPF learned routes to be handled by the action rules.

#	Name	From	OSPFProcess	RoutingTable	Comments

Right-click on a row for further options.



Untitled

General

A Dynamic Routing Policy rule creates a filter to catch statically configured or OSPF learned routes. The matched routes can be controlled by the action rules to be either exported to OSPF processes or to be added to one or more routing tables.

Name: Untitled

● From OSPF Process: Available | Selected

○ From Routing Table: Available: Routes, Untitled | Selected

Destination interface: (None)

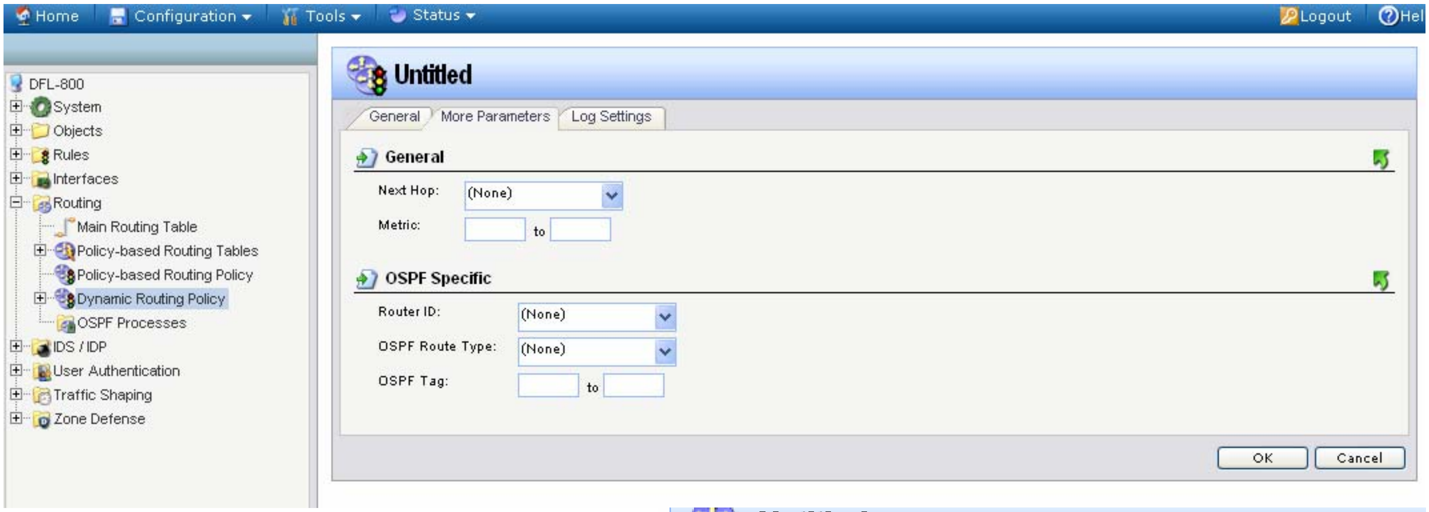
Destination Network

...Exactly Matches: (None)

...Or is within: (None)

Comments

Comments:



Untitled

General

Next Hop: (None)

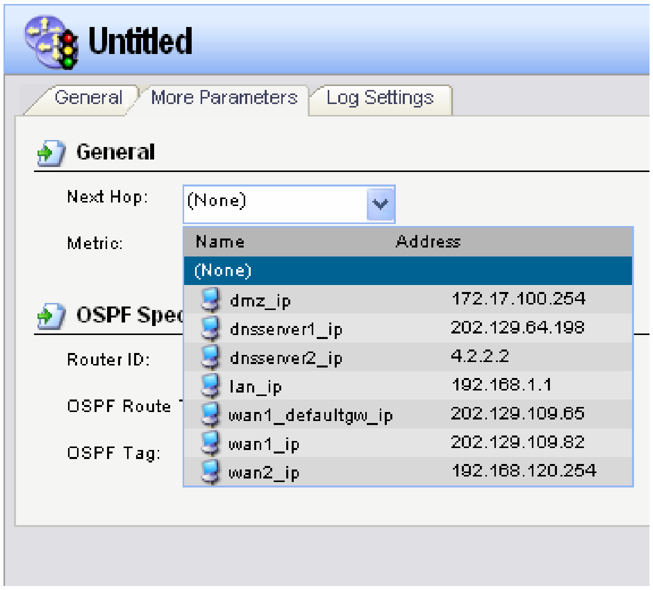
Metric: ______ to ______

OSPF Specific

Router ID: (None)

OSPF Route Type: (None)

OSPF Tag: ______ to ______



Untitled

General

Next Hop: (None)

Metric:

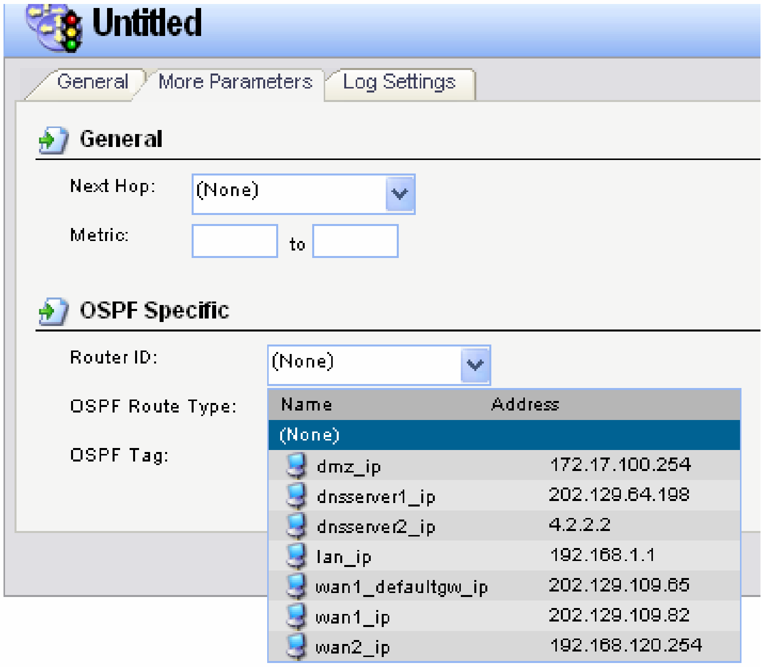
OSPF Spec

Router ID:

OSPF Route

OSPF Tag:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254



Untitled

General

Next Hop: (None)

Metric: ______ to ______

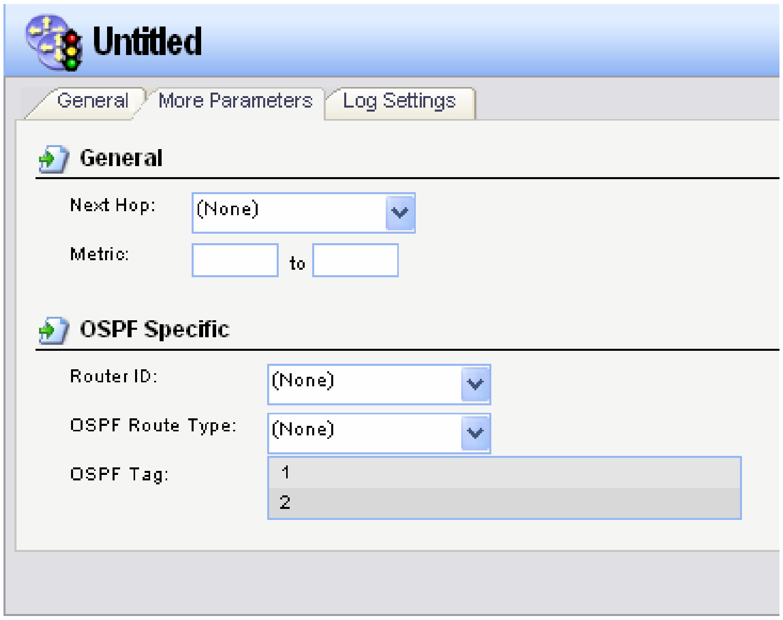
OSPF Specific

Router ID: (None)

OSPF Route Type:

OSPF Tag:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254



Untitled

General

Next Hop: (None)

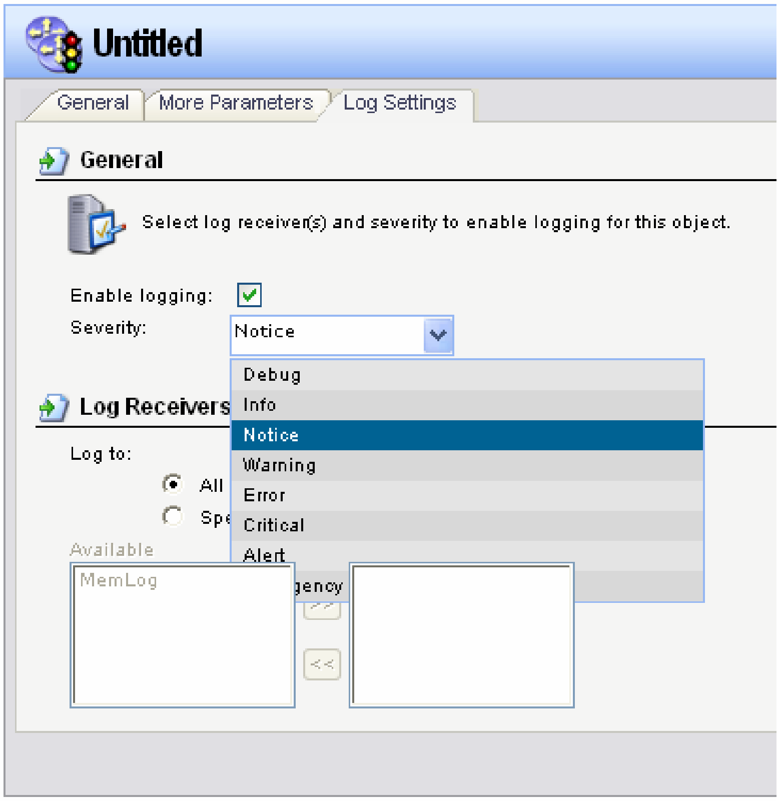
Metric: to

OSPF Specific

Router ID: (None)

OSPF Route Type: (None)

OSPF Tag: 1
2



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: ☑

Severity: Notice

Debug
Info
Notice
Warning
Error
Critical
Alert
gency

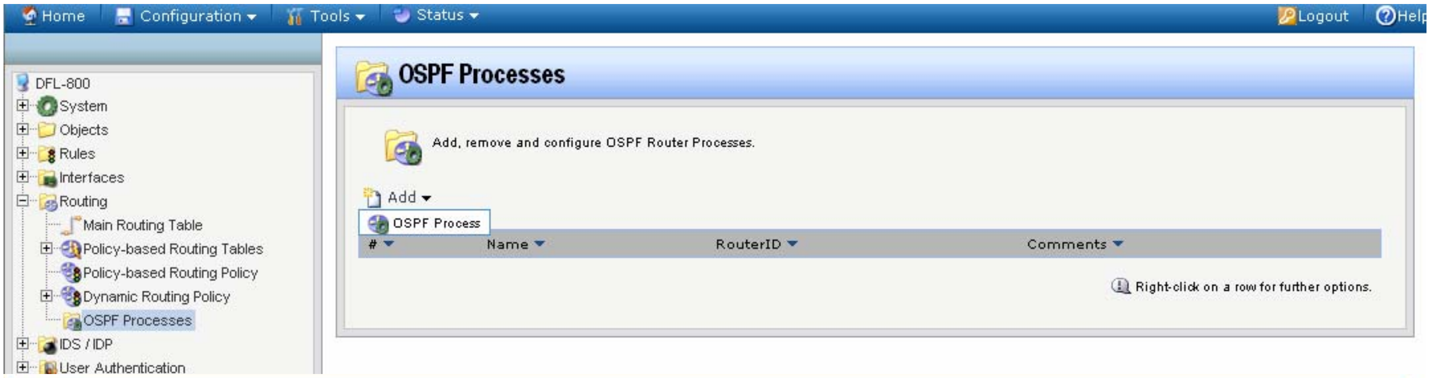
Log Receivers

Log to:

● All
○ Spe

Available

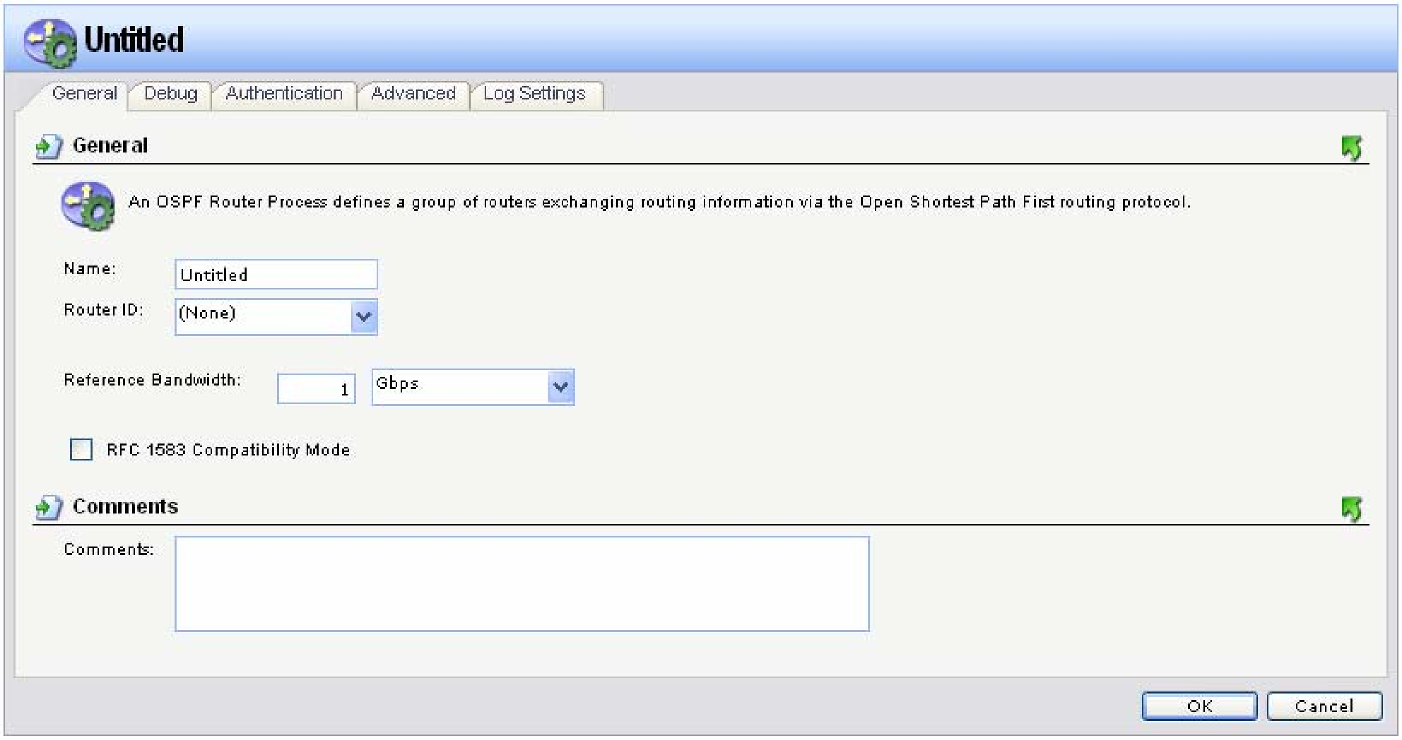
MemLog



OSPF Processes

Add, remove and configure OSPF Router Processes.

Right-click on a row for further options.



Untitled

General

An OSPF Router Process defines a group of routers exchanging routing information via the Open Shortest Path First routing protocol.

Name: Untitled

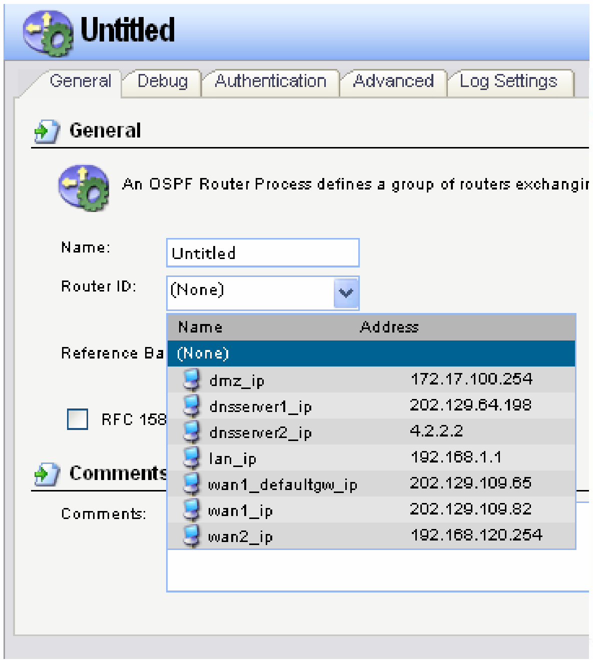
Router ID: (None)

Reference Bandwidth: 1 Gbps

□ RFC 1583 Compatibility Mode

Comments

Comments:



Untitled

General

An OSPF Router Process defines a group of routers exchangir

Name: Untitled

Router ID: (None)

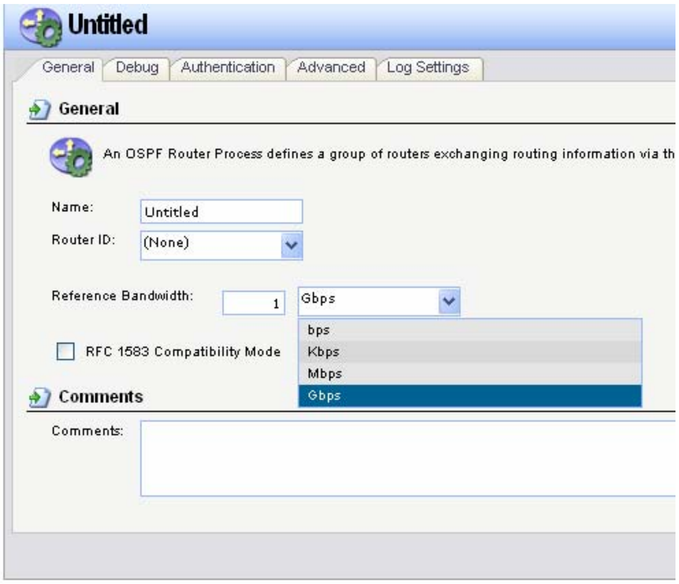
Reference Ba

□ RFC 158

Comments

Comments:

Name	Address
(None)	
dmz_ip	172.17.100.254
dnsserver1_ip	202.129.64.198
dnsserver2_ip	4.2.2.2
lan_ip	192.168.1.1
wan1_defaultgw_ip	202.129.109.65
wan1_ip	202.129.109.82
wan2_ip	192.168.120.254



Untitled

General

An OSPF Router Process defines a group of routers exchanging routing information via th

Name: Untitled

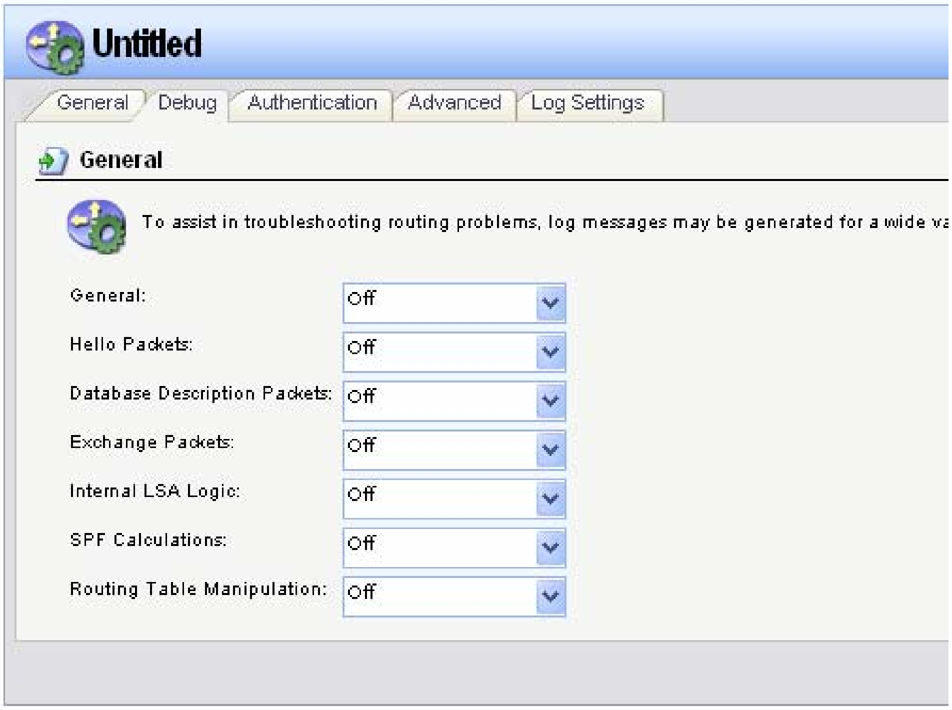
Router ID: (None)

Reference Bandwidth: 1 Gbps

□ RFC 1583 Compatibility Mode

Comments

Comments:



General

To assist in troubleshooting routing problems, log messages may be generated for a wide va

General: Off

Hello Packets: Off

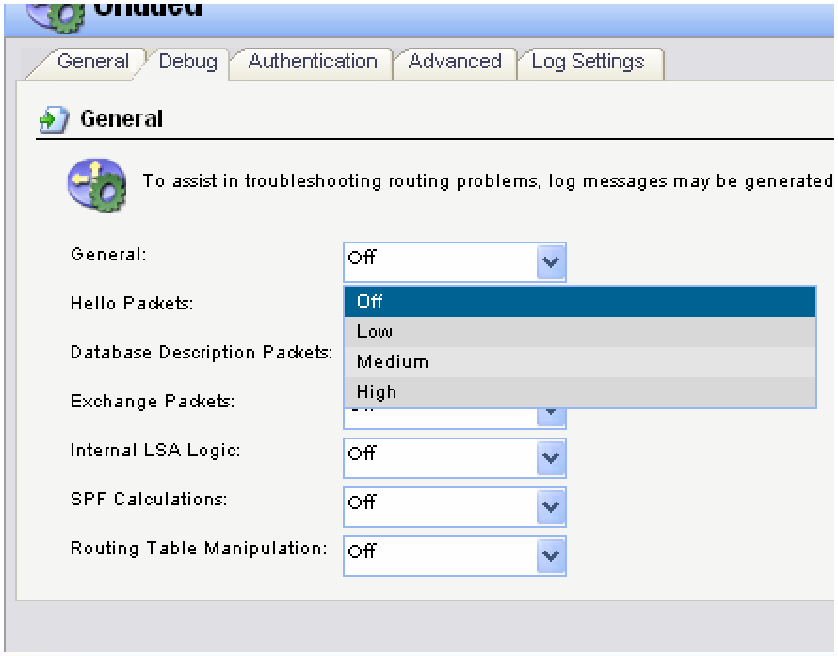
Database Description Packets: Off

Exchange Packets: Off

Internal LSA Logic: Off

SPF Calculations: Off

Routing Table Manipulation: Off



General

To assist in troubleshooting routing problems, log messages may be generated

General: Off

Hello Packets:

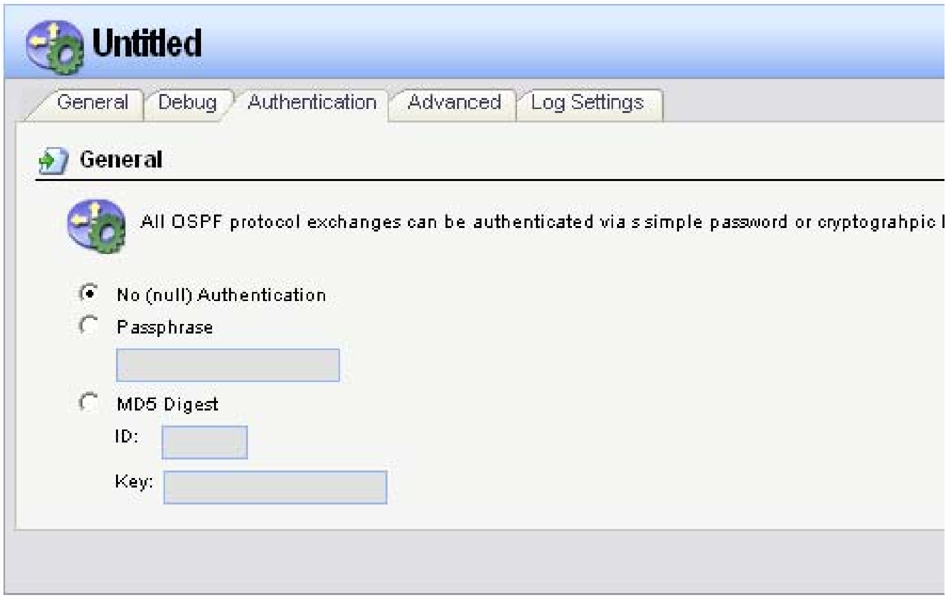
Database Description Packets:

Exchange Packets:

Internal LSA Logic: Off

SPF Calculations: Off

Routing Table Manipulation: Off



General

All OSPF protocol exchanges can be authenticated via s simple password or cryptograhpic l

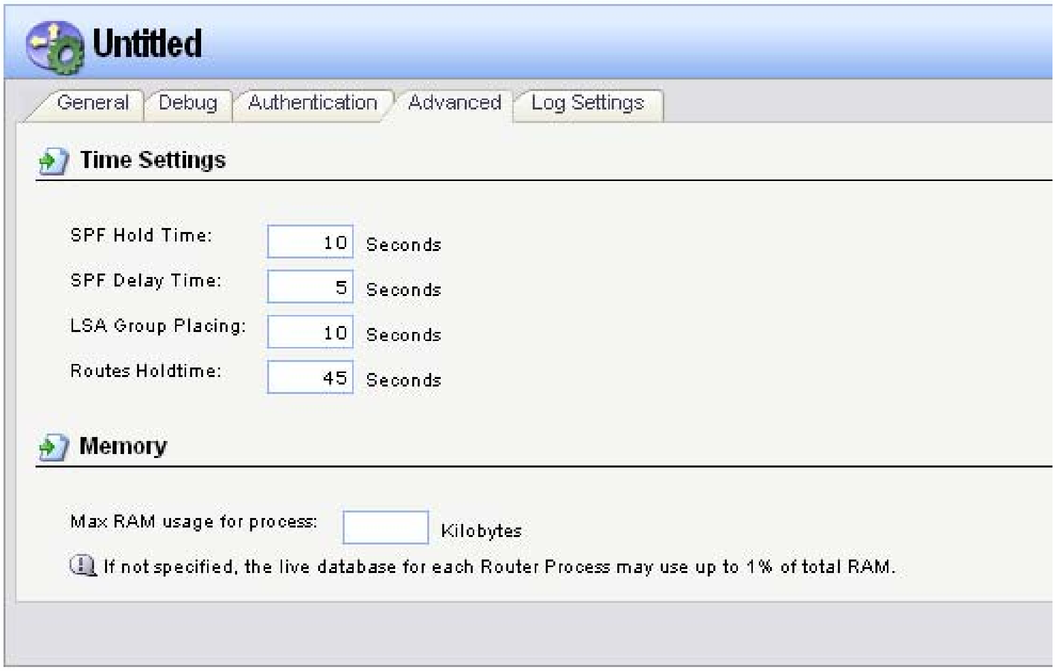
● No (null) Authentication

○ Passphrase

○ MD5 Digest

ID:

Key:



Time Settings

SPF Hold Time: 10 Seconds

SPF Delay Time: 5 Seconds

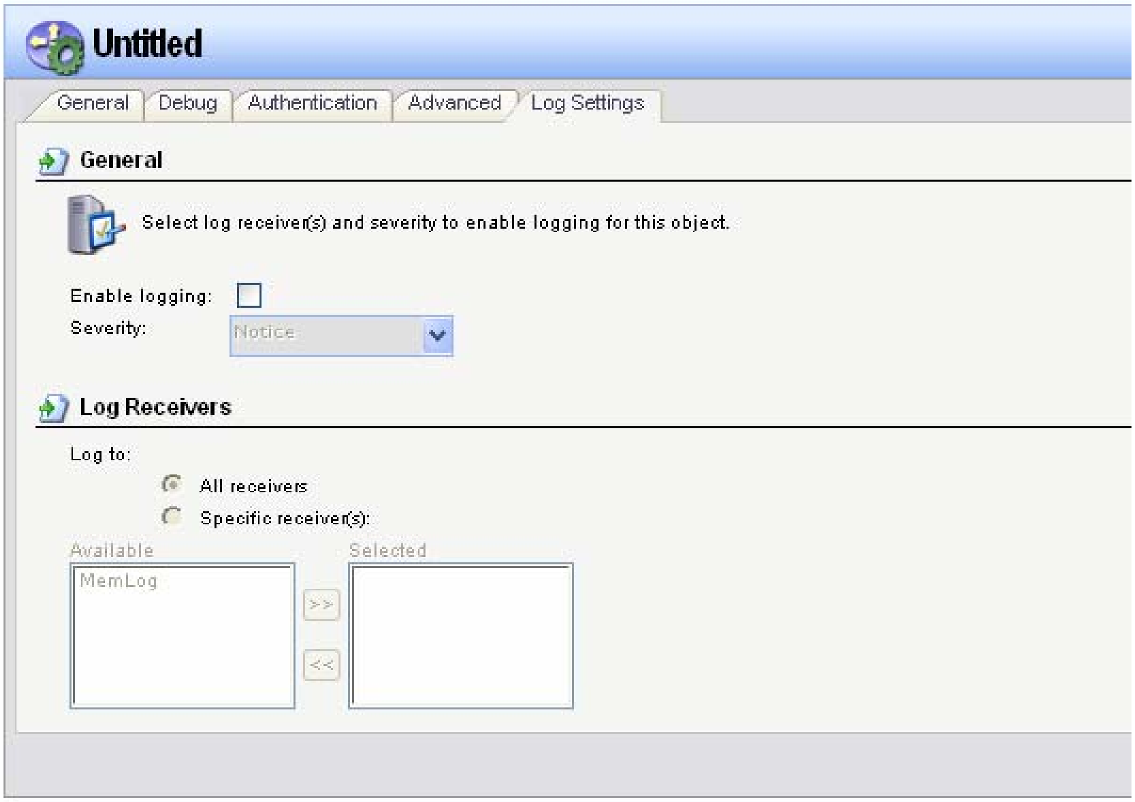
LSA Group Placing: 10 Seconds

Routes Holdtime: 45 Seconds

Memory

Max RAM usage for process: Kilobytes

If not specified, the live database for each Router Process may use up to 1% of total RAM.



General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

Log Receivers

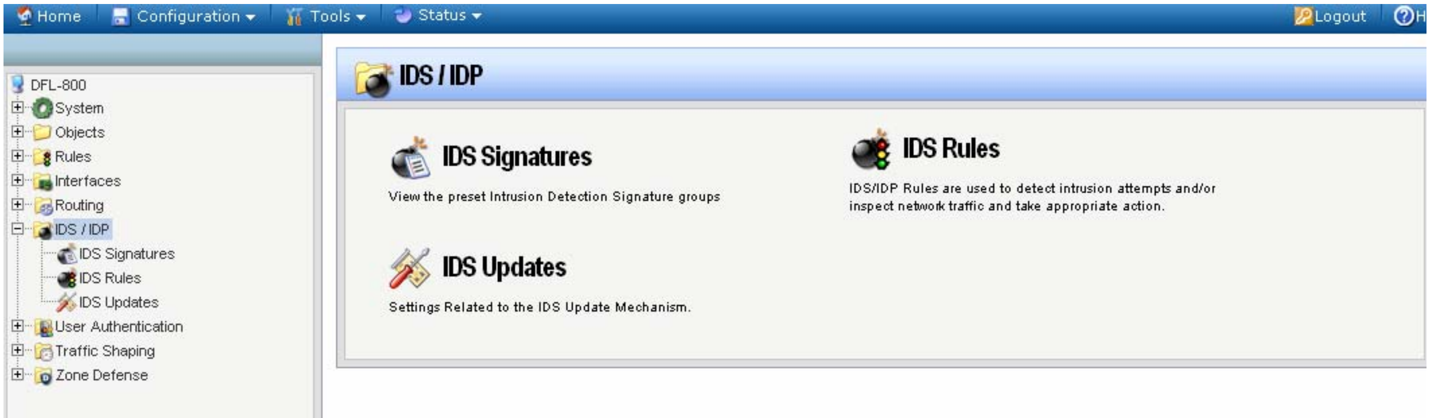
Log to:

● All receivers

○ Specific receiver(s):

Available: MemLog

Selected:



IDS / IDP

IDS Signatures

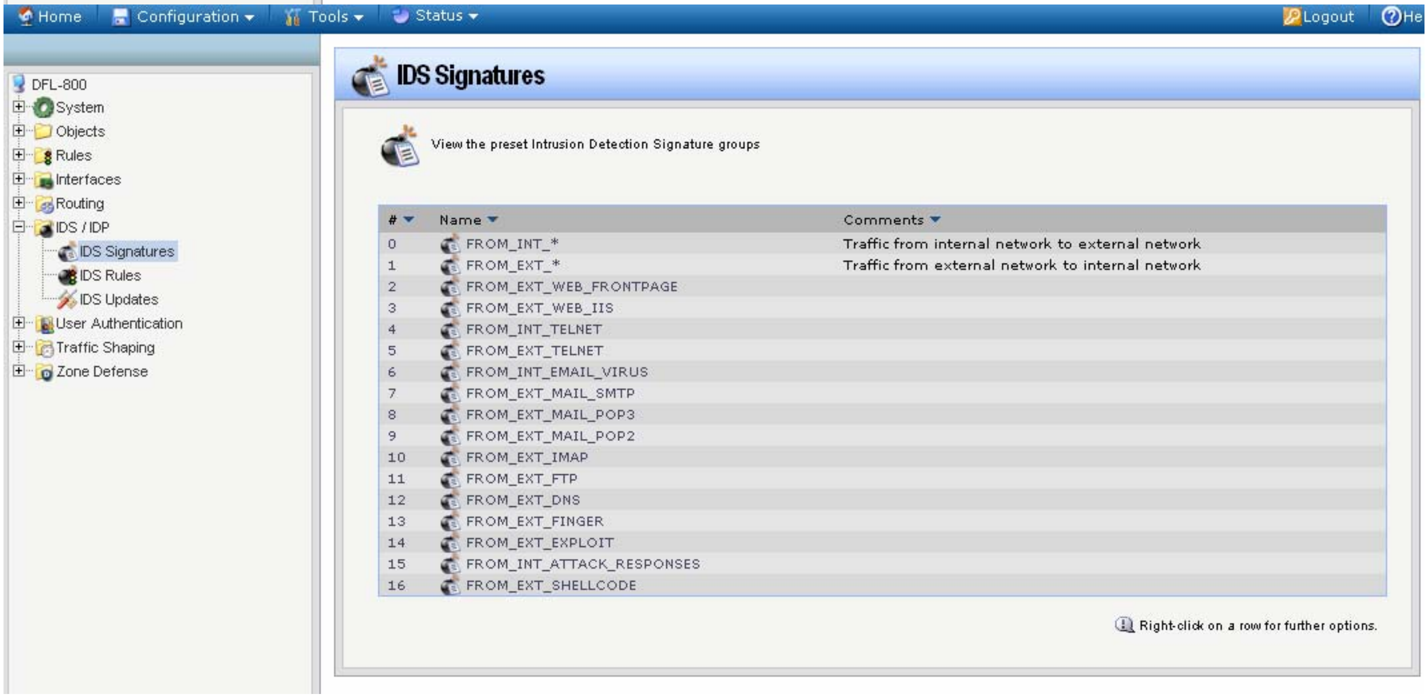
View the preset Intrusion Detection Signature groups

IDS Rules

IDS/IDP Rules are used to detect intrusion attempts and/or inspect network traffic and take appropriate action.

IDS Updates

Settings Related to the IDS Update Mechanism.

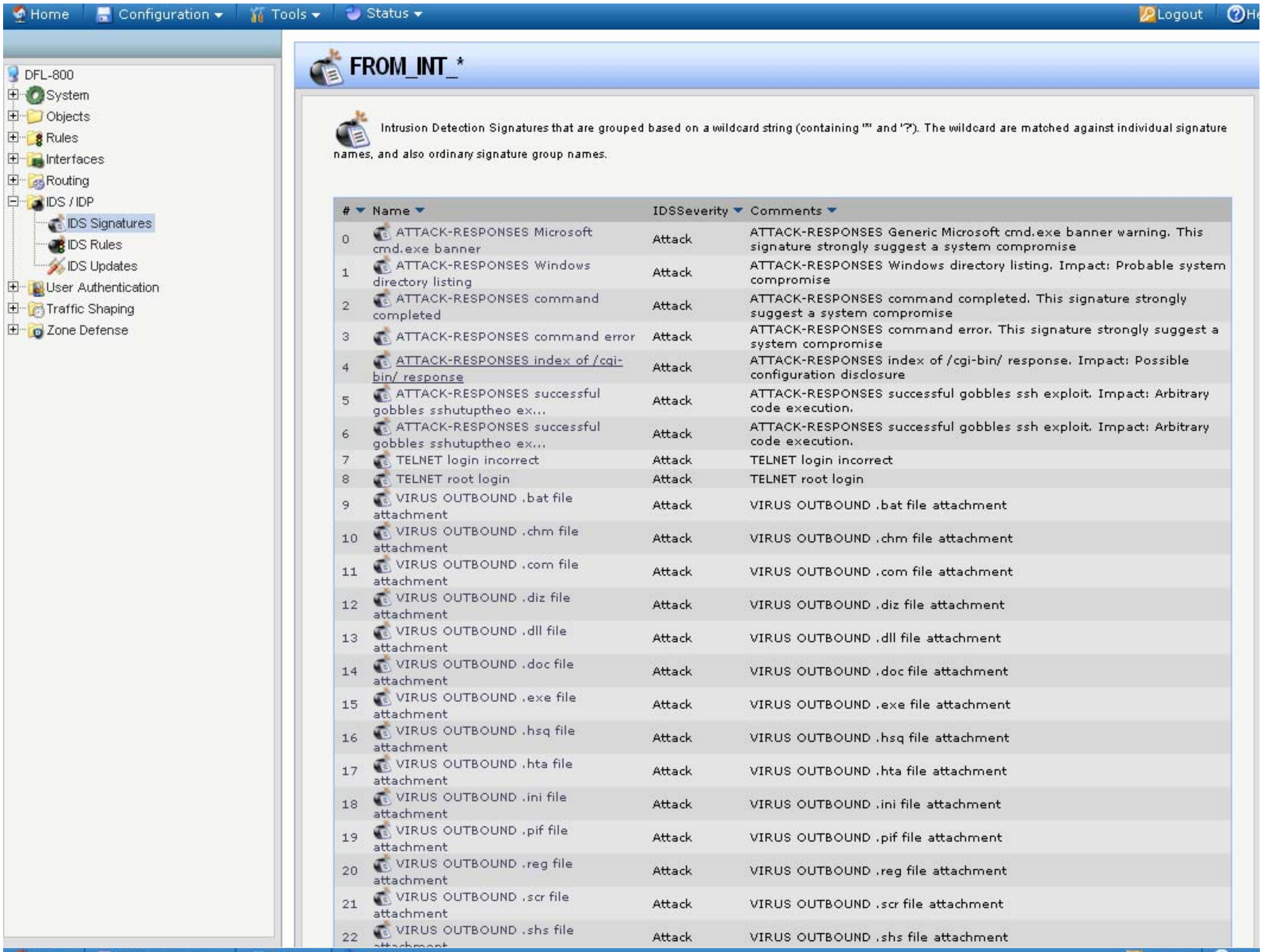


IDS Signatures

View the preset Intrusion Detection Signature groups

#	Name	Comments
0	FROM_INT_*	Traffic from internal network to external network
1	FROM_EXT_*	Traffic from external network to internal network
2	FROM_EXT_WEB_FRONTPAGE	
3	FROM_EXT_WEB_IIS	
4	FROM_INT_TELNET	
5	FROM_EXT_TELNET	
6	FROM_INT_EMAIL_VIRUS	
7	FROM_EXT_MAIL_SMTP	
8	FROM_EXT_MAIL_POP3	
9	FROM_EXT_MAIL_POP2	
10	FROM_EXT_IMAP	
11	FROM_EXT_FTP	
12	FROM_EXT_DNS	
13	FROM_EXT_FINGER	
14	FROM_EXT_EXPLOIT	
15	FROM_INT_ATTACK_RESPONSES	
16	FROM_EXT_SHELLCODE	

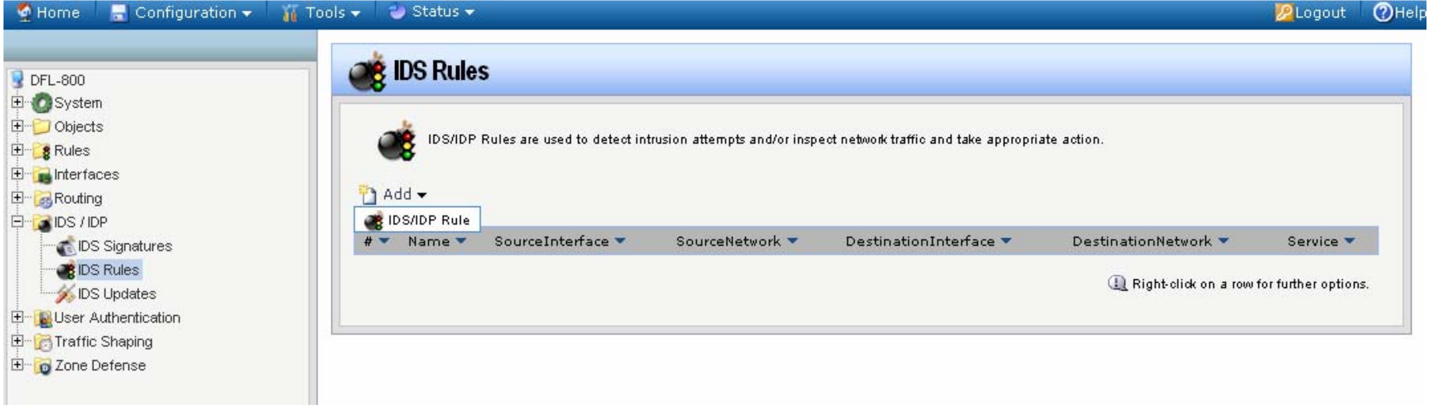
Right-click on a row for further options.



FROM_INT_*

Intrusion Detection Signatures that are grouped based on a wildcard string (containing '*' and '?'). The wildcard are matched against individual signature names, and also ordinary signature group names.

#	Name	IDSSeverity	Comments
0	ATTACK-RESPONSES Microsoft cmd.exe banner	Attack	ATTACK-RESPONSES Generic Microsoft cmd.exe banner warning. This signature strongly suggest a system compromise
1	ATTACK-RESPONSES Windows directory listing	Attack	ATTACK-RESPONSES Windows directory listing. Impact: Probable system compromise
2	ATTACK-RESPONSES command completed	Attack	ATTACK-RESPONSES command completed. This signature strongly suggest a system compromise
3	ATTACK-RESPONSES command error	Attack	ATTACK-RESPONSES command error. This signature strongly suggest a system compromise
4	ATTACK-RESPONSES index of /cgi-bin/ response	Attack	ATTACK-RESPONSES index of /cgi-bin/ response. Impact: Possible configuration disclosure
5	ATTACK-RESPONSES successful gobbles sshutuptheo ex...	Attack	ATTACK-RESPONSES successful gobbles ssh exploit. Impact: Arbitrary code execution.
6	ATTACK-RESPONSES successful gobbles sshutuptheo ex...	Attack	ATTACK-RESPONSES successful gobbles ssh exploit. Impact: Arbitrary code execution.
7	TELNET login incorrect	Attack	TELNET login incorrect
8	TELNET root login	Attack	TELNET root login
9	VIRUS OUTBOUND .bat file attachment	Attack	VIRUS OUTBOUND .bat file attachment
10	VIRUS OUTBOUND .chm file attachment	Attack	VIRUS OUTBOUND .chm file attachment
11	VIRUS OUTBOUND .com file attachment	Attack	VIRUS OUTBOUND .com file attachment
12	VIRUS OUTBOUND .diz file attachment	Attack	VIRUS OUTBOUND .diz file attachment
13	VIRUS OUTBOUND .dll file attachment	Attack	VIRUS OUTBOUND .dll file attachment
14	VIRUS OUTBOUND .doc file attachment	Attack	VIRUS OUTBOUND .doc file attachment
15	VIRUS OUTBOUND .exe file attachment	Attack	VIRUS OUTBOUND .exe file attachment
16	VIRUS OUTBOUND .hsq file attachment	Attack	VIRUS OUTBOUND .hsq file attachment
17	VIRUS OUTBOUND .hta file attachment	Attack	VIRUS OUTBOUND .hta file attachment
18	VIRUS OUTBOUND .ini file attachment	Attack	VIRUS OUTBOUND .ini file attachment
19	VIRUS OUTBOUND .pif file attachment	Attack	VIRUS OUTBOUND .pif file attachment
20	VIRUS OUTBOUND .reg file attachment	Attack	VIRUS OUTBOUND .reg file attachment
21	VIRUS OUTBOUND .scr file attachment	Attack	VIRUS OUTBOUND .scr file attachment
22	VIRUS OUTBOUND .shs file attachment	Attack	VIRUS OUTBOUND .shs file attachment

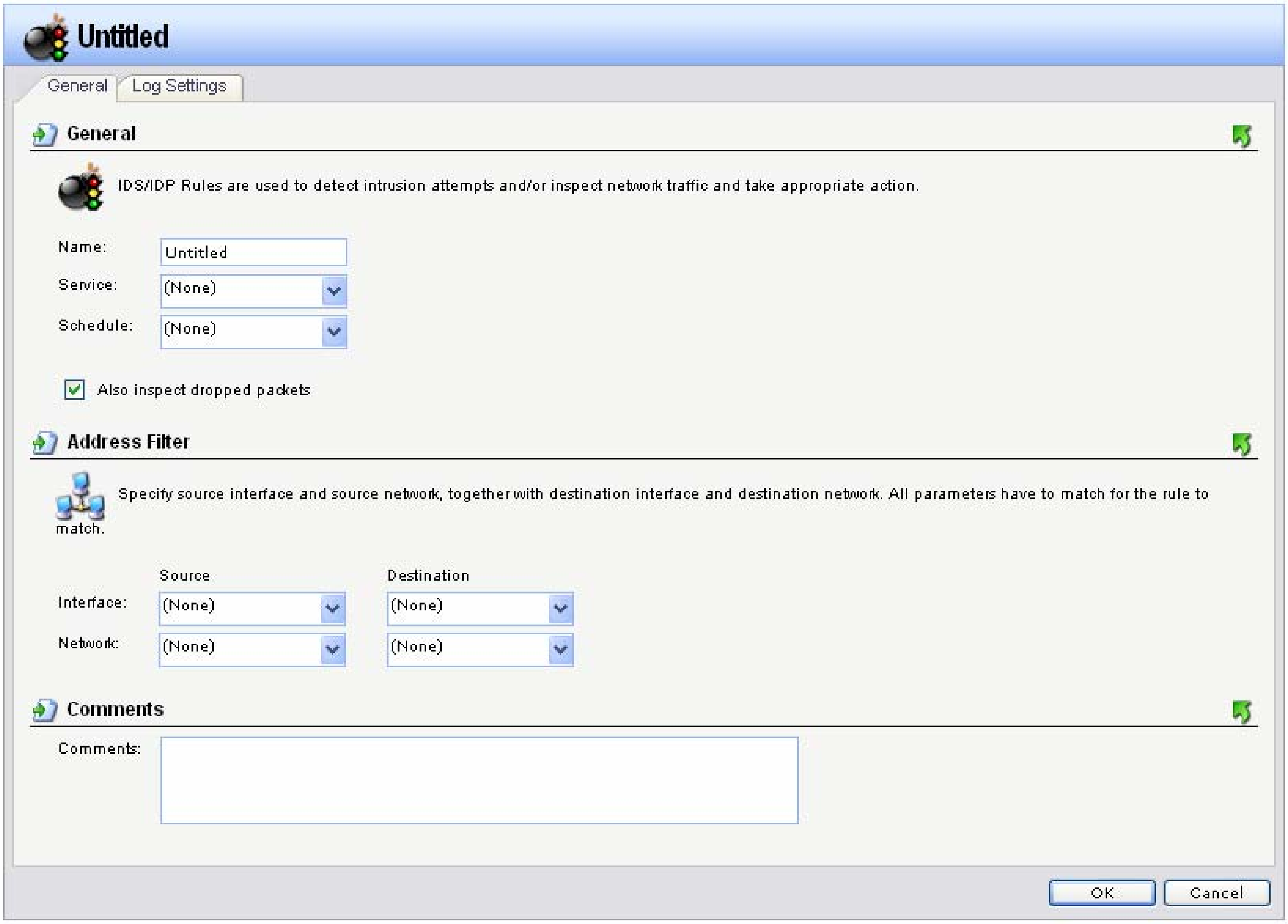


IDS Rules

IDS/IDP Rules are used to detect intrusion attempts and/or inspect network traffic and take appropriate action.

#	Name	SourceInterface	SourceNetwork	DestinationInterface	DestinationNetwork	Service

Right-click on a row for further options.



General

IDS/IDP Rules are used to detect intrusion attempts and/or inspect network traffic and take appropriate action.

Name: Untitled

Service: (None)

Schedule: (None)

☑ Also inspect dropped packets

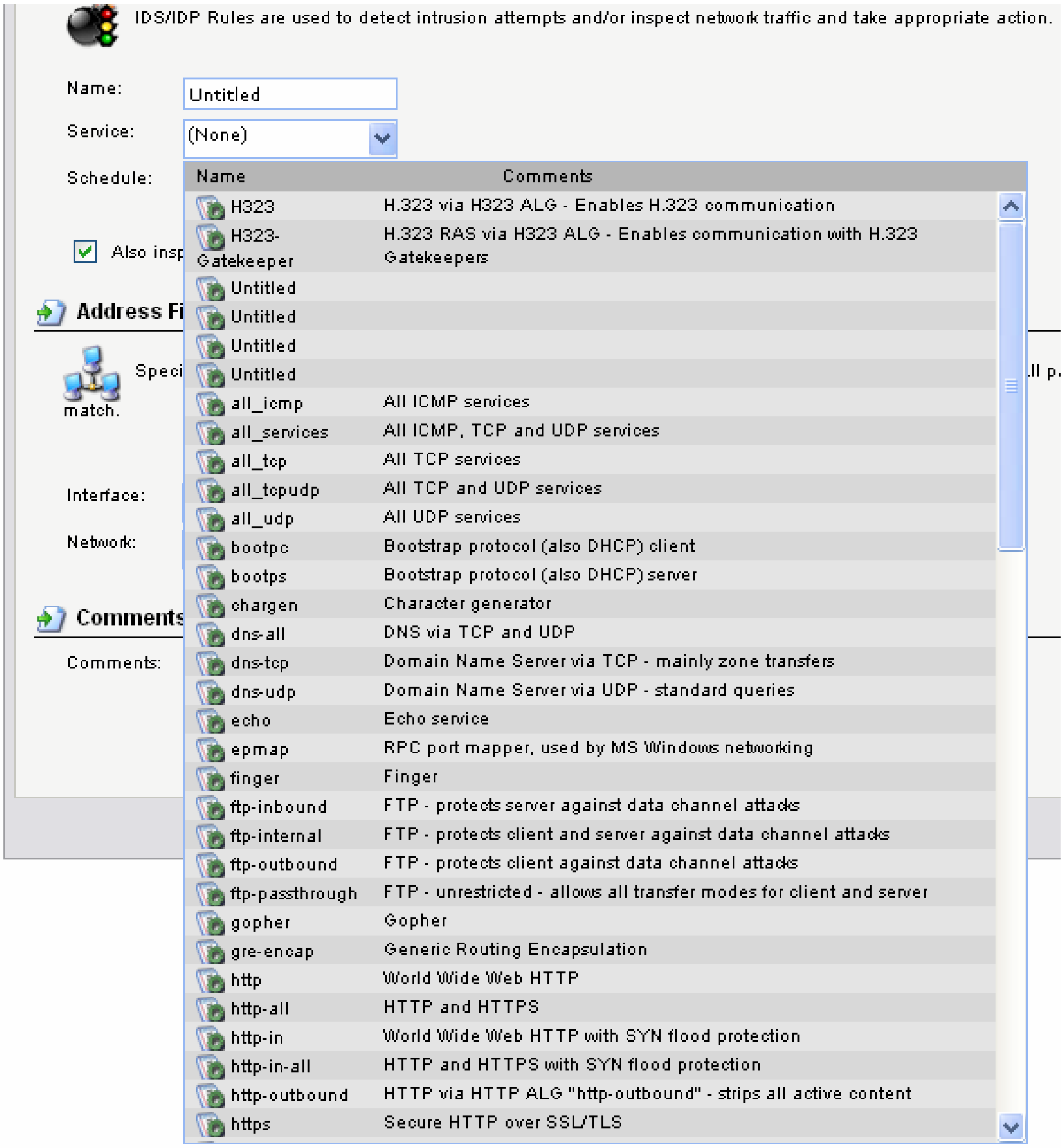
Address Filter

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

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:



IDS/IDP Rules are used to detect intrusion attempts and/or inspect network traffic and take appropriate action.

Name: Untitled

Service: (None)

Schedule:

☑ Also insp

Address Fi

Speci ... ll p.

match.

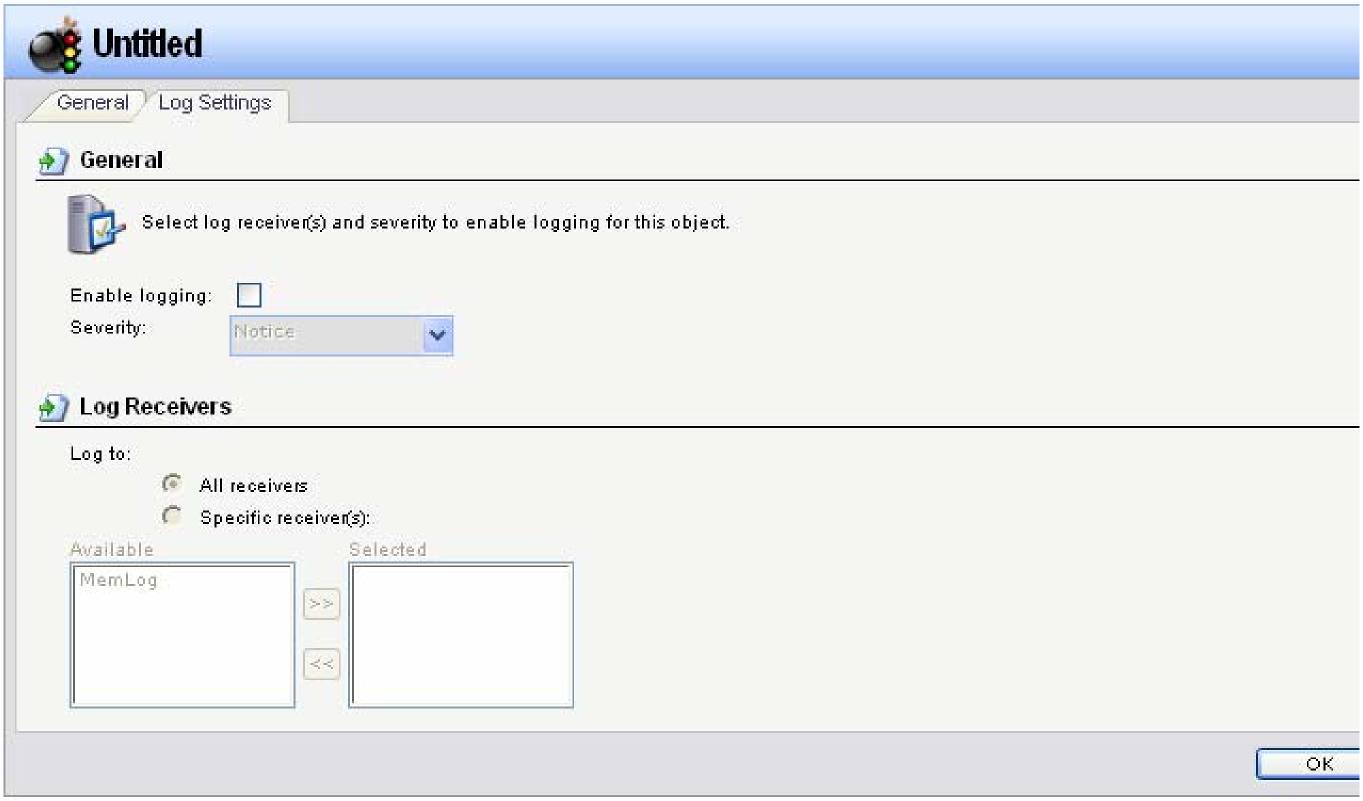
Interface:

Network:

Comments

Comments:

Name	Comments
H323	H.323 via H323 ALG - Enables H.323 communication
H323-Gatekeeper	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers
Untitled	
Untitled	
Untitled	
Untitled	
all_icmp	All ICMP services
all_services	All ICMP, TCP and UDP services
all_tcp	All TCP services
all_tcpudp	All TCP and UDP services
all_udp	All UDP services
bootpc	Bootstrap protocol (also DHCP) client
bootps	Bootstrap protocol (also DHCP) server
chargen	Character generator
dns-all	DNS via TCP and UDP
dns-tcp	Domain Name Server via TCP - mainly zone transfers
dns-udp	Domain Name Server via UDP - standard queries
echo	Echo service
epmap	RPC port mapper, used by MS Windows networking
finger	Finger
ftp-inbound	FTP - protects server against data channel attacks
ftp-internal	FTP - protects client and server against data channel attacks
ftp-outbound	FTP - protects client against data channel attacks
ftp-passthrough	FTP - unrestricted - allows all transfer modes for client and server
gopher	Gopher
gre-encap	Generic Routing Encapsulation
http	World Wide Web HTTP
http-all	HTTP and HTTPS
http-in	World Wide Web HTTP with SYN flood protection
http-in-all	HTTP and HTTPS with SYN flood protection
http-outbound	HTTP via HTTP ALG "http-outbound" - strips all active content
https	Secure HTTP over SSL/TLS



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

Log Receivers

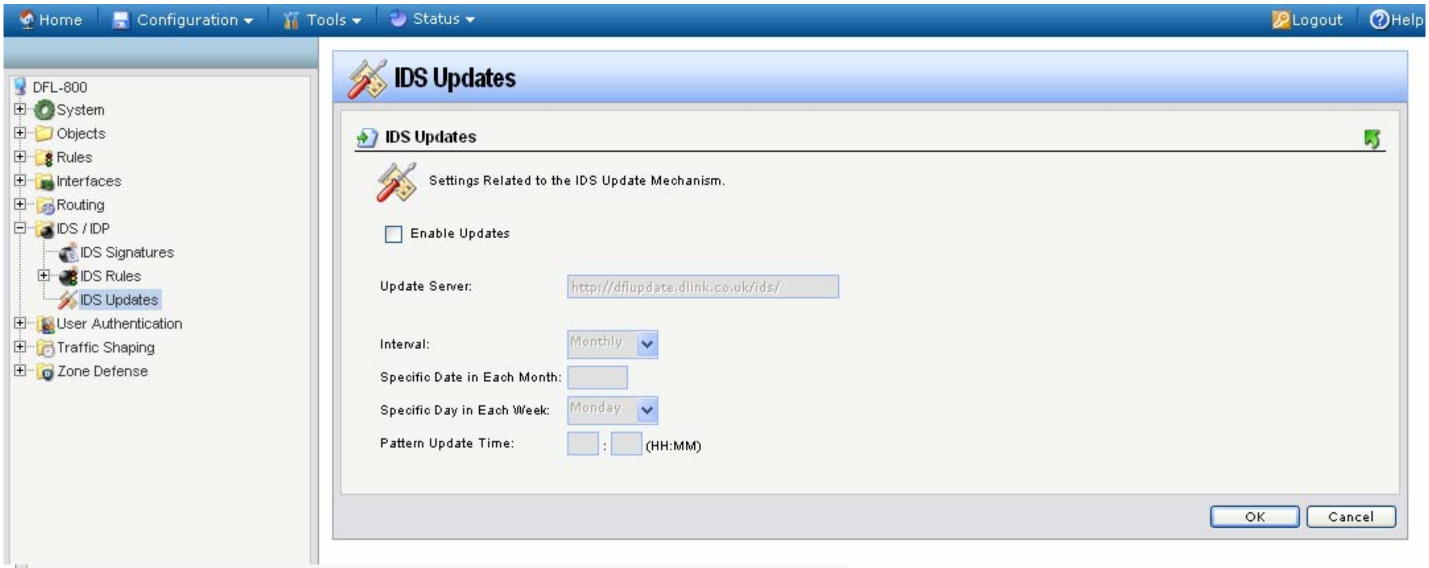
Log to:

● All receivers

○ Specific receiver(s):

Available: MemLog

Selected:



IDS Updates

IDS Updates

Settings Related to the IDS Update Mechanism.

□ Enable Updates

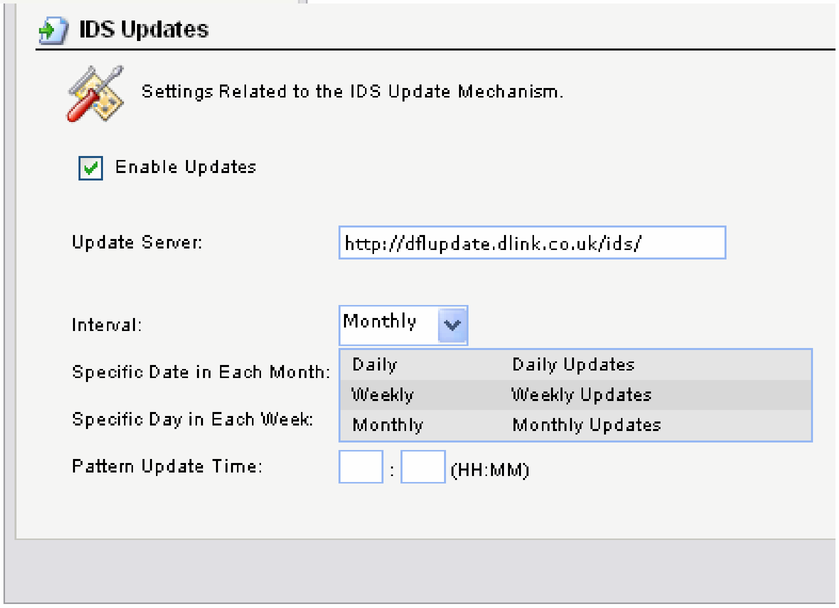
Update Server: http://dflupdate.dlink.co.uk/ids/

Interval: Monthly

Specific Date in Each Month:

Specific Day in Each Week: Monday

Pattern Update Time: : (HH:MM)



IDS Updates

Settings Related to the IDS Update Mechanism.

☑ Enable Updates

Update Server: http://dflupdate.dlink.co.uk/ids/

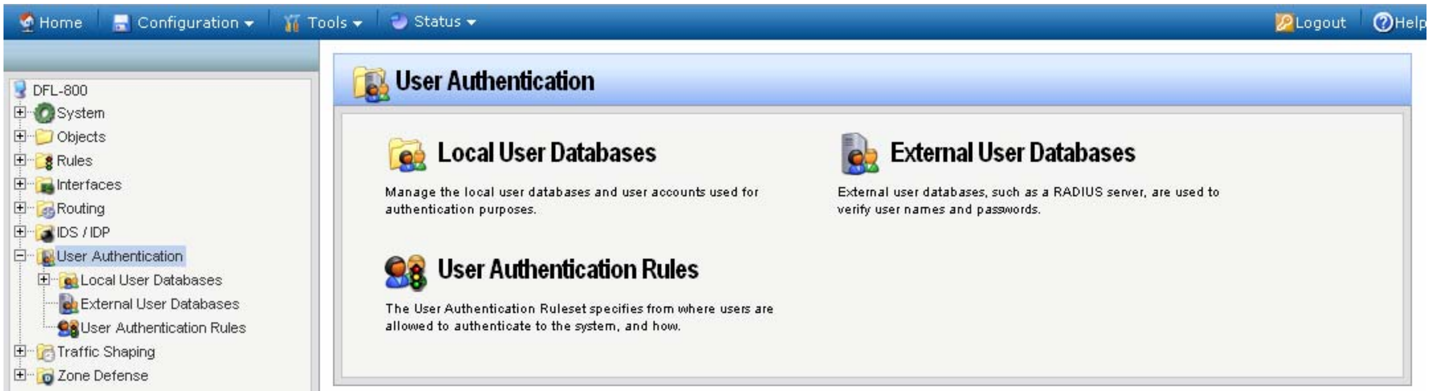
Interval: Monthly

Specific Date in Each Month:

Specific Day in Each Week:

Pattern Update Time: : (HH:MM)

Daily	Daily Updates
Weekly	Weekly Updates
Monthly	Monthly Updates



User Authentication

Local User Databases

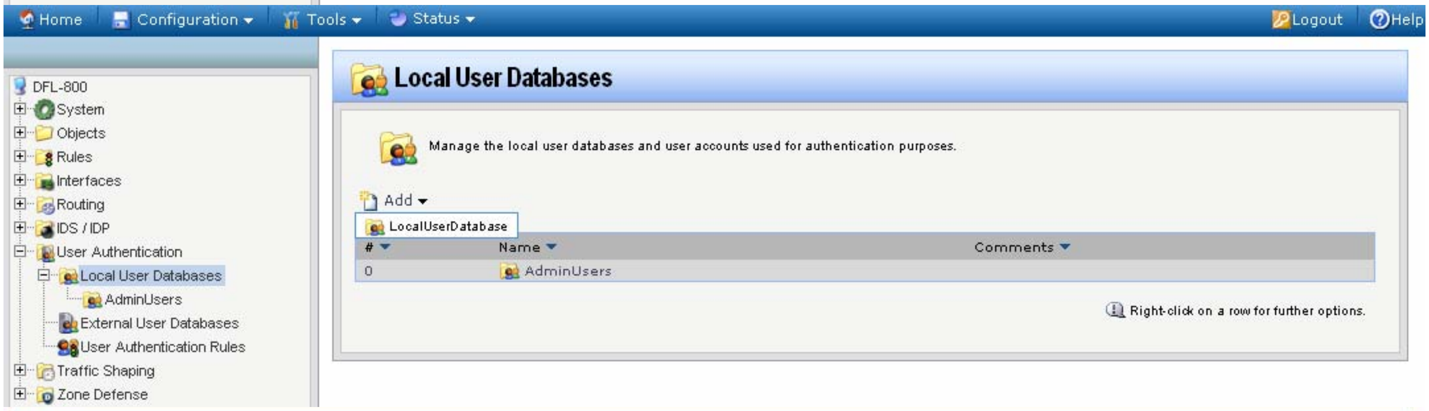
Manage the local user databases and user accounts used for authentication purposes.

External User Databases

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

User Authentication Rules

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

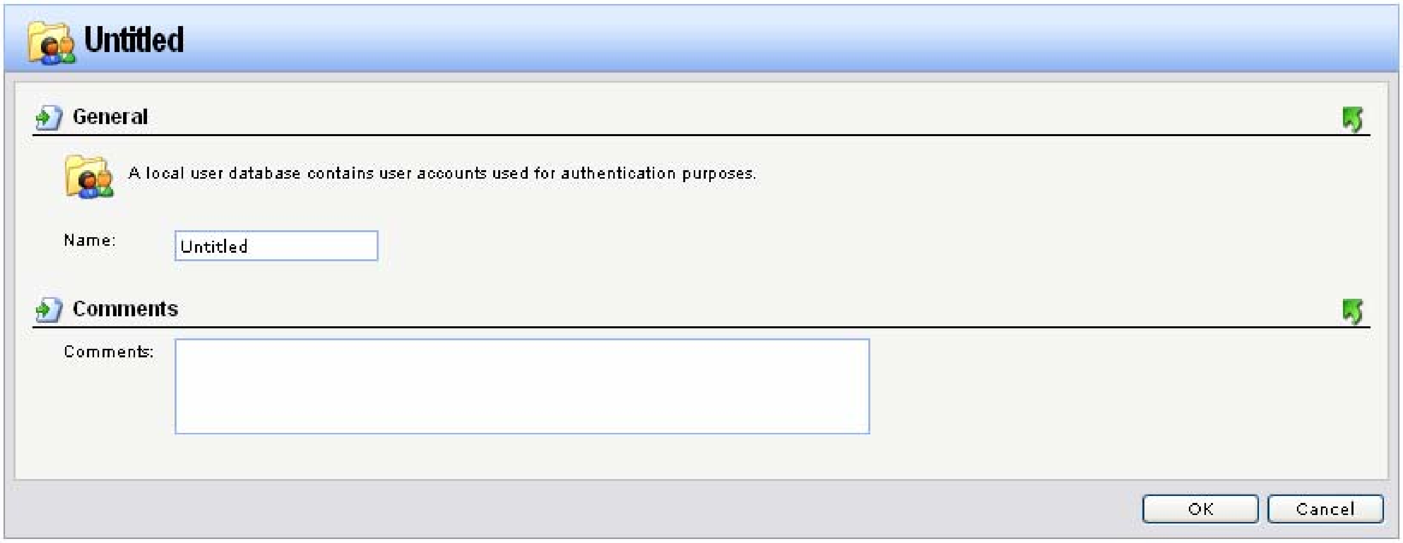


Local User Databases

Manage the local user databases and user accounts used for authentication purposes.

#	Name	Comments
0	AdminUsers	

Right-click on a row for further options.



Untitled

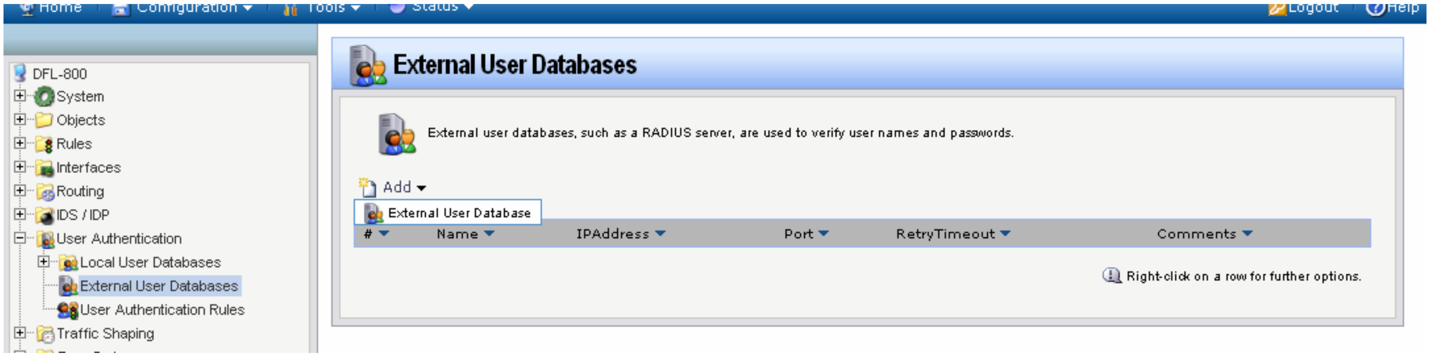
General

A local user database contains user accounts used for authentication purposes.

Name: Untitled

Comments

Comments:

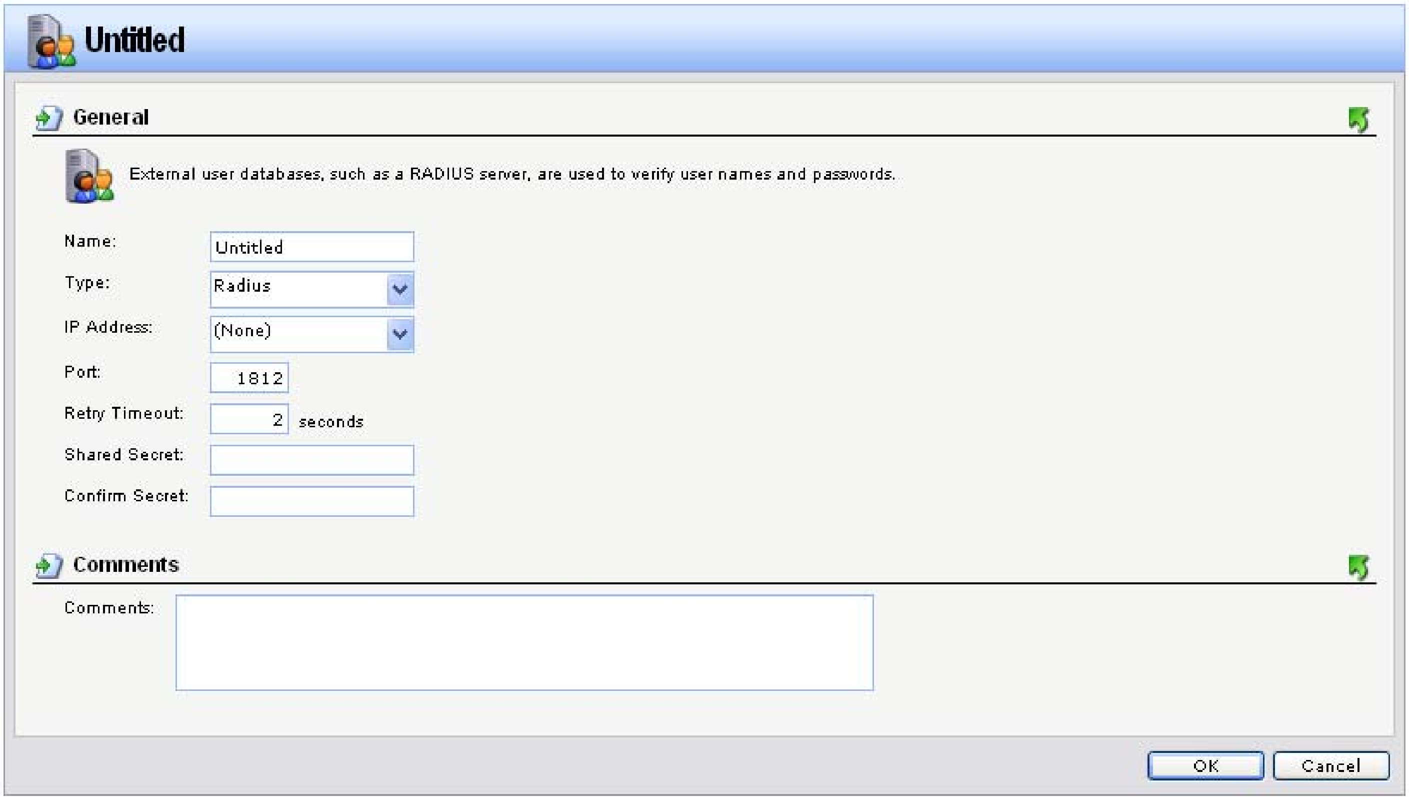


External User Databases

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

#	Name	IPAddress	Port	RetryTimeout	Comments

Right-click on a row for further options.



Untitled

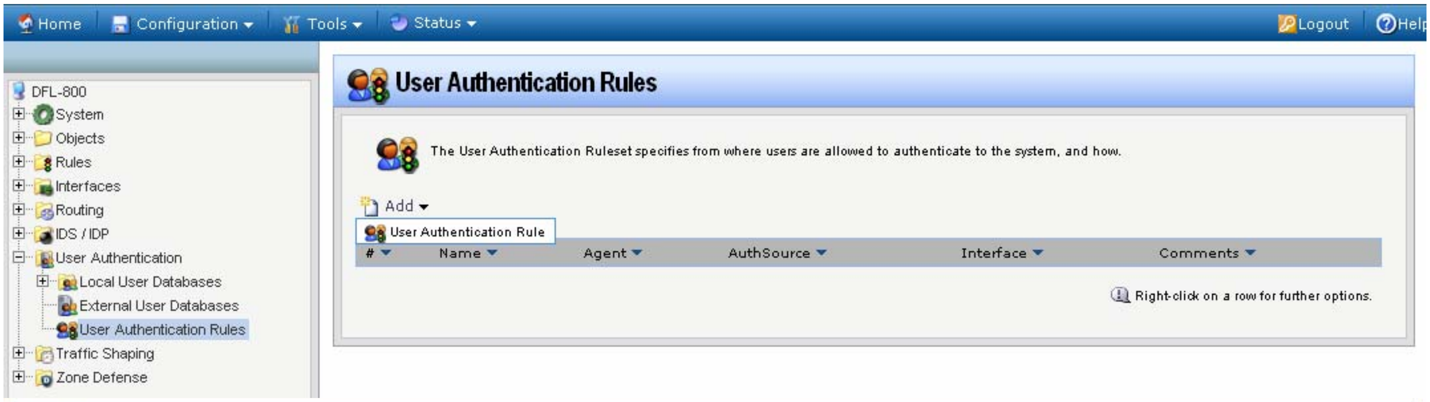
General

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

Name:	Untitled
Type:	Radius
IP Address:	(None)
Port:	1812
Retry Timeout:	2 seconds
Shared Secret:	
Confirm Secret:	

Comments

Comments:

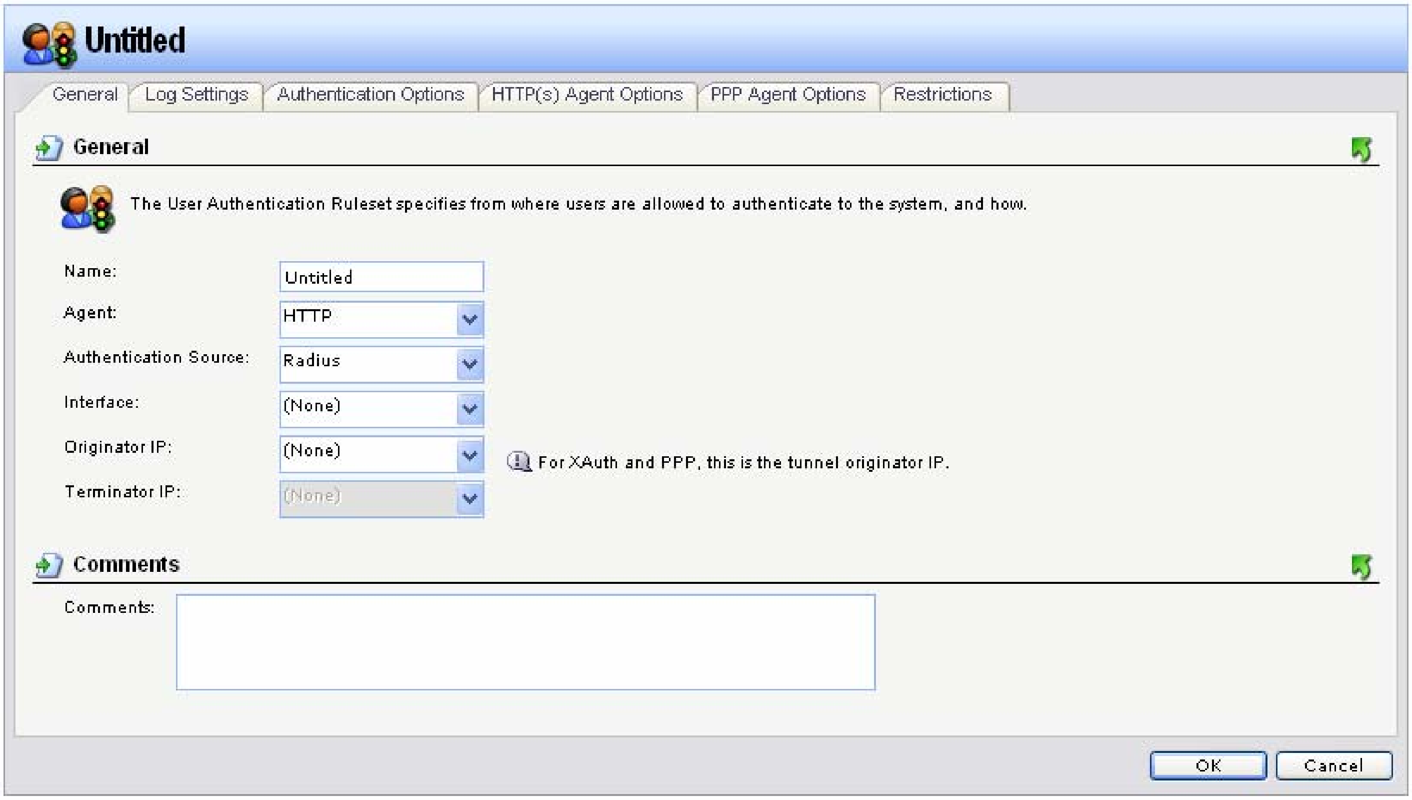


User Authentication Rules

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

#	Name	Agent	AuthSource	Interface	Comments

Right-click on a row for further options.



Untitled

General

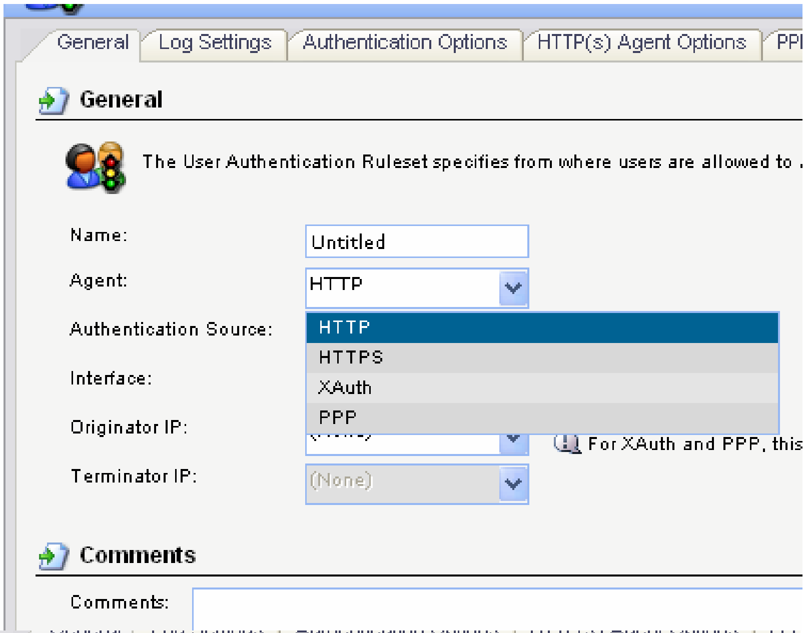
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

Name:	Untitled
Agent:	HTTP
Authentication Source:	Radius
Interface:	(None)
Originator IP:	(None)
Terminator IP:	(None)

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

Comments

Comments:



General

The User Authentication Ruleset specifies from where users are allowed to a

Name: Untitled

Agent: HTTP

Authentication Source:

Interface:

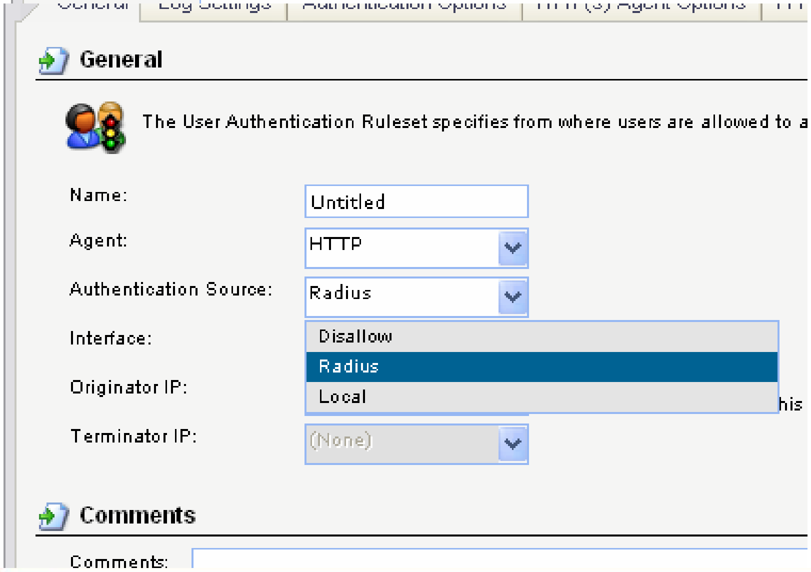
Originator IP:

Terminator IP: (None)

For XAuth and PPP, this

Comments

Comments:



General

The User Authentication Ruleset specifies from where users are allowed to a

Name: Untitled

Agent: HTTP

Authentication Source: Radius

Interface:

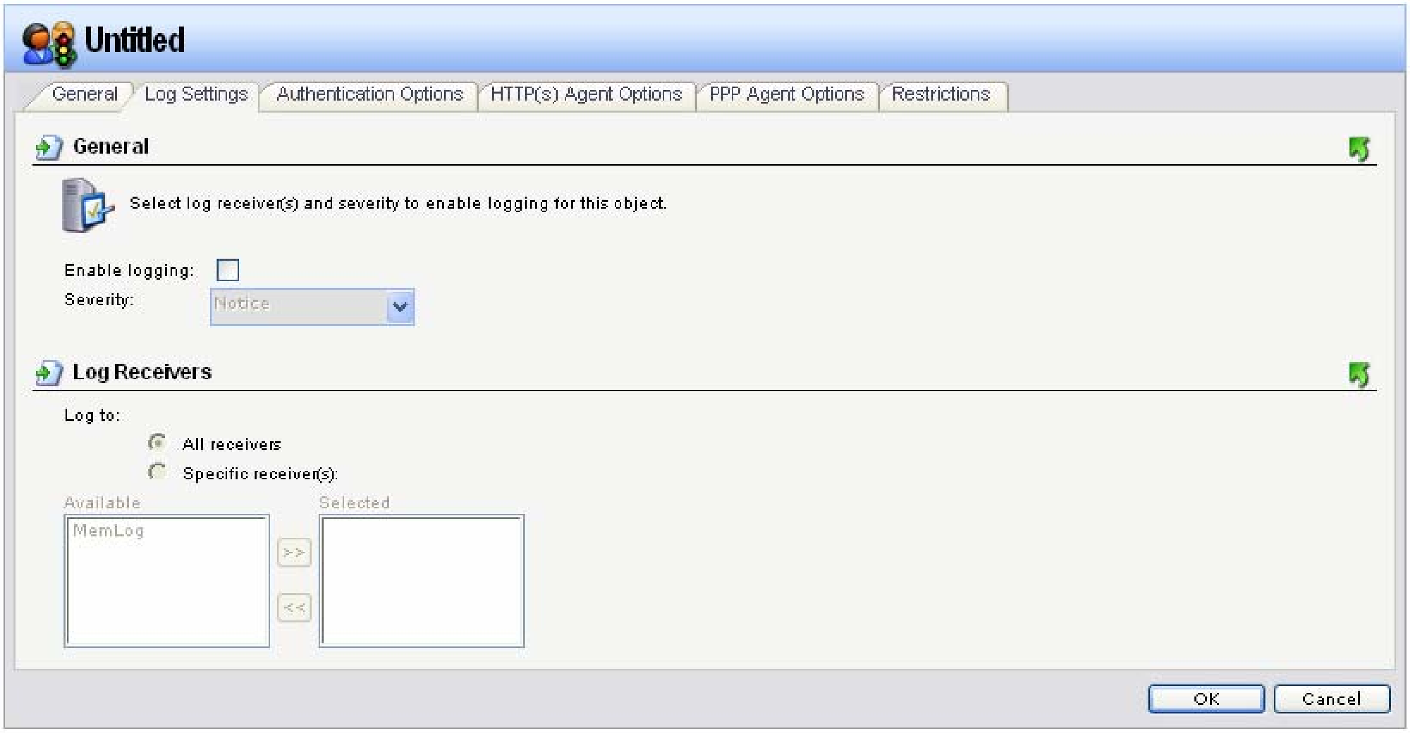
Originator IP:

Terminator IP: (None)

his

Comments

Comments:


Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

Log Receivers

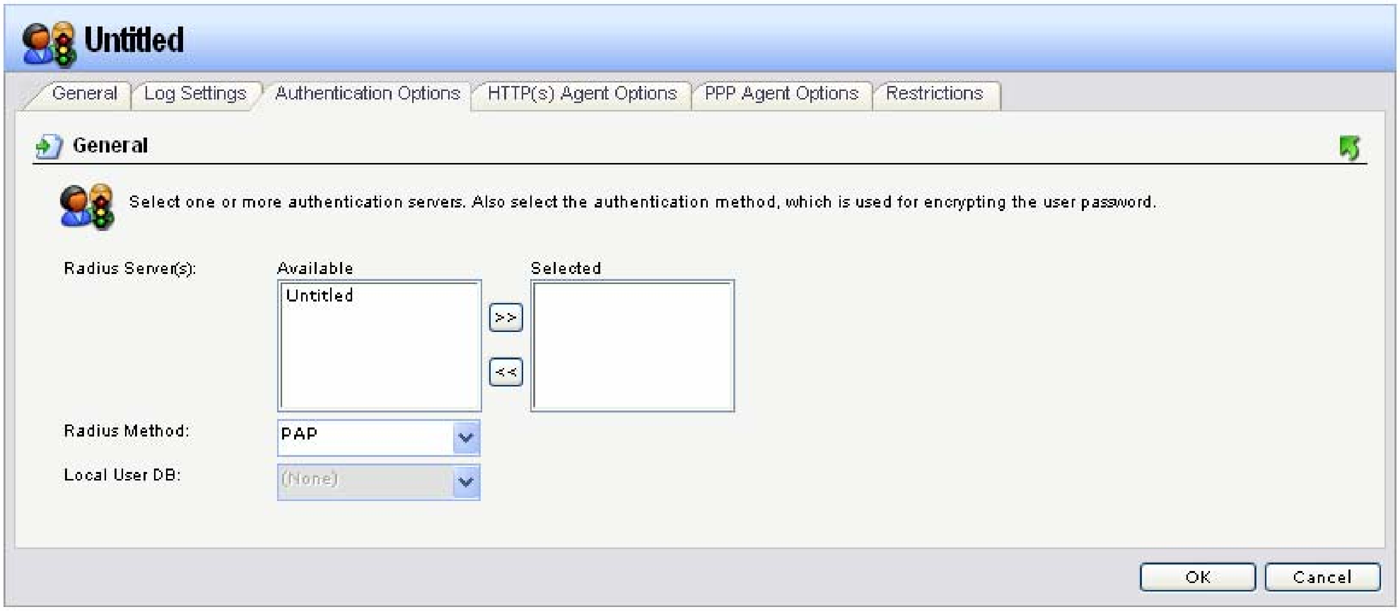
Log to:

● All receivers

○ Specific receiver(s):

Available: MemLog

Selected:



Untitled

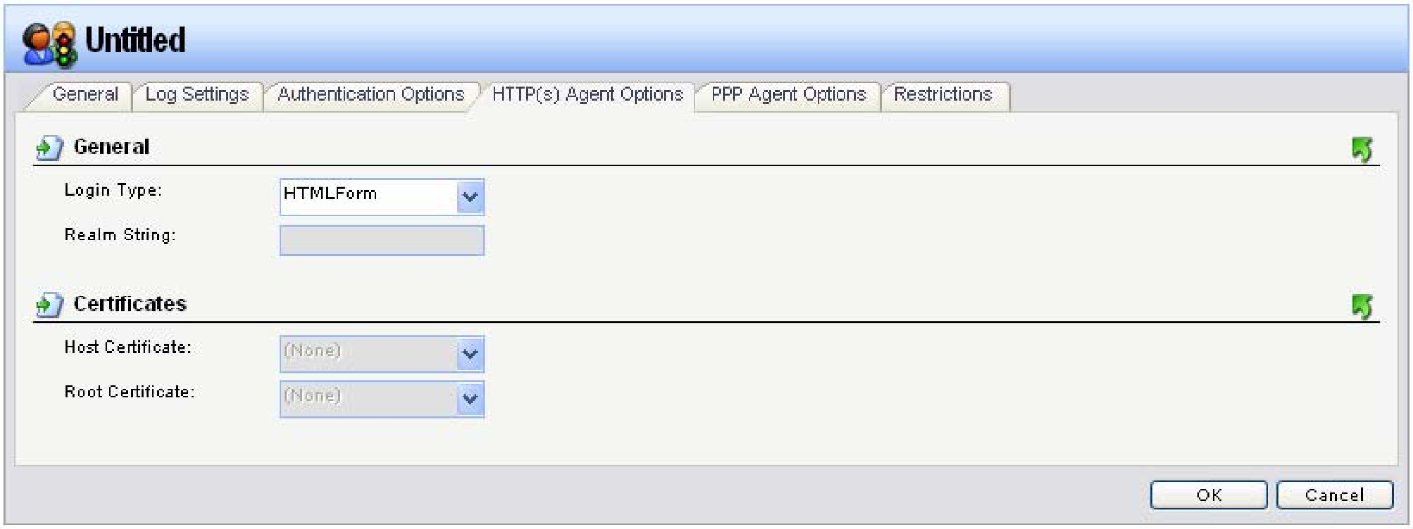
General

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

Radius Server(s): Available: Untitled; Selected:

Radius Method: PAP

Local User DB: (None)



Untitled

General

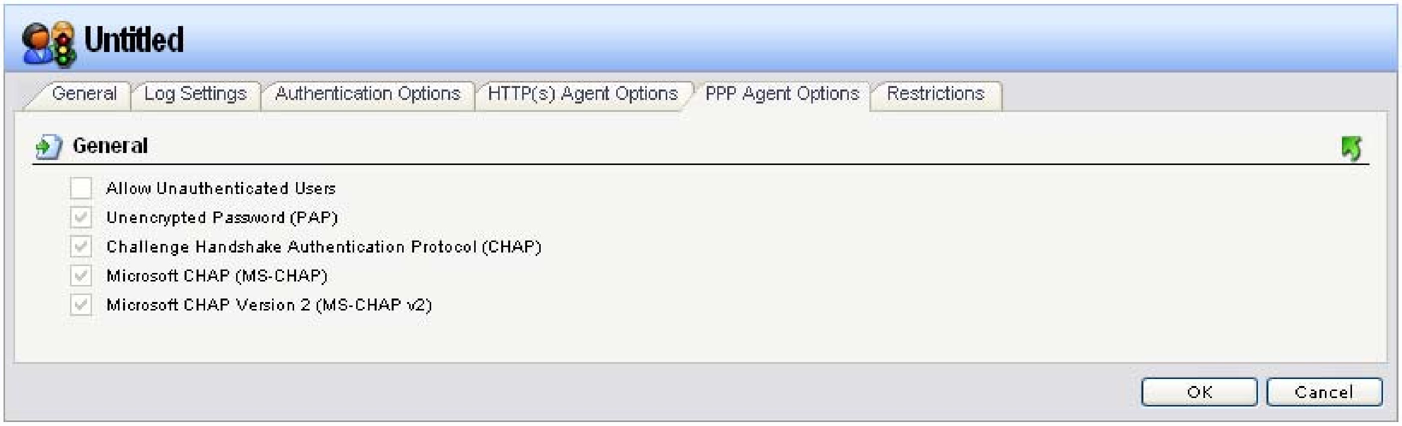
Login Type: HTMLForm

Realm String:

Certificates

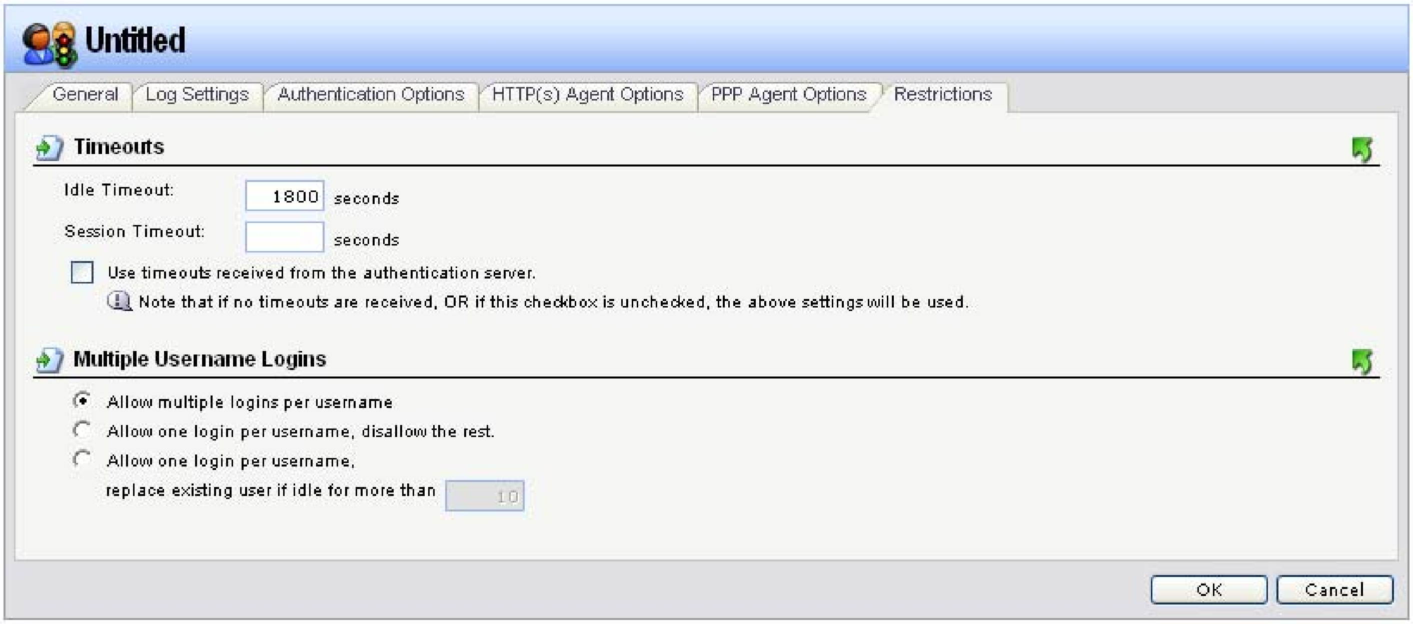
Host Certificate: (None)

Root Certificate: (None)



General

☐ Allow Unauthenticated Users
☑ Unencrypted Password (PAP)
☑ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP (MS-CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)



Timeouts

Idle Timeout: 1800 seconds

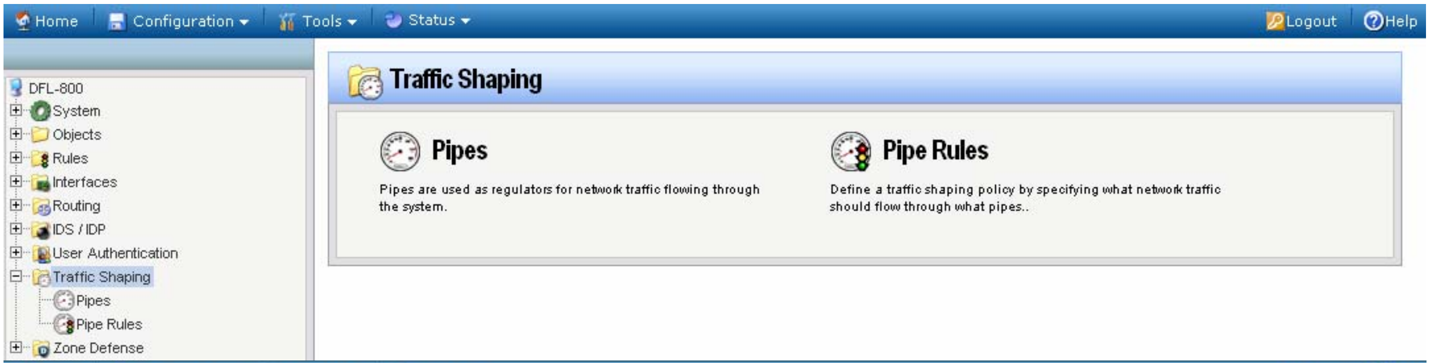
Session Timeout: seconds

☐ Use timeouts received from the authentication server.

Note that if no timeouts are received, OR if this checkbox is unchecked, the above settings will be used.

Multiple Username Logins

● Allow multiple logins per username
○ Allow one login per username, disallow the rest.
○ Allow one login per username,
replace existing user if idle for more than 10



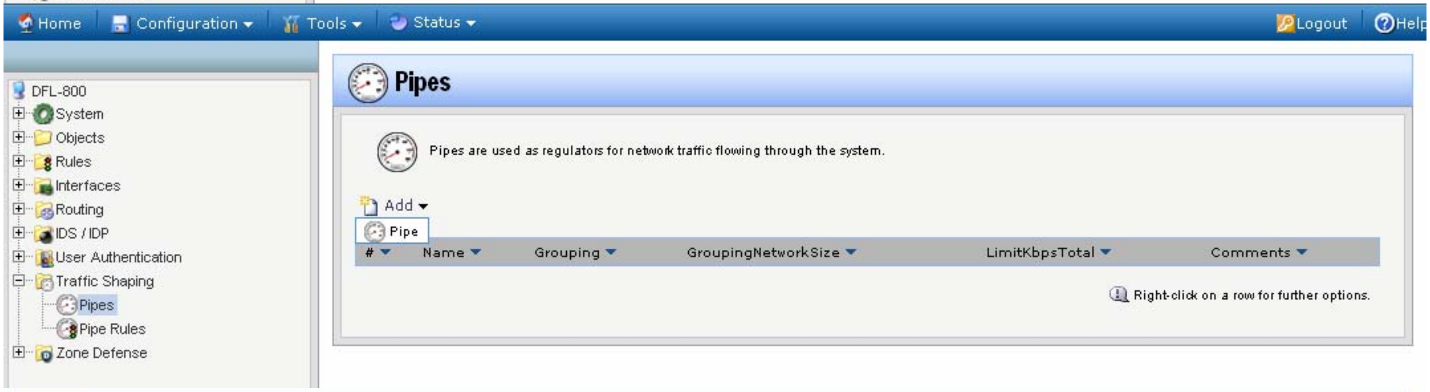
Traffic Shaping

Pipes

Pipes are used as regulators for network traffic flowing through the system.

Pipe Rules

Define a traffic shaping policy by specifying what network traffic should flow through what pipes..

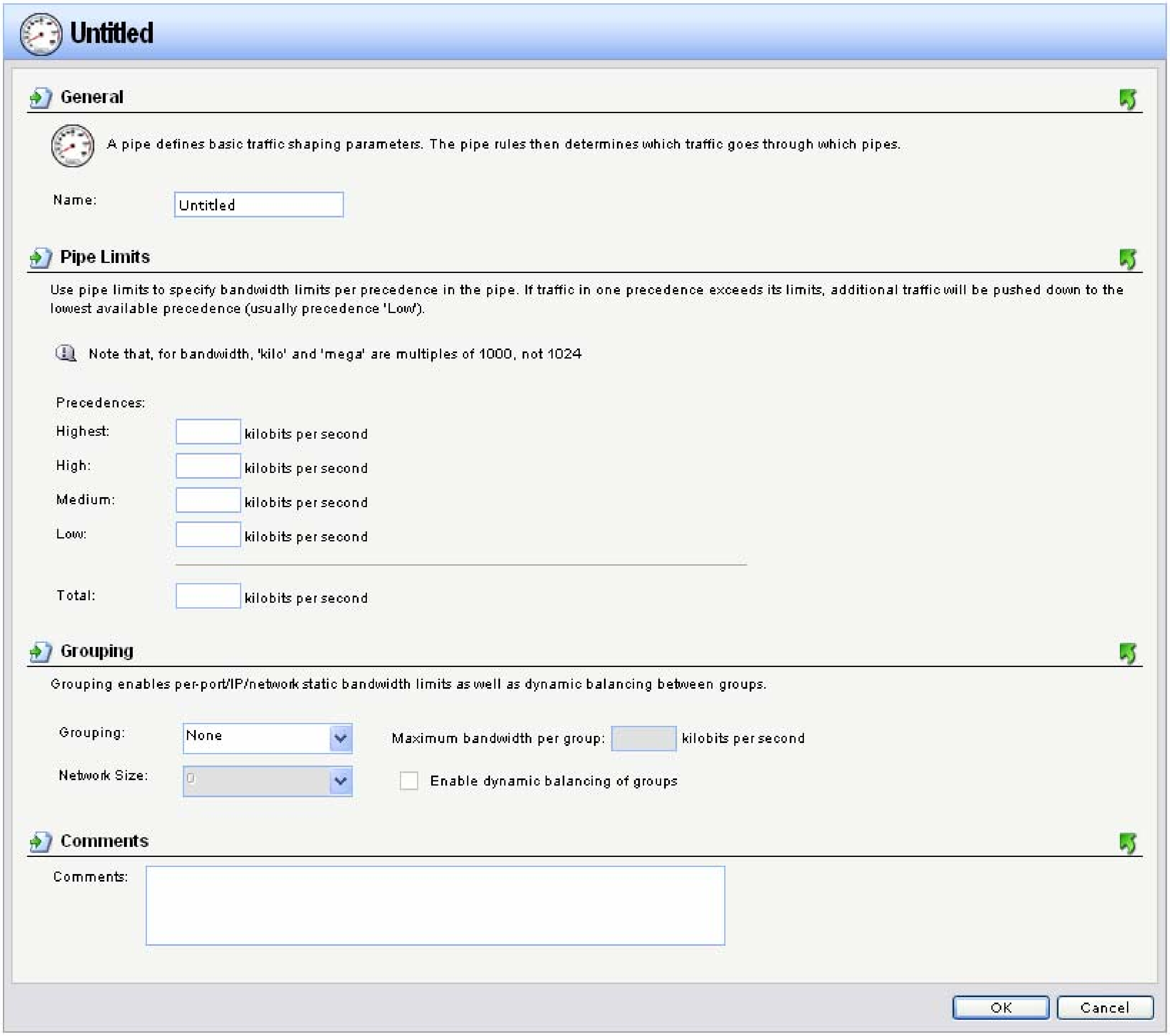


Pipes

Pipes are used as regulators for network traffic flowing through the system.

#	Name	Grouping	GroupingNetworkSize	LimitKbpsTotal	Comments

Right-click on a row for further options.



Untitled

General

A pipe defines basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes.

Name: Untitled

Pipe Limits

Use pipe limits to specify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed down to the lowest available precedence (usually precedence 'Low').

Note that, for bandwidth, 'kilo' and 'mega' are multiples of 1000, not 1024

Precedences:

Highest: kilobits per second

High: kilobits per second

Medium: kilobits per second

Low: kilobits per second

Total: kilobits per second

Grouping

Grouping enables per-port/IP/network static bandwidth limits as well as dynamic balancing between groups.

Grouping: None

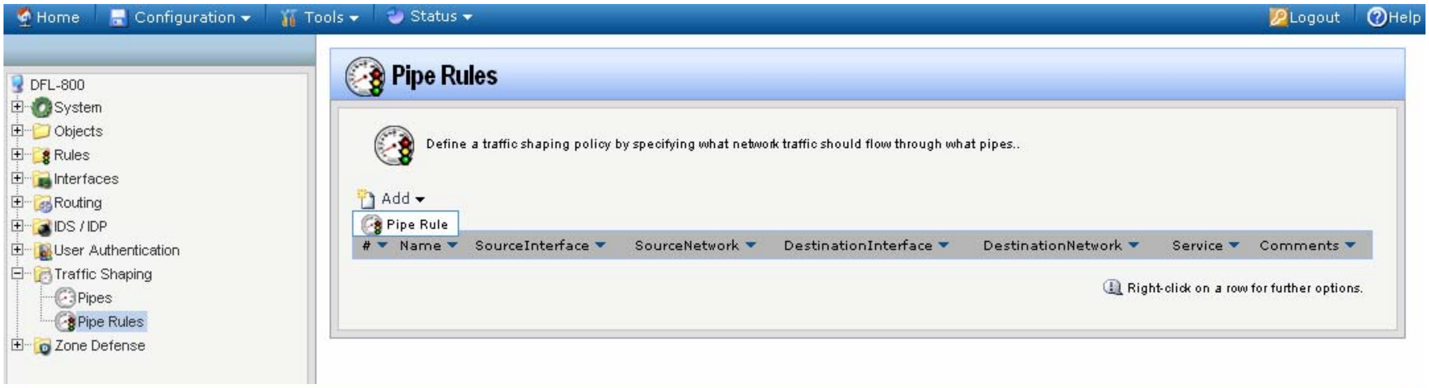
Maximum bandwidth per group: kilobits per second

Network Size: 0

□ Enable dynamic balancing of groups

Comments

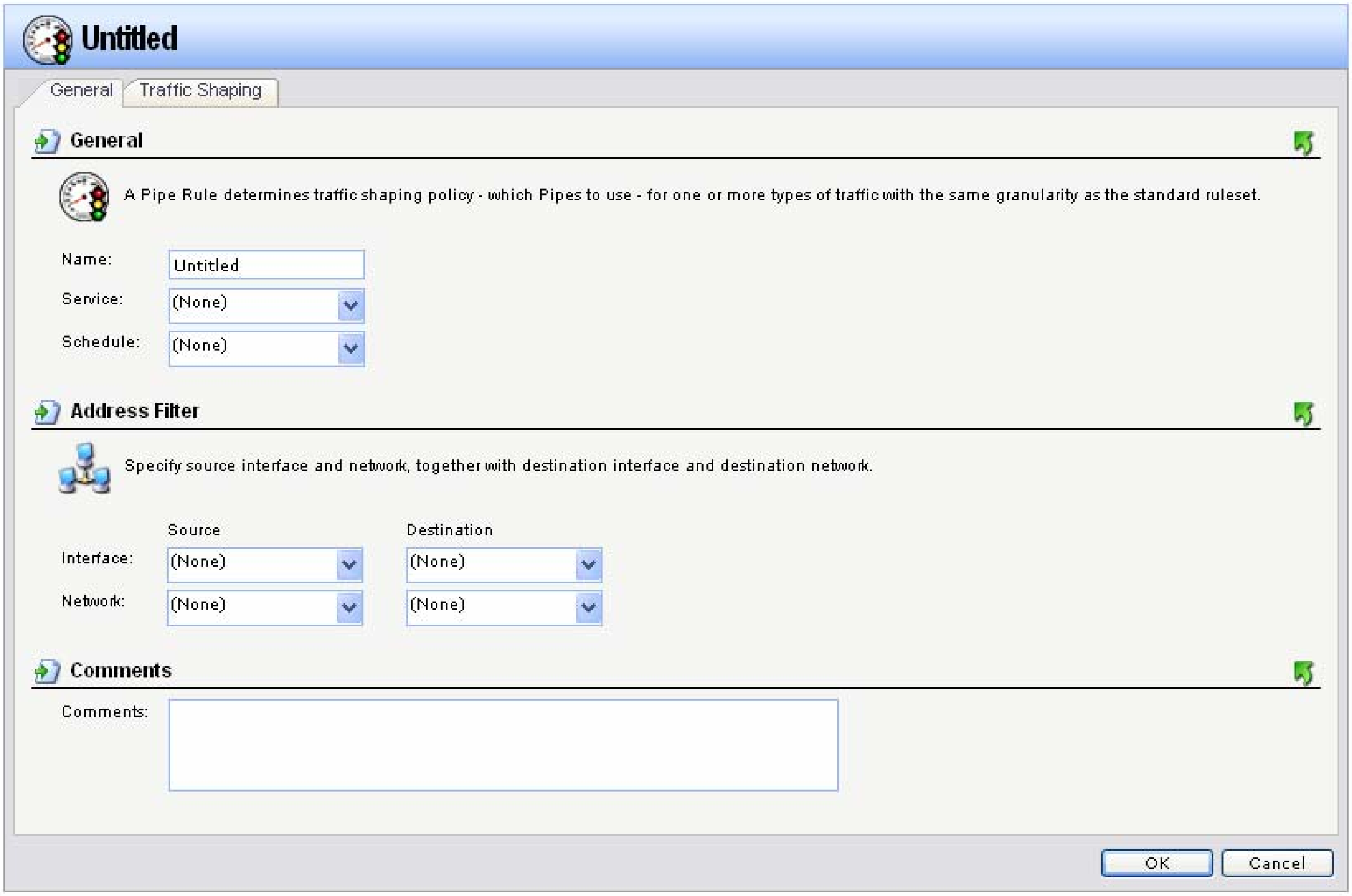
Comments:



Pipe Rules

Define a traffic shaping policy by specifying what network traffic should flow through what pipes..

Right-click on a row for further options.



Untitled

General

A Pipe Rule determines traffic shaping policy - which Pipes to use - for one or more types of traffic with the same granularity as the standard ruleset.

Name: Untitled

Service: (None)

Schedule: (None)

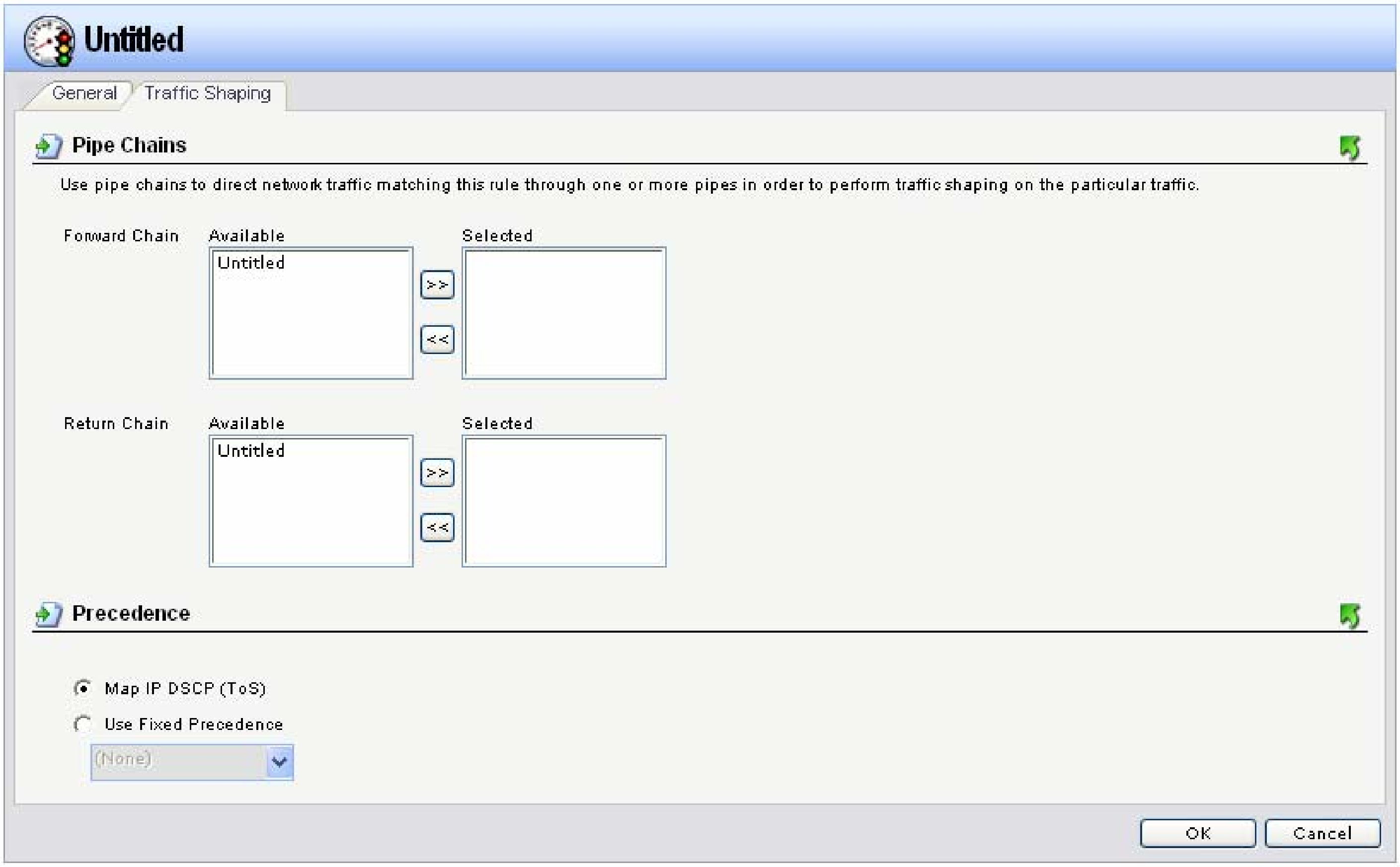
Address Filter

Specify source interface and network, together with destination interface and destination network.

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:



Untitled

Pipe Chains

Use pipe chains to direct network traffic matching this rule through one or more pipes in order to perform traffic shaping on the particular traffic.

Forward Chain Available: Untitled Selected:

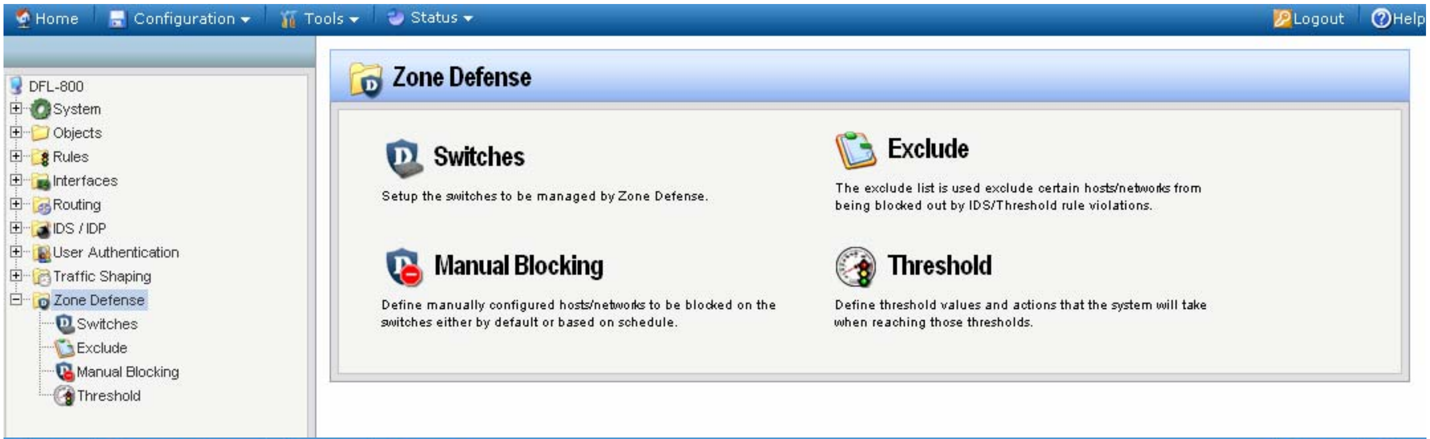
Return Chain Available: Untitled Selected:

Precedence

● Map IP DSCP (ToS)

○ Use Fixed Precedence

(None)



Zone Defense

Switches

Setup the switches to be managed by Zone Defense.

Exclude

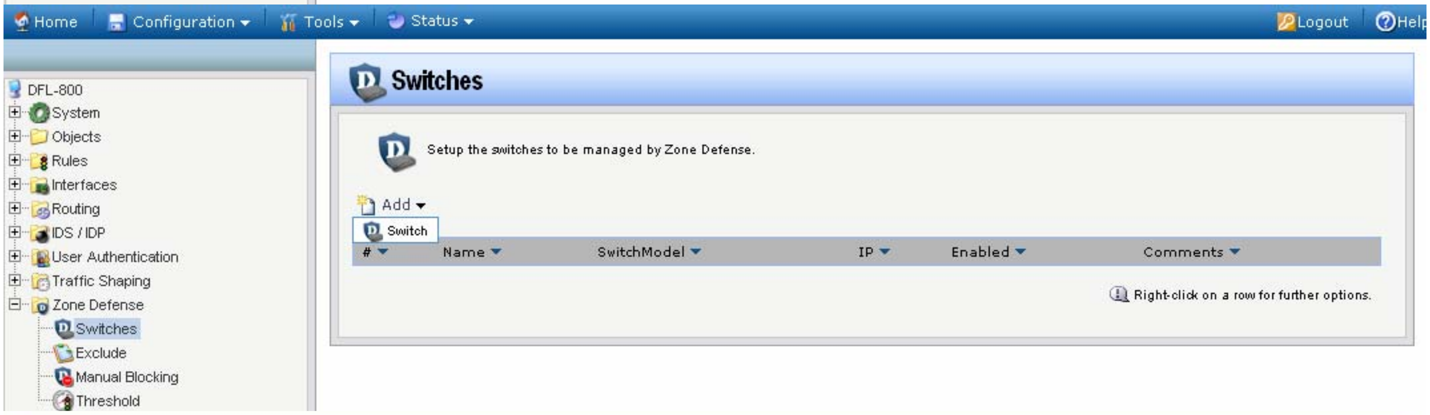
The exclude list is used exclude certain hosts/networks from being blocked out by IDS/Threshold rule violations.

Manual Blocking

Define manually configured hosts/networks to be blocked on the switches either by default or based on schedule.

Threshold

Define threshold values and actions that the system will take when reaching those thresholds.

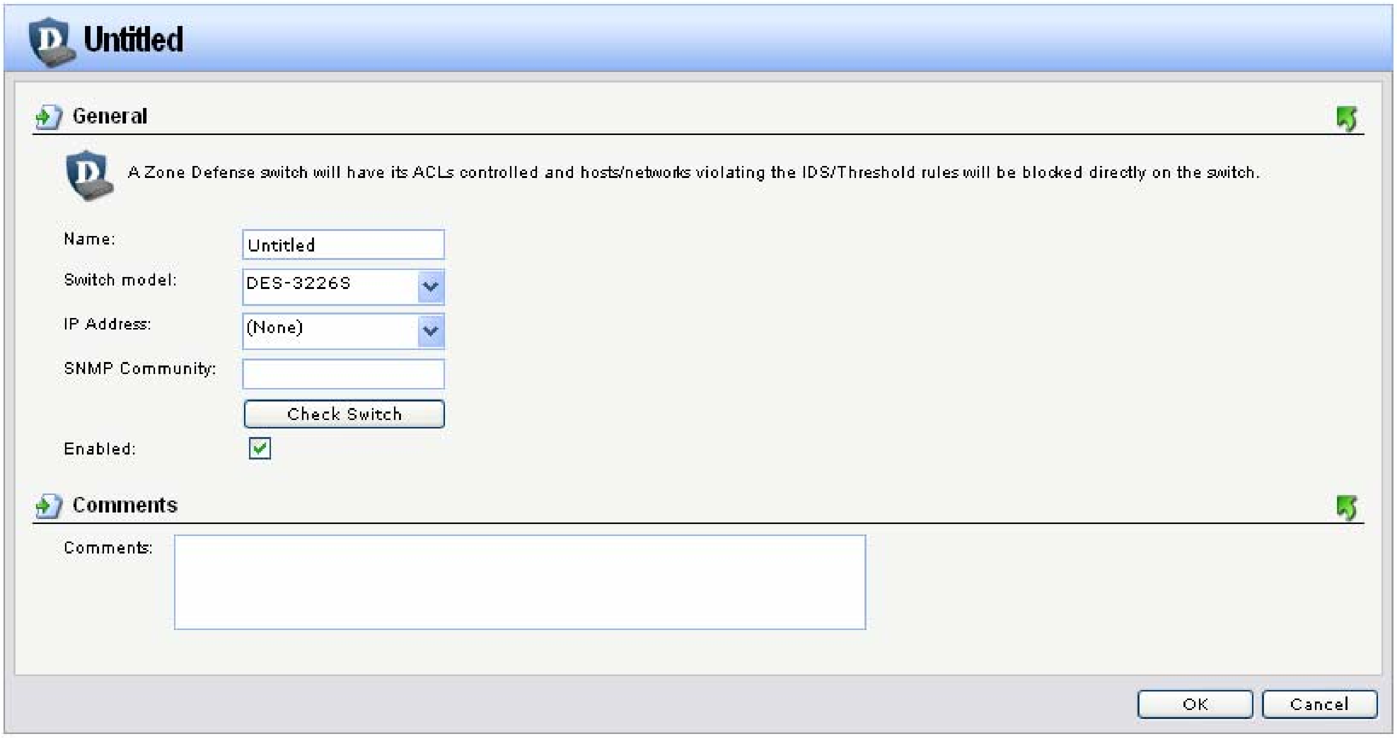


Switches

Setup the switches to be managed by Zone Defense.

#	Name	SwitchModel	IP	Enabled	Comments

Right-click on a row for further options.



Untitled

General

A Zone Defense switch will have its ACLs controlled and hosts/networks violating the IDS/Threshold rules will be blocked directly on the switch.

Name: Untitled

Switch model: DES-3226S

IP Address: (None)

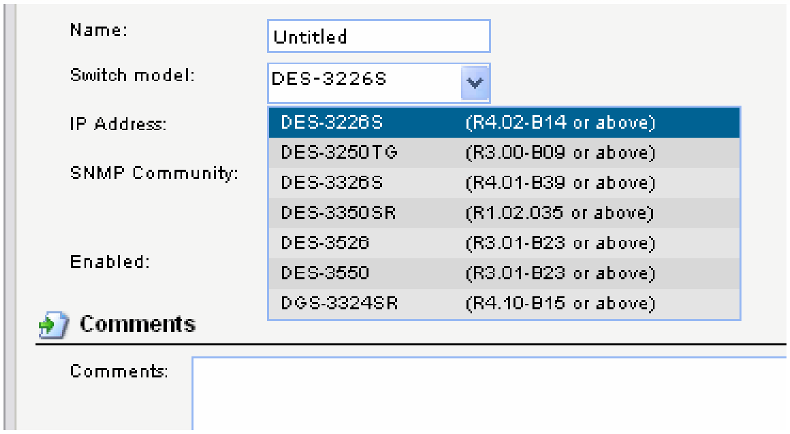
SNMP Community:

Check Switch

Enabled: ☑

Comments

Comments:



Name: Untitled

Switch model: DES-3226S

IP Address:

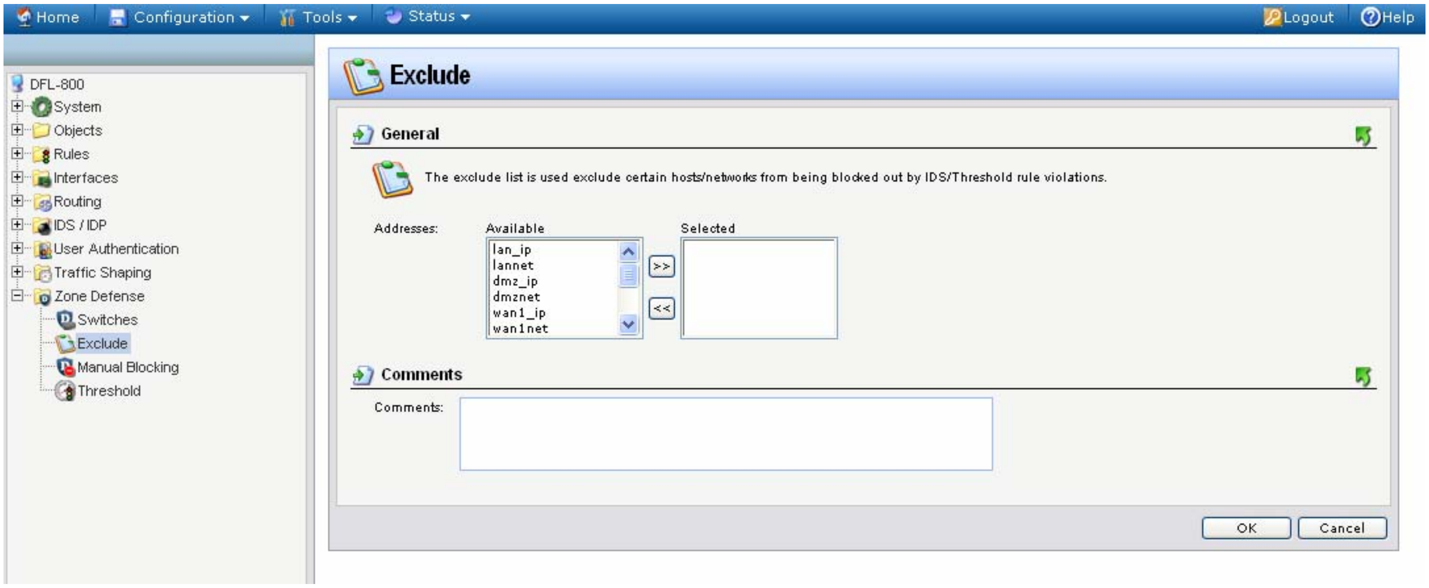
SNMP Community:

Enabled:

DES-3226S	(R4.02-B14 or above)
DES-3250TG	(R3.00-B09 or above)
DES-3326S	(R4.01-B39 or above)
DES-3350SR	(R1.02.035 or above)
DES-3526	(R3.01-B23 or above)
DES-3550	(R3.01-B23 or above)
DGS-3324SR	(R4.10-B15 or above)

Comments

Comments:



Exclude

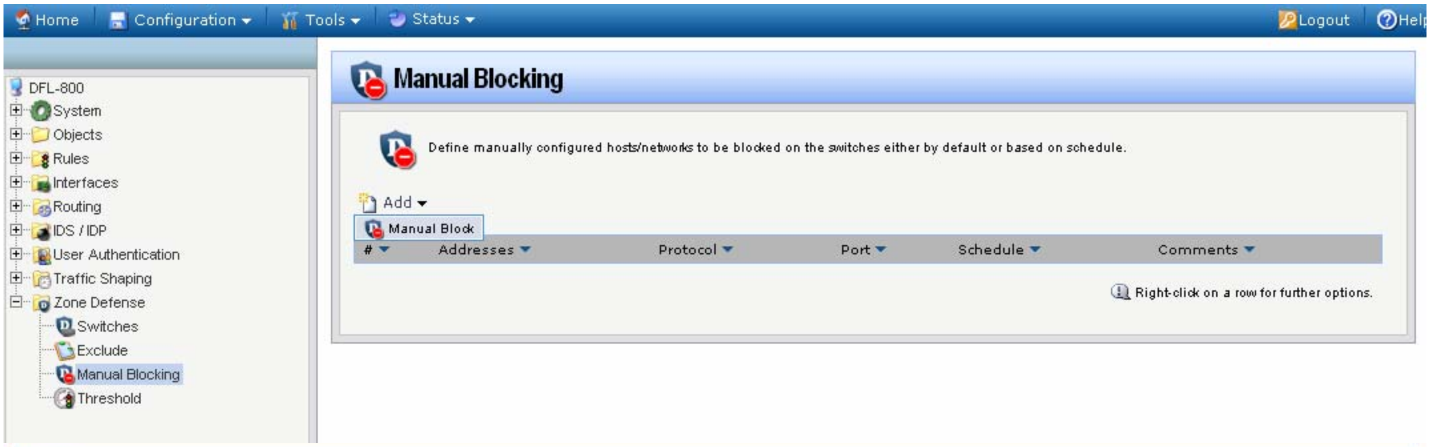
General

The exclude list is used exclude certain hosts/networks from being blocked out by IDS/Threshold rule violations.

Addresses: Available: lan_ip, lannet, dmz_ip, dmznet, wan1_ip, wan1net — Selected:

Comments

Comments:

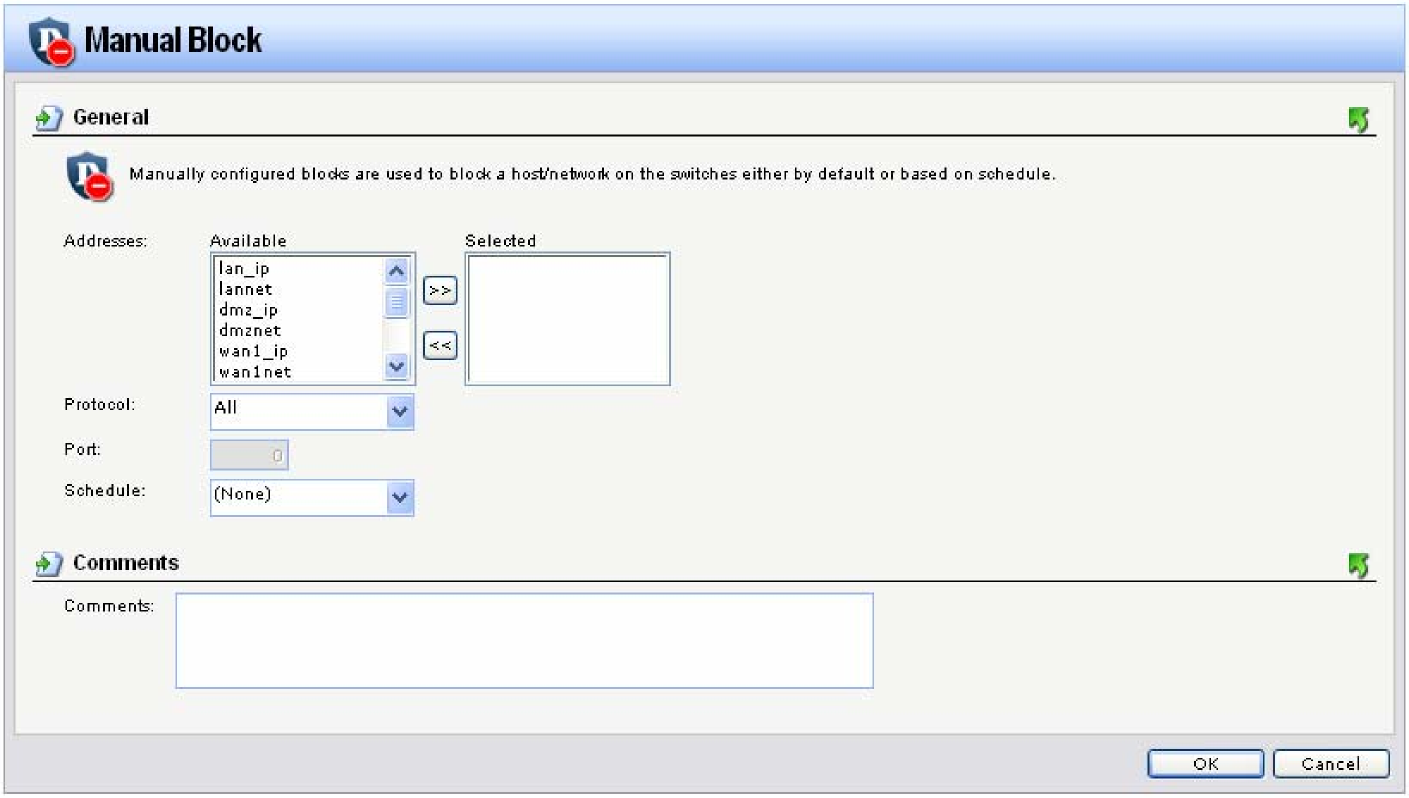


Manual Blocking

Define manually configured hosts/networks to be blocked on the switches either by default or based on schedule.

#	Addresses	Protocol	Port	Schedule	Comments

Right-click on a row for further options.



Manual Block

General

Manually configured blocks are used to block a host/network on the switches either by default or based on schedule.

Addresses: Available: lan_ip, lannet, dmz_ip, dmznet, wan1_ip, wan1net — Selected:

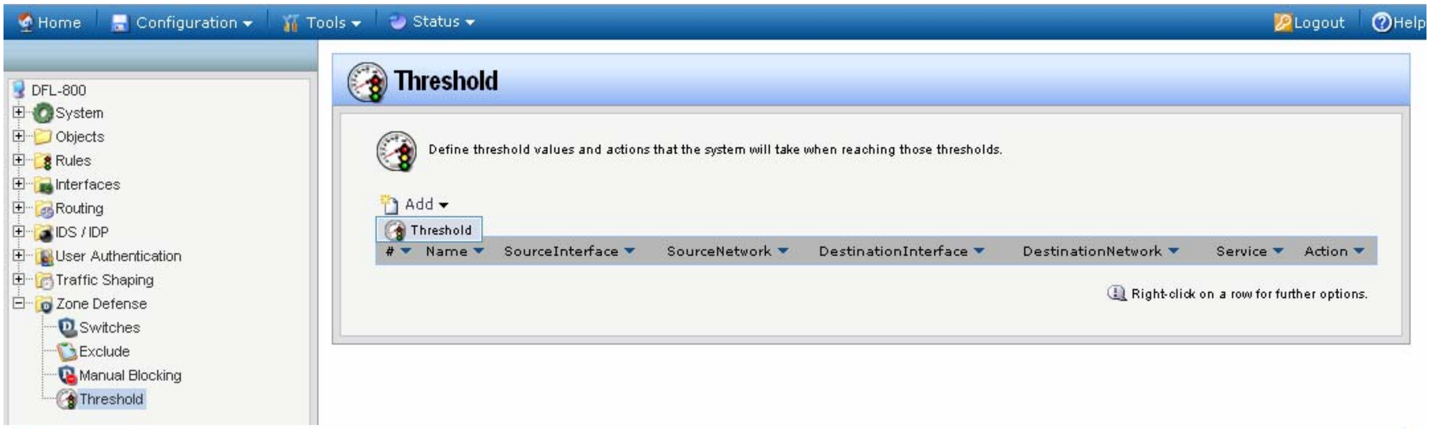
Protocol: All

Port: 0

Schedule: (None)

Comments

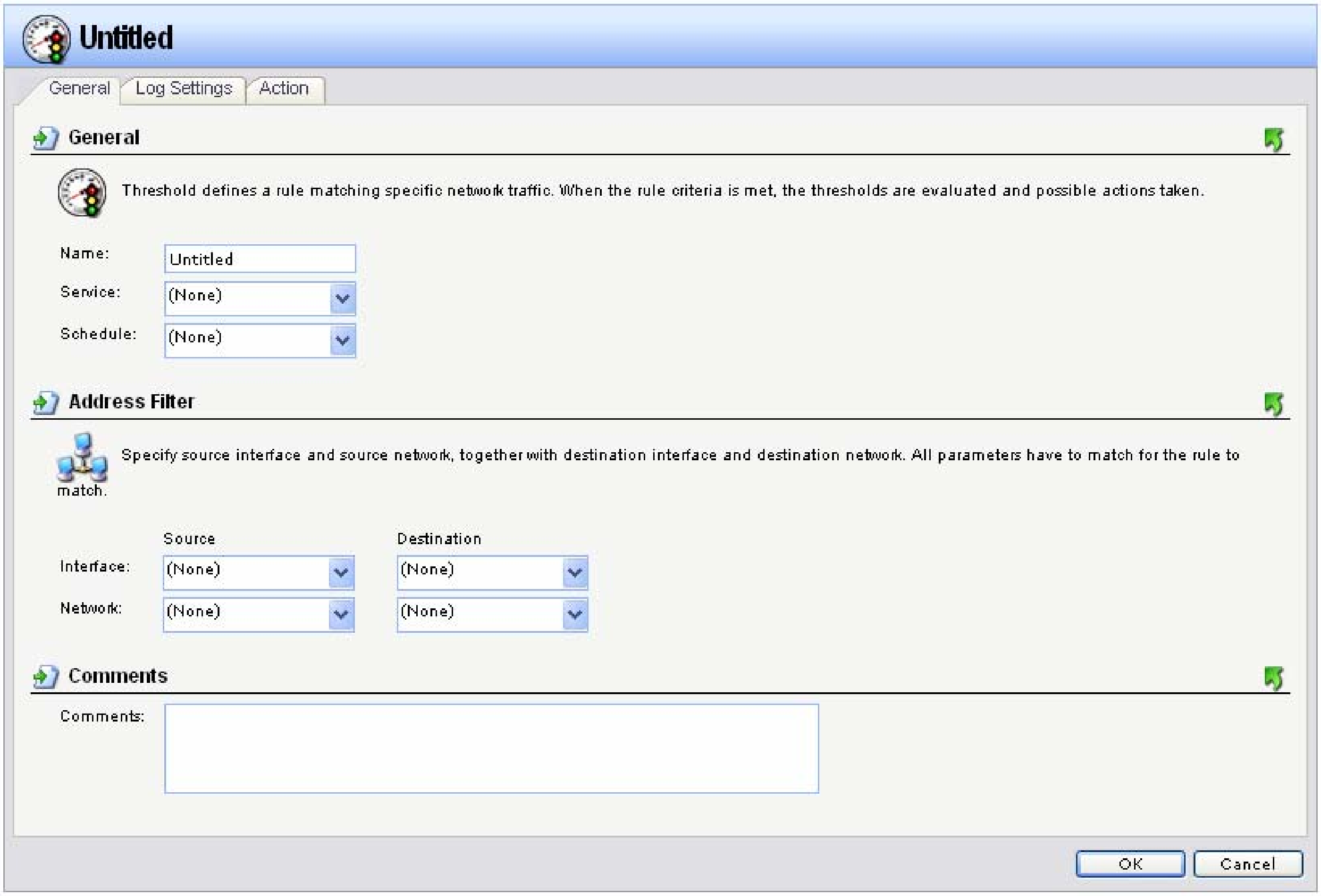
Comments:



Threshold

Define threshold values and actions that the system will take when reaching those thresholds.

Right-click on a row for further options.



Untitled

General

Threshold defines a rule matching specific network traffic. When the rule criteria is met, the thresholds are evaluated and possible actions taken.

Name: Untitled

Service: (None)

Schedule: (None)

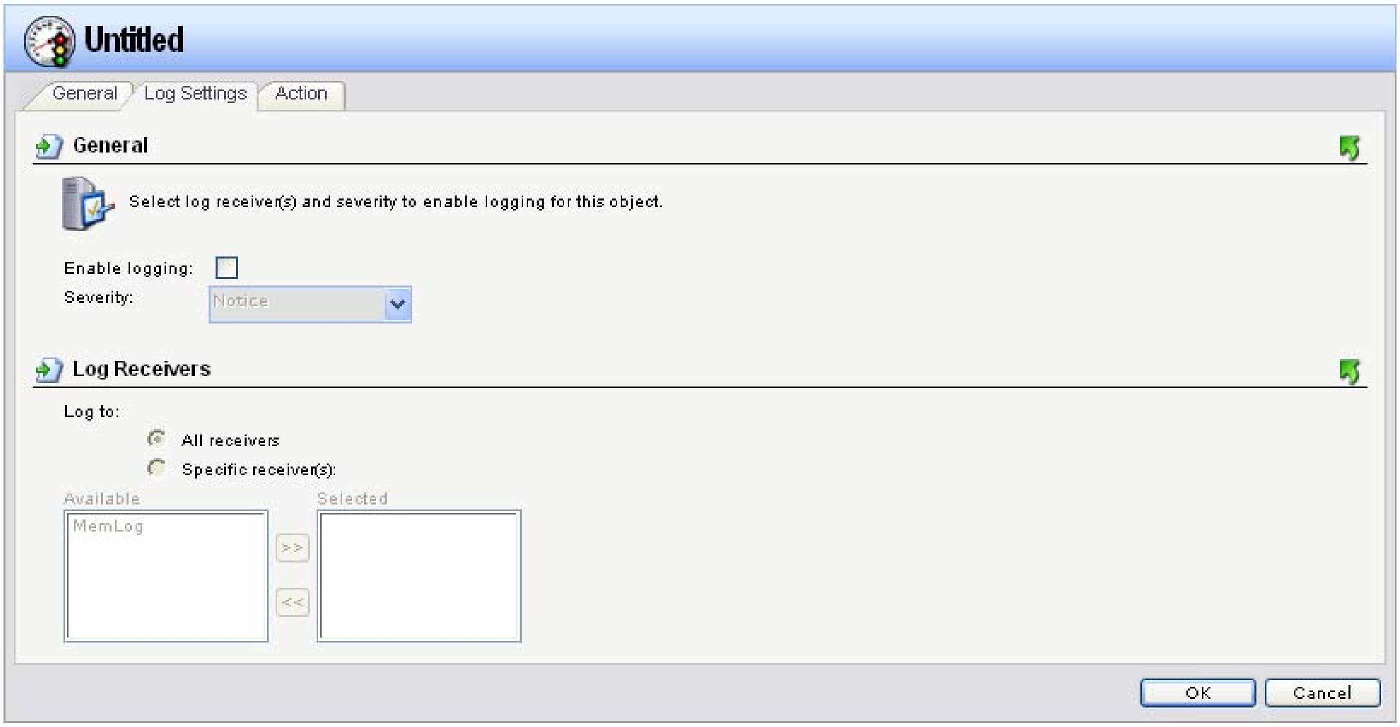
Address Filter

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

	Source	Destination
Interface:	(None)	(None)
Network:	(None)	(None)

Comments

Comments:



Untitled

General

Select log receiver(s) and severity to enable logging for this object.

Enable logging: □

Severity: Notice

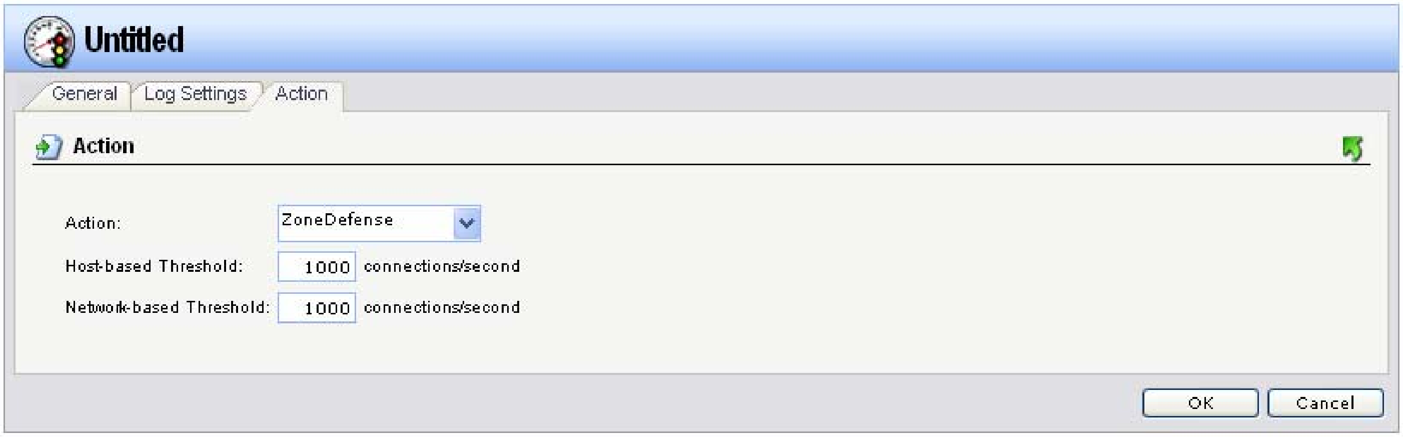
Log Receivers

Log to:

● All receivers

○ Specific receiver(s):

Available	Selected
MemLog	



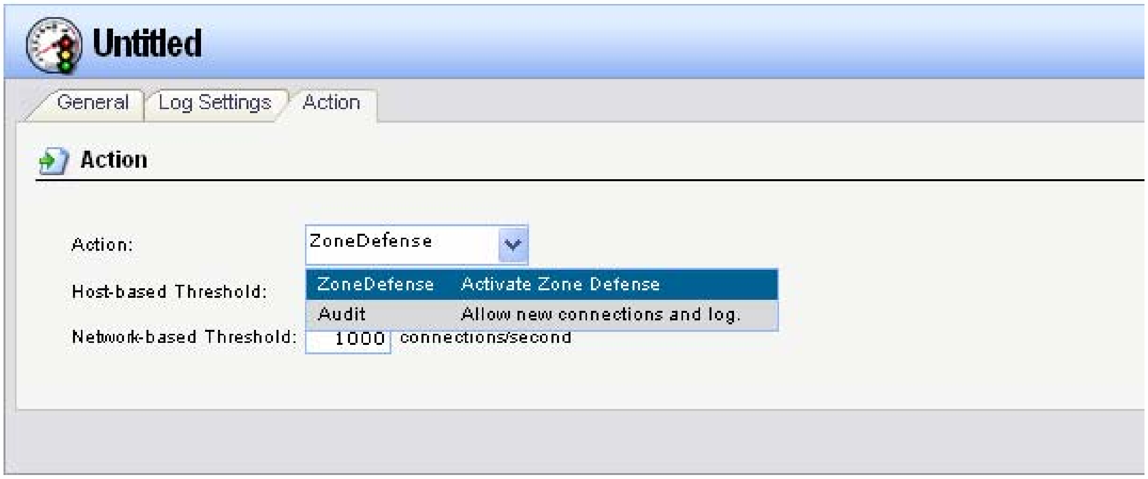
Untitled

Action

Action: ZoneDefense

Host-based Threshold: 1000 connections/second

Network-based Threshold: 1000 connections/second



Untitled

Action

Action: ZoneDefense

ZoneDefense	Activate Zone Defense
Audit	Allow new connections and log.

Host-based Threshold:

Network-based Threshold: 1000 connections/second