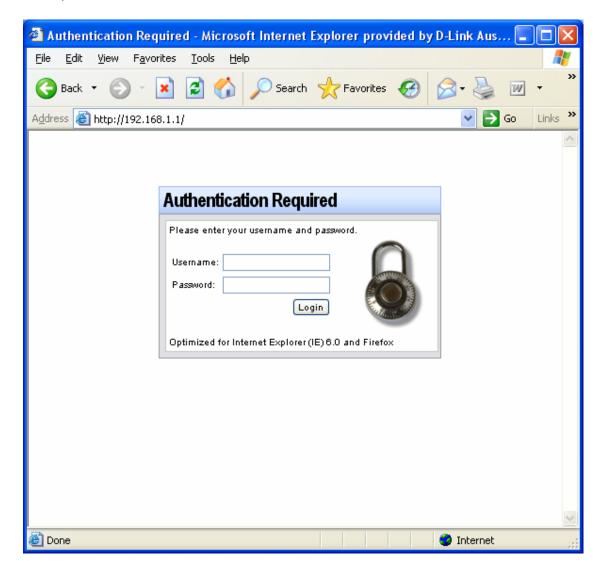
http://192.168.1.1 admin, admin



Web Page Dialog	?
🤶 D-Link Setup wizard	
🛃 Welcome	5
Welcome Welcome	
Welcome to the D-Link Setup Wizard.	
Proceed using the Next button below	
	Cancel Next >>
o://192.168.1.1/ModalFrame.htm?Page=WizardSetup	🥝 Internet

🕙 Web Page Dialog		? 🗙
🤶 D-Link Setup) wizard	
🛃 Administrator use	r settings	<u>5</u>
Administrator o	iser settings	
Please enter a passwor	d for protecting the administrative interface of the unit	
Username	admin	
Password	•••••	
Confirm password	•••••	
	is case sensitive, and that you should pick a password that contains upper- and I as numbers and/or special characters.	
	Cancel << Previous Next >	
	Cancel << Previous Next >	
http://192.168.1.1/ModalFram	e.htm?Page=WizardSetup 🥘 Internet	

Web Page I	Dialog						?
🎈 D-Link	Setup wizard						
艩 Time, time	e zone and daylight	t saving ti	ime settings	;			5
🚫 Time	e, time zone and dayli	ght saving '	time settings				
Setup the cor	rect time and timezon	e settings f	or the firewall				
Date:	2005-06-30						
Time: Set time	09:41:11						
Timezone Time zone:	settings						ন
_	daylight saving time	*					
Offset:	60						
Start Date	March 🔽	26	*				
End Date	October 🔽 🗸	30	*				
				C	ancel << Pre	vious Ne	xt≻≻
/192.168.1.1/M	odalFrame.htm?Page:	=WizardSe	tup		🔮 Internet		

Time zone:	(GMT+10:00)	
	(GMT+03:30) Tehran	~
Enable	(GMT+04:00) Abu Dhabi, Baku, Muscat, Tbilist	
	(GMT+04:30) Kabul	
Offset:	(GMT+05:00) EKaterinburg, Islamabad, Karachi, Tashikent	
	(GMT+05:30) New Delhi	
Start Date	(GMT+06:00) Astana, Almaty, Colombo, Dhaka	
End Date	(GMT+07:00) Bangkok, Hanoi, Jakarta	
End Date	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei	
	(GMT+09:00) Seoul, Tokoyo, Yakutsk	
	(GMT+09:30) Adelaide, Danvin	=
	(GMT+10:00) Canberra, Guam, Port Moresby, Vladivostok	
	(GMT+11:00) Magadan, Solomon Islands	
	(GMT+12:00) Fiji, Kamchatka, Marshall Islands, Wellington	~
	Cancel << Pi	reviou

省 http://192.168.1.1 - D-Link Firewall - Microsoft Interne 🔳 🗖	X
Set Date and Time	
The date and time settings will be applied instantly	
Date: 2005 ♥ . Jun ♥ . 30 ♥ Time: 09:41:11 (HH:MM:SS)	
OK Cancel	~
🙆 Done 🥥 Internet	

-	ce settings		え
WAN inf	terface settings		
Select the interf	ace that is connected	to the ISP	
Interface	wan1		
	Name	Comments	
	wan1		
	时 wan2 Mai dmz		
	iiii Ian		

-	Page Dialog
😸 D-I	Link Setup wizard
헌 WAN	interface settings 😽
≡ ₿	WAN interface settings
	the appropriate configuration type of the internet-facing (WAN) interface. Your ISP normally tells you ype to use.
œ	Static - manual configuration
	Most commonly used in dedicated-line internet connections. Your ISP provides the IP configuration parameters to you.
0	DHCP - automatic configuration
	Regular ethernet connection with DHCP-assigned IP address. Used in many DSL and cable modem networks. Everything is automatic.
0	PPPoE - account details needed
	PPP over Ethernet connection. Used in many DSL and cable modem networks. After providing account details, everything is automatic.
0	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.
0	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".
	Cancel << Previous Next >>
p://192.168.	1.1/ModalFrame.htm?Page=WizardSetup 💣 Internet

	5
Static IP setting	gs
Static WAN interface co usually provides this info	nfiguration is most commonly used in dedicated-line internet connections. Your ISP ormation 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	2	
PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.		
Username		
Password		
Confirm password		
Service		
Cancel << Previous Next >>		
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup		

Web Page Dialog		?
🤶 D-Link Setu	p wizard	
PPTP settings		3
PPTP setting	5	
details, and possibly a	onnections are used in some DSL and cable modem networks. You need account Iso IP configuration parameters of the actual physical interface that the PPTP tunnel ould supply this information.	I
PPTP tunnel parame	ters:	
Username		
Password		
Confirm password		
Remote Endpoint		
Physical interface pa	ameters:	
OHCP		
C Static		
IP Address		
Network		
Gateway		
	Cancel (<< Previous) Next >	>
;//192.168.1.1/ModalFrar	ne.htm?Page=WizardSetup 🍎 Internet	

省 Web Page Dialog	? 🗙
🤶 D-Link Setup wizard	
🔊 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.	i
Username	
Password Confirm password	
Cancel << Previous Next >>	
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup 🔹 👔 Internet	

省 Web Page Dialog 🛛 💽	
🤶 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 Ian	
Enter a range of IP addresses to hand out to DHCP clients: IP Range	
Netmask	
Cancel << Previous Next >>	J
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup 🔮 Internet	

省 Web Page Dialog 🛛 🤶	X
🤶 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 Ian Name Comments	
Enter a range of IP ad 🕮 wan1 IP Range 🛛 🕮 wan2	
Netmask III Ian	
Cancel << Previous Next >>	
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup	

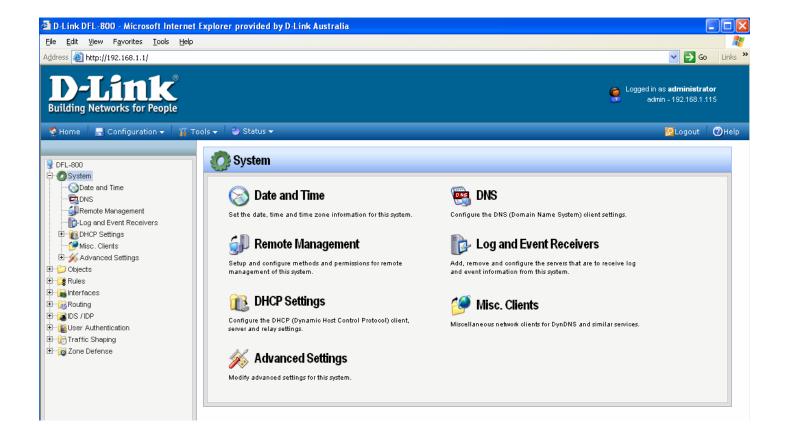
🖄 Web Page Dialog 🛛 💡	X
🤶 D-Link Setup wizard	
🛃 Helper server settings 😽	
Helper server settings	
You may enable additional servers for keeping the time accurate and for logging data	
Time servers - for automatically keeping the unit's time accurate	
Primary NTP Server Secondary NTP Server (Optional)	
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)	
Cancel << Previous Next >>	
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup 🧐 Internet	

🚰 Web Page Dialog	? 🗙
🤶 D-Link Setup wizard	
Activate setup	5
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.	
Cancel << Previous Activ	vate
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup	

🕘 Web Page Dialog	?×
🤶 D-Link Setup wizard	
Activate changes	5
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 chang will revert to its previous configuration.	es to be finalized. If this fails, the unit
This page will automatically refresh in 14 seconds in an attempt to do If the automatic refresh fails, you can:	o this automatically.
 Reconnect to the unit manually. 	
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup	🔮 Internet

🐔 Web Page Dialog	? 🛛
🤶 D-Link Setup wizard	
	5
Changes committed to the configuration file	
The configuration has now been saved.	
	Close
http://192.168.1.1/ModalFrame.htm?Page=WizardSetup	🔮 Internet





D-Link DFL-800 - Microsoft Internet	Explorer provided by D-Link Australia	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
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 👻 🛛 🌃 To	ols 🗸 👘 🤩 Status 🗸	😕 Logout 🕜 Help
DFL-800	🔀 Date and Time	
- O System		1
	🔊 General	<u>5</u>
	Set the date, time and time zone information for this system.	
The DHCP Settings Misc. Clients	Current Date and Time: 2005-06-30 09:49:53 Set Date and Time	
⊞ — ≫ Advanced Settings	Time zone and daylight saving time settings	5
⊡; Objects ⊡ ∰ Rules		
	Time zone: (GMT+10:00)	
E	Enable daylight saving time	
E - Straffic Shaping	Offset: 60 minutes	
E Zone Defense	Start Date: March 🗸 26 🗸	
	End Date: October 🗸 30 🗸	
	Automatic time synchronization	<u>5</u>
	Enable time synchronization	
	Time Server Type:	
	Primary Time Server: (None)	
	Secondary Time Server: (None)	
	Tertiary Time Server:	
	Interval between each synchronization: 86400 seconds	
	Maximum time drift that a server is allowed to adjust: 36000 seconds	
	Coord Seconds	
	Interval according to which server responses will be grouped:	
		OK Cancel
e Done		📑 🛛 🔮 Internet 💷

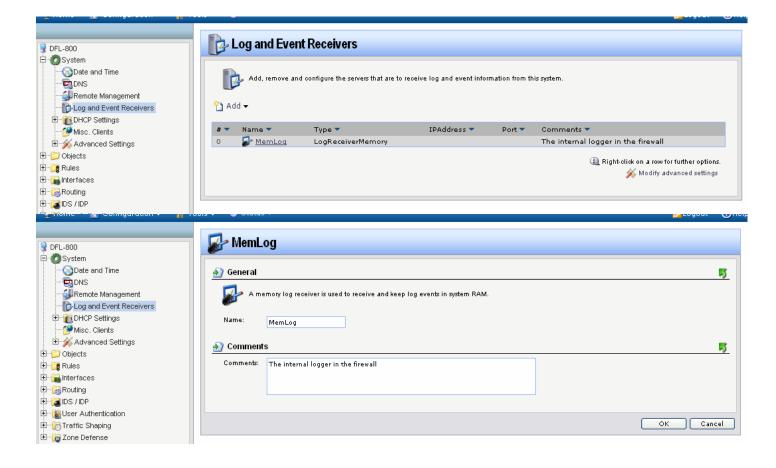
💁 Home 🛛 📑 Configuration 👻 🍟	Tools 🗸 🔮 Status 🗸	2 Logout 0 Hel
DFL-800 System Date and Time DNS Remote Management Log and Event Receivers Compared Event Receivers Compared Settings Advanced Settings Cobjects Rules Interfaces	Image: Secondary Server: dnsserver1_ip Secondary Server: dnsserver2_ip Tertiary Server: (None)	<u>5</u>
Souting Souting Souting Souting Souting Souting Souting Description		OK Cancel

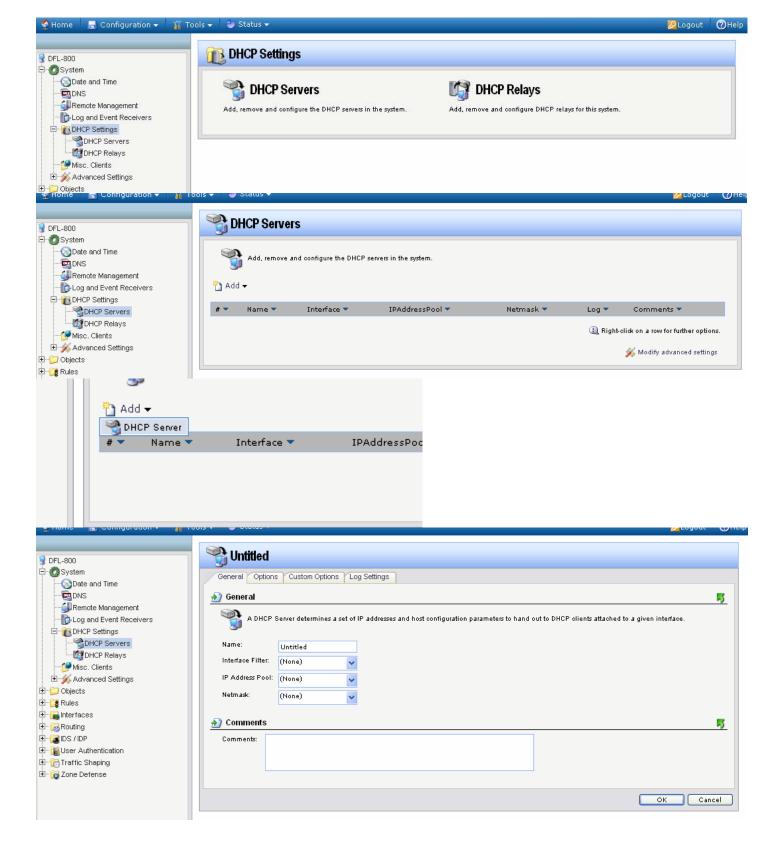
Primary Server:	dnsserver1_ip	*	
Secondary Server:	Name	Address	
	(None)		
Tertiary Server:	🧕 dmz_ip	172.17.100.254	
	🧧 dnsserver1_ip	202.129.64.198	
	🧕 dnsserver2_ip	4.2.2.2	
	🧕 lan_ip	192.168.1.1	
	🧕 wan1_defaultgw_	_ip 202.129.109.65	
	🧕 wan1_ip	202.129.109.82	
	🧕 wan2_ip	192.168.120.254	

🔊 DNS		
Configure the	: DNS (Domain Name Syster	n) client settings.
Primary Server:	dnsserver1_ip 🗸 🗸 🗸	
Secondary Server:	dnsserver2_ip 🗸 🗸	
Tertiary Server:	Name A	ddress
	(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	e DNS (Domain Name System	n) client settings.
Primary Server:	dnsserver1_ip 🗸 🗸	
Secondary Server:	dnsserver2_ip 🗸 🗸	
Tertiary Server:	(None)	
	Name Ad	ddress
	(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

🦉 Home 👘 🔂 Configura		ils 🗸 🛛 🥥 Status 👻			ZLogout (7)Help
🚽 DFL-800		剑 Remote Management			
∃ OSystem					
Date and Time		Setup and configure methods and perm	nissions for remote management of this :	system.	
	-t	30°			
Log and Event Rece		🎦 Add 🔫			
E DHCP Settings					
🧐 Misc. Clients		# Type Type Type Type Type Type Type Type	Mode 🕶		letwork Comments
🗄 🚿 Advanced Settings		0 GRemoteMamtHTTP	Admin: HTTP, HTTPS	🔂 any 🕔	Jannet
Đ∽j⊃ Objects Đ∽ j≴ Rules					() Right-click on a row for further options.
± G Interfaces					🐝 Modify advanced settings
± 🛜 Routing					The settings
Home Configur	adon 🗸 🛛 🔐 Tot	ns 🗸 🔰 Status 🗸			ZLOGOUL (7Heij
-					_
		ITTP/HTTPS Management			
SUFL-800 ⊟∽ OOSystem		Se in the management			
Date and Time		Remote Access Type			5
		Themore Access Type			2
Remote Manageme		Select the remote access types that sho	uld be enabled.		
bog and Event Rec	eivers	3-			
Image: The setting of the setting					
E - j Advanced Settings		HTTPS			
E 💬 Objects		Access			5
🗄 📴 Rules					
🗄 🚘 Interfaces		Select the user database to use for login and th	e access level to grant to the user.		
		User Database: AdminUsers 🗸			
E. Kuthentication					
🗄 📆 Traffic Shaping		Access Level: Admin			
🗄 🖓 📷 Zone Defense		🔊 Access Filter			_
		Access Filler			<u></u>
		Remote access is granted from the following in	terface and network.		
		Interface: any 🗸			
		Network: lannet 🗸			
		Orments			<u>5</u>
		Comments:			
					OK Cancel
			🔅 🕺 Access Hiter		
			Meecoo Tiker		
			Remote access is	granted from the foll	lowing interface and network.
			Interface:	any	*
			Network:	lannet	*
<u> </u>				Name	Address
			衸 Comments	🧕 all-nets	0.0.0.0/0
Remote access is	granted from t	the following interface and network.		dmz_ip	172.17.100.254
		-	Comments:	dmz_rp	172.17.100.0/24
Interface:	any			-	202.129.64.198
	any	*		dnsserver1_ip	
Network:	Name	Comments		dnsserver2_ip	4.2.2.2
	📷 any			Jan_ip	192.168.1.1
-	core			a lannet	192.168.1.0/24
魡 Comments	📖 dmz			🤤 wan1_default	
Commenter	📑 lan		-	🧕 🧕 wan1_ip	202.129.109.82
Comments:	wan1			🤤 wan1net	202.129.109.0/27
				🧕 wan2_ip	192.168.120.254
	📲 wan2			🧕 wan2net	192.168.120.0/24





🐏 Home 👘 🔚 Configuration 👻 🛛 🚻 Tools 👻 🗋 🥥 Status 🔻 💋 Logout 👘 🕐 Help 📲 Untitled 😼 DFL-800 🗄 🕜 System General Options Custom Options Log Settings 🚫 Date and Time 射 General DNS 📴 5 剑 Remote Management 👒 A DHCP Server determines a set of IP addresses and host configuration parameters to hand out to DHCP clients attached to a given interface - Toy and Event Receivers DHCP Settings DHCP Servers Default GW: (None) ~ DHCP Relays Domain: 🧐 Misc. Clients 🗄 🚿 Advanced Settings Lease Time: 86400 seconds 🗄 🗁 📁 Objects 🗄 📑 Rules Primary Secondary DNS: 🗄 🔂 Interfaces (None) ¥ (None) ¥ 🗄 🤯 Routing NBNSAVINS: (None) (None) ¥ ~ 🗄 🖓 IDS / IDP E. Buser Authentication Next Server: (None) v 🗄 🖓 Traffic Shaping 🗄 🗑 Zone Defense Cancel ОК 🐏 Untitled 😼 DFL-800 🗄 🕜 System General Options Custom Options Log Settings 🔞 Date and Time 艩 General - 📴 DNS ろ 🗐 Remote Management $Custom \ parameters \ of \ the \ lease \ may \ also \ be \ configured, see: \ http://www.iana.org/assignments/bootp-dhop-parameters \ and \ be \ and \ and \ be \ and \ and \ and \ be \ and \ be \ and \ and$ by Log and Event Receivers E- OHCP Settings DHCP Servers 🕕 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 Misc. Clients 🎦 Add 🗸 🗄 🚿 Advanced Settings 🗄 😳 Objects # 🔻 Code 🔻 Param 🔻 Comments 🔻 Type 🔻 🗄 📑 Rules 🗄 🚔 Interfaces Right-click on a row for further options. 🗄 🖓 Routing 🗄 🔂 IDS / IDP OK Cancel 🗄 👔 User Authentication 🗄 🕞 Traffic Shaping General Options / Custom Options / Log Settings 魡 General Custom parameters of the lease may also be configured, see: (I) Adding/modifying a custom option will discard changes to the DHC saved before attempting to access a custom option 🎦 Add 🗲 🐏 Custom Option # Code 🔻 Туре 🔻

DFL-800	Custom Option	
System System Date and Time DNS Government Dovernment Dovernment	General Seneral Extend the DHCP Server functionality by adding custom options that will be handed out to the DHCP olients. Code: (None) Type: UINT8 Parameter: Comments Comments	<u>R</u>
Interfaces Routing Southing		OK Cancel
Custom Option		

General 1 Extend the DHCP Server functionality by adding custom options that v 🏹 Custom Option Code: (None) v 魡 General 4 Type: Timeserver Addresses ~ 5 Name Server Addresses Parameter: Extend the DHCP Server functionality by adding custom options tha 7 Log Server Addresses 8 Quotes Server Addresses 9 LPR Server Addresses Comments Code: (None) v 10 Impress Server Addresses Comments: 11 RLP Server Addresses Type: 42 NTP Server Addresses 12 Hostname 43 Vendor Specific Information Parameter: 13 Size of boot file in 512 byte chunks 45 NETBIOS Distribution Srv 14 Merit Dump File 46 NETBIOS Node Type 16 Swap Server Address Comments 17 Path name for root disk Comments: 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 Path MTU Aging Timeout 24 25 Path MTU Plateau Table Interface MTU Size 26 MTU Subnet 27 Broadcast Address 28 29 Mask Discovery 30 Mask Supplier

31

32

33

34

35

36

37

38

39

40

41

Router Discovery

Static Routing Table

Trailer Encapsulation

ARP Cache Timeout

Default TCP TTL

Keepalive Time

Keepalive Data

NIS Senrer Addresses

NIS Domain

Ethernet Encapsulation

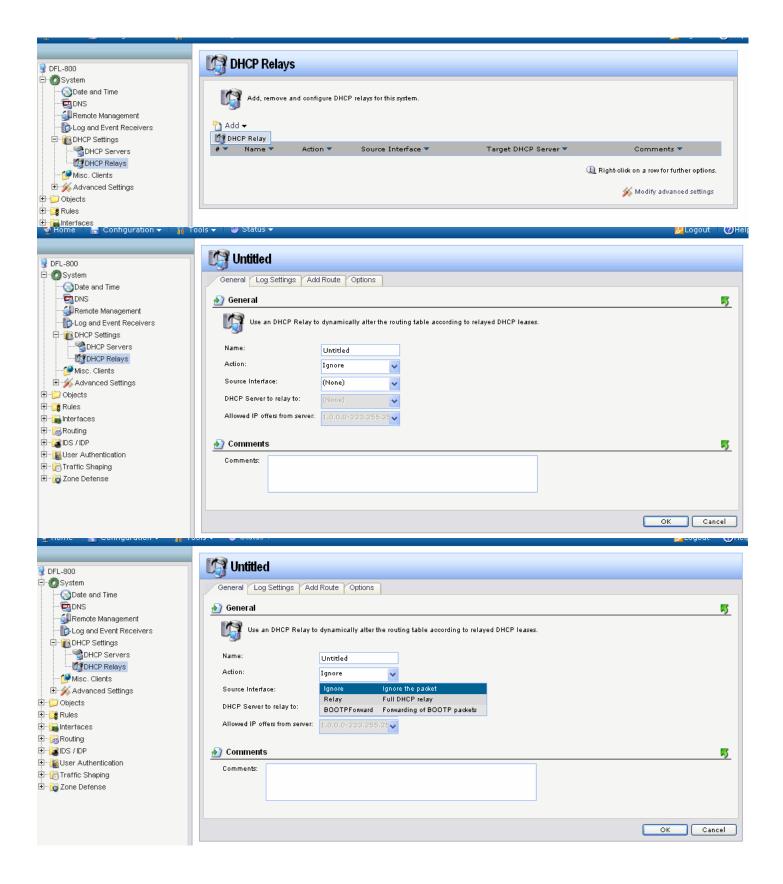
Router Solicitation Address

		-10	NET DIOD NODE Type
s	;	47	NETBIOS Scope
1		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	StreatTalk Server Addresses

~

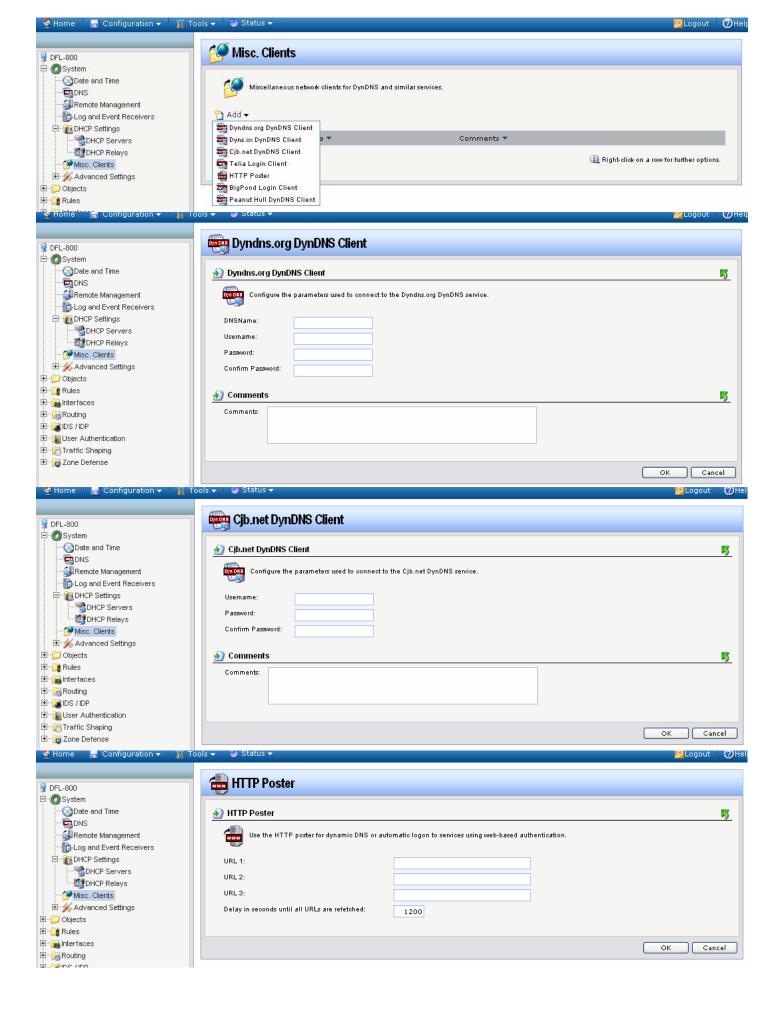
) General		
Extend	the DHCP Server fun	ctionality by adding custom options th
<u>_</u>		
Code:	(None)	
_		
Туре:	UINT8	~
Parameter:	UINTS	1 byte
	UINTELIST	1 byte list
Commente	UINT16	2 bytes
) Comments	UINT16LIST	2 bytes list
Comments:	UINT32	4 bytes
	UINT32LIST	4 bytes list
	IP4	IP address
	IP4LIST	IP address list
	STRING	Character data
	BINARY	Hexadecimal data

🍨 Home 👘 🔚 Configuration 👻 🕴 🏭	Tools → I 🥥 Status → 🥠 Logout I 🕐
] or:	Tutitled
DFL-800	Si chaoa
∃~ @ System — ⊗ Date and Time	General Options Custom Options Log Settings
Remote Management	🔊 General 🐬
Log and Event Receivers	Select log receiver(s) and severity to enable logging for this object.
E- R DHCP Settings	
DHCP Servers	Enable logging:
DHCP Relays	Severity: Notice
🧐 Misc. Clients	
E 🕺 Advanced Settings	
∃	Dog Receivers
🗄 📴 Rules	Log to:
	G All receivers
E- 🙀 Routing	C Specific receiver(s):
	Available Selected
	MemLog >>
E- 👩 Traffic Shaping	
E- 🐻 Zone Defense	
	OK Cancel
Untitled	
Jonadod	
General Options Custor	Options / Log Settings
釣 General	
Select log receiver(s	and severity to enable logging for this object.
Enable logging: 🔽	
Severity: Notice	▼
Debug	
Log Receivers Info	
Notice	
Log to: Warning	
All Error	
C Spe Critical	
Mandan	
IMemLog gen	¥
C	

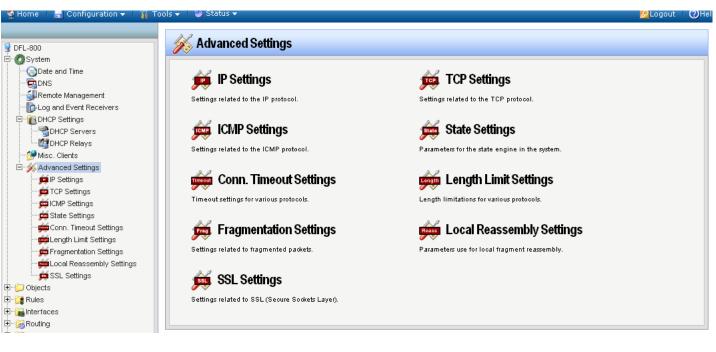


Untitled	1				
General Log	Settings Add	Route Options			
🎒 General					
Use ar	n DHCP Relay to	dynamically alter the routi	ng table according to relaye	ed DHCP I₁	
Name:		Untitled			
Action:		Ignore 🗸 🗸			
Source Interfa	ce:	(None) 🗸			
DHCP Server t	o relay to:		ments		
Allowed IP off	ers from server:	(None) 🚘 any			
🔊 Comments	i -	ing core			
Comments:		iiii) lan iiii) wan1			
		时 wan2			
Pone Configuration		Untitled		_	Mradian - Que
⊡ • 💋 System ⊗Date and Time		General Log Settings Add Rout	e Options		
DNS Remote Management Log and Event Receive DHCP Settings DHCP Servers DHCP Relays		General Select log receiver(s) and se Enable logging: Severity: Notice	everity to enable logging for this object.		<u> </u>
⊞ - Á Advanced Settings ⊞ - 🎾 Objects	<u>ź</u>	🔰 Log Receivers			<u>5</u>
Rules Interfaces IDS / IDP Sulting Jos / IDP Sulting Sultant Authentication Traffic Shaping Sone Defense		Log to: C All receivers Specific receiver(s): Available MemLog C C C	ecte d		
					OK Cancel

🦉 Home 🛛 🔂 Configuration 👻 🛛 🚻	Tools 🗸 T 🧉 Status 🗸	ZLogout (20H
	-	
😼 DFL-800	Mittled Control of the second se	
Ē. OSystem	General Log Settings Add Route Options	
🛛 🚫 Date and Time	General Log Settings Add Route Options	
	🔊 General	5
	Add dynamic routes for this relayed DHCP lease.	
Log and Event Receivers		
DHCP Settings	Parameters to be set in added route	<u>म</u>
DHCP Servers		
Misc. Clients	RoutingTable: (None)	
	Local IP: (None)	
🗄 📲 📴 Rules	Gateway IP: (None)	
🗄 🕞 Interfaces		
E. Bouting	2 Proxy ARP	న
E- Contraction of the second s	Interface to ARP publish the added route on.	
Wer Authentication Traffic Shaping	Available Selected	
E. O Zone Defense	wan1	
	wan2 dmz	
	lan <	
	Always select ALL interfaces, including new ones.	
		OK Cancel
Superior Configuration - III		Zagodi 🕐 🗸
😨 DFL-800	Intitled	
En Coool	- 32	
Date and Time	General Log Settings Add Route Options	
	n General	5
Remote Management		
Log and Event Receivers	Max relays per Interface:	
DHCP Settings	(1) If this option is not specified (or is 0) unlimited relays is assumed.	
DHCP Servers		
Misc. Clients	Define what ip the relayer should use as gateway ip when passing the requests to the DHCP server.	
E → Advanced Settings	C 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.	
E. Sales	Allow NULL offers	
E linterfaces	(1) Accept server responses offering IP address "0.0.0.0" (no IP address offered).	
E		
E B IDS / IDP		OK Cancel
Generation		



🧐 Home 🛛 🔂 Configuration 👻 🛛 🚻	Tools 🗸 🛛 😈 Status 🗸	💋 Logout 🗆 🕐 Help
2	BigPond Login Client	
3 DFL-800		
🖻 🧑 System		
	n 🔊 BigPond Login Client	5
	Configure the parameters used to provide automatic logon to BigPond internet service.	
E- n DHCP Settings		
DHCP Servers	Usemame:	
DHCP Relays	Password:	
	Confirm Password:	
Misc. Clients		
🗄 🚿 Advanced Settings		
🗄 🗁 Objects	Comments	5
🗄 📲 🙀 Rules	Comments:	
⊞ 🚰 Interfaces	comments.	
E. Brouting		
. Ser Authentication		
E 🖓 Traffic Shaping		OK Cancel
🗄 🖓 📷 Zone Defense		
		200000 VIII0
😏 DFL-800	Peanut Hull DynDNS Client	
🖻 🕜 System		
	Peanut Hull DynDNS Client	5
		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Remote Management	Configure the parameters used to connect to the Peanut Hull DynDNS service.	
	Configure the parameters used to connect to the Peanut Hull DynDNS service.	
Log and Event Receivers		
⊟ In DHCP Settings	DNSNames:	
	Username:	
DHCP Relays		
🧐 Misc. Clients	Password:	
🗄 🝌 Advanced Settings	Confirm Password:	
⊕ j Objects		
	Ormments	5
	Comments:	
🗄 🗠 🛜 Routing	Comments.	
🖳 🖓 IDS / IDP		
🗄 📓 User Authentication		
E. G Zone Defense		
~		OK Cancel
🧐 Home 👘 🚽 Configuration 👻 👘	Tools 🗸 🗏 🥶 Status 🗸	💋 Logout 🛛 🕐 He
-	Telia Login Client	
3 DFL-800		
🗄 🧑 System		
	🔊 Telia Login Client	5
	Configure the parameters used to provide automatic logon to Telia internet service.	
Log and Event Receivers		
DHCP Settings	Username:	
DHCP Servers	Password:	
DHCP Relays		
🧐 Misc. Clients	Confirm Password:	
표 🍌 Advanced Settings		
	Somments	5
Em 🔓 Rules		
Endes Endes	Comments:	
E. Souting		
E-Contraction (IDP)		
E 🕵 User Authentication		
🗄 😳 Traffic Shaping		OK Cancel
🗄 🔂 Zone Defense		



🔮 Home 🔄 🔚 Configuration 👻 🛛 🌇 Tools 👻 🛛 🥪 Status 👻 🖉 Logout 💷 🕐 He 🗰 IP Settings 😼 DFL-800 🗄 🕜 System 🚫 Date and Time 射 IP Settings 5 🖻 DNS 뤻 Remote Management Settings related to the IP protocol. http://www.communications.com/ E- M DHCP Settings Log Checksum Errors: **~** Log IP packets with bad checksums CHCP Servers Log non IP4: **~** Log occurences of non-IPv4 packets DHCP Relays Log Received TTL 0: **~** Log received packets with TTL=0; this should never happen! 🧐 Misc. Clients Block 0000 SRC: Drop Block 0.0.0.0 as source address Y Advanced Settings DropLog Block 0 Net: Block 0.* source addresses 🗯 IP Settings 🗯 TCP Settings DropLog Block 127 Net: ¥ Block 127.* source addresses 🗯 ICMP Settings Block Multicast SRC: DropLog Block multicast source addresses (224.0.0.0--255.255.255.255) 🗯 State Settings 🚎 Conn. Timeout Settings TTL Min: The minimum IP Time-To-Live value accepted on receipt 3 🚎 Length Limit Settings DropLog TTL on Low: v What action to take on too low TTL values Fragmentation Settings Default TTL: The default IP Time-To-Live of packets originated by the firewall (32-255) 255 🚎 Local Reassembly Settings 🗯 SSL Settings ValidateLogBad Laver Size Consistency: ¥ TCP/UDP/ICMP/etc laver data and header sizes matching lower laver size information SecuRemoteUDP Allow IP data to contain eight bytes more than the UDP total length field specifies -- Checkpoint Securemote violates NAT-T drafts 🗄 📴 Rules Compability: 🗄 🔂 Interfaces IP Option Sizes: ValidateLogBad Validity of IP header option sizes v 🗄 🖓 👸 Routing DropLog IP Option Source/Return: ¥ How to handle IP packets with contained source or return routes 🗄 🖓 IDS / IDP E 🔂 User Authentication IP Options Timestamps: DropLog How to handle IP packets with contained Timestamps ¥ 🗄 🔀 Traffic Shaping IP Options Route Alert: ValidateLogBad ~ How to handle IP packets with contained Route Alert 🗄 🖓 📷 Zone Defense IP Options Other: DropLog ¥ How to handle IP options not specified above Directed Broadcasts: DropLog v How to handle directed broadcasts being passed from one iface to another DropLog ¥ IP Reserved Flag: How to handle the IP Reserved Flag, if set; it should never be Strip DontFragment: Strip the Dont Fragment flag for packets of this size or smaller 65535 οк Cancel 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 packets with TTL=0 Log Received TTL 0: Drop Block 0000 SRC: ¥ Block 0.0.0.0 as source address Ignore Ignore and pass on Block 0 Net: ses Log Log and pass on Block 127 Net: Drop Drop the entire packet resses DropLog Drop and log the packet Block Multicast SRC: prote manucast source addresses ( TTL Min: з The minimum IP Time-To-Live v DropLog TTL on Low: What action to take on too lo Default TTL: 255 The default IP Time-To-Live ValidateLogBad v TCP/UDP/ICMP/etc layer da Layer Size Consistency: Validate and pass on SecuRemoteUDP ValidateSilent n eig Compability: Validate and pass on, log if bad AT-T ValidateLogBad ValidateLogBad IP Option Sizes: v Validity of IP header option

## D-Link® Building Networks for People

IP Settings
 TCP Settings
 ICMP Settings
 State Settings
 Conn. Timeout Settings
 I andth Linit Settings

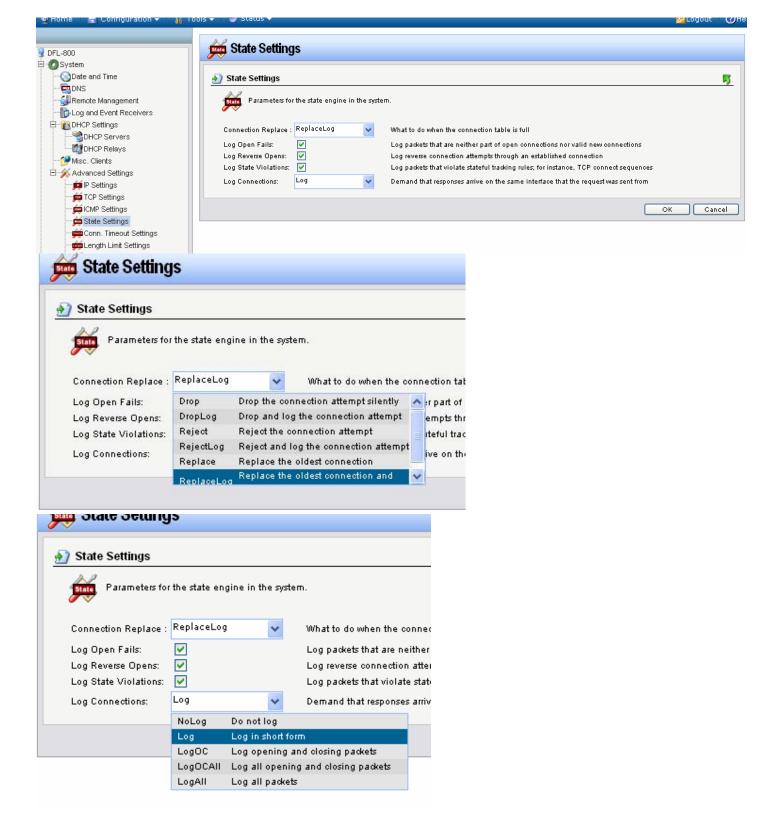
🤹 Home 🛛 🚍 Configuration 👻 🦷 🌠 Tools 👻 😂 Status 👻

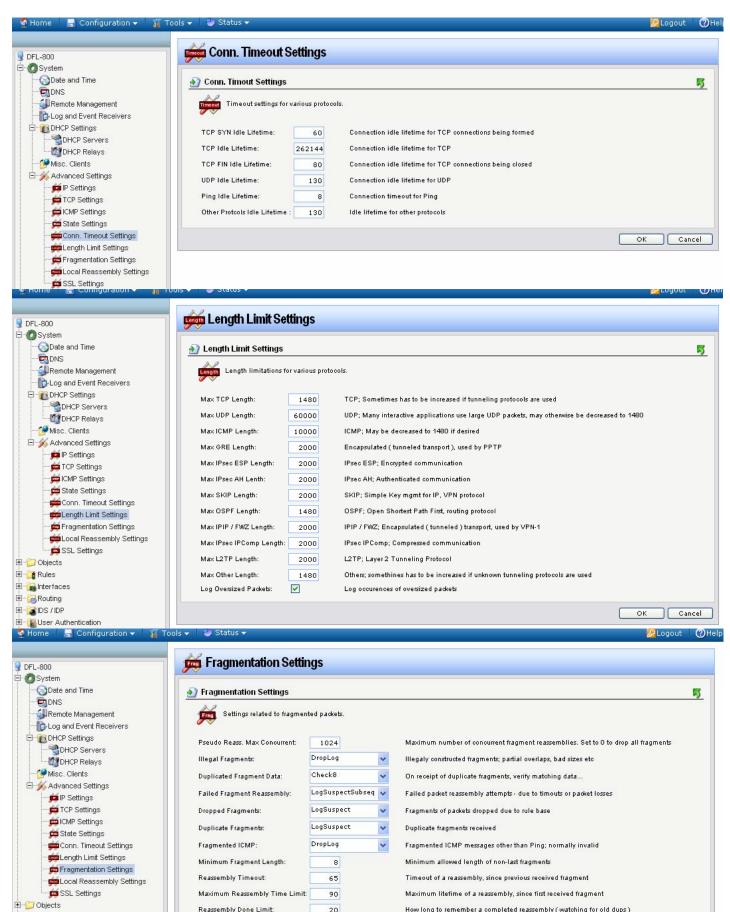


Logged in as **administrator** admin - 192.168.1.115

🖉 Logout 🛛 🕐 Help

300	10 TCP Settings		
ystem Date and Time	TCP Settings		E)
DNS	 }		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Remote Management	Settings related to the T	CP protocol.	
Log and Event Receivers			
DHCP Servers	TCP Option Sizes:	ValidateLogBad 💙	Validity of TCP header option sizes
DHCP Relays	TCP MSS Min:	100	Minimum allowed TCP MSS ( Maximum Segment Size)
Misc. Clients	TCP MSS on Low:	DropLog 🗸 🗸	How to handle too low MSS values
Advanced Settings	TCP MSS Max:	1460	Maximum allowed TCP MSS ( Maximum Segment Size )
TCP Settings	TCP MSS VPN Max:	1400	Limits TCP MSS for VPN connections; minimizes fragmentation
GICMP Settings	TCP MSS on High:	Adjust 🗸	How to handle too high MSS values
🗯 State Settings			
Conn. Timeout Settings	TCP MSS Log Level: TCP Auto Clamping:	7000	When to log regarding too high TCP MSS, if not logged by 'TCP MSS on high' Automatically clamp TCP MSS according to MTU of involved interfaces - in addidtion to 'TCP MSS max'
🚎 Length Limit Settings	TCP Zero Unused ACK:	V	Force unused ACK fields to zero; helps prevent connection spoofing
- Docal Reassembly Settings	TCP Zero Unused URG:		Force unused LIRG fields to zero; prevents small information leak
🗯 SSL Settings	TCP Option WSOPT:	ValidateLogBad 🛛 🗸	The WSOPT (Window Scale) option (common)
bjects	TCP Option SACK:	ValidateLogBad 🗸 🗸	The SACK/SACKPERMIT (Selective ACK) options (common )
ules	TCP Option TSOPT:	ValidateLogBad 🗸	The TSOPT ( Timestamp ) option ( common )
terfaces outing			
S / IDP	TCP Option ALTCHKREQ:	StripLog 🖌	The ALTCHKREQ (Alternate Checksum Request) option
ser Authentication	TCP Option ALTCHKDATA:	StripLog 🖌 🖌	The ALTCHKDATA ( Alternate Checksum Data ) option
affic Shaping	TCP Option Connection Timeou	t: StripLogBad 🛛 🖌 🍟	The CC ( Connection Count ) option series ( semi common )
one Defense	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 )
			The TCP PSH flag together with SYN; normally invalid but always used by some IP stacks (strip=strip PSH)
	TCP SYN / 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:		
			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
			OK Cancel
CP MSS on Low:	DropLog	Mow to	OK Cancel
CP MSS on Low: CP MSS Max:	DropLog 1460		
		Maxim	handle too low M!
CP MSS Max: CP MSS VPN Max:	1460	Maxim Limits 1	handle too low M: um allowed TCP N TCP MSS for VPN
CP MSS Max: CP MSS VPN Max: CP MSS on High:	1460 1400 Adjust	Maxim Limits ⁻ How to	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N
CP MSS Max: CP MSS VPN Max:	1460 1400 Adjust Ignore Ign	Maxim Limits ⁻ How to ore	handle too low M: um allowed TCP N TCP MSS for VPN
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level:	1460 1400 Adjust Ignore Ign Log Log	Maxim Limits ⁻ • How to ore	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too
CP MSS Max: CP MSS VPN Max: CP MSS on High:	1460 1400 Adjust Ignore Ign Log Log	Maxim Limits ⁻ How to ore	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj	Maxim Limits ⁻ • How to ore	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj	Maxim Limits How to ore a just to comply and iust to comply and	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro	Maxim Limits Wow to ore g just to comply just to comply and p the entire pack	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. iet
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro	Maxim Limits How to ore g just to comply just to comply and p the entire pack p and log the pa	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ds. ts. too
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro	Maxim Limits How to ore g just to comply just to comply and p the entire pack p and log the pa	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. iet
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The With	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ds. ts. too
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The With	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The With	handle too low M: um allowed TCP M TCP MSS for VPN handle too high M CF d log too CF d log ts. tet ds SOPT (Window Sc
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The W The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK:	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The W The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration -	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad	Maxim Limits How to ore g just to comply iust to comply and p the entire pack p and log the pa The W The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration V	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad	Maxim Limits How to ore g ust to comply iust to comply and or p and log the pack or p and log the pack The WS The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: Ime Configuration	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad	Maxim Limits How to ore g ust to comply iust to comply and or p and log the pack or p and log the pack The WS The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. tet ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: Ime Configuration -	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro validateLogBad ValidateLogBad	Maxim Limits How to ore g ust to comply iust to comply and or p and log the pack or p and log the pack The WS The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. ret ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration <	1460 1400 Adjust Ignore Ign Log Log Adjust Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad ValidateLogBad	Maxim Limits How to ore g just to comply just to comply and p the entire pack p and log the pa The W The SA	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts. ret ts SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration <	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad ValidateLogBad	Maxim Limits 7 We have to ore g ust to comply iust to comply and or p and log the part or p and log the part The SA tings s elated to the ICMP prote	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N CF d log ts- too CF d log ts- tot SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration V System System System Data and Time DNS Arenote Management CO Decestings	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad ValidateLogBad	Maxim Limits T How to ore g just to comply inst to comply and op the entire pack op and log the pa The W The SA tings s elated to the ICMP proto Second Limit: 500	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts- tet ds SOPT (Window Sc ACK/SACKPERMIT Cool. Maximum number of ICMP responses that will be sent each second
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: Imme Configuration > 600 System System Solate and Time DNS Remote Management CD DHCP Settings DHCP Settings	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad ValidateLogBad	Maxim Limits 7 We have to ore g ust to comply iust to comply and or p and log the part or p and log the part The SA tings s elated to the ICMP prote	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N CF d log ts- too CF d log ts- tot SOPT (Window Sc ACK/SACKPERMIT
CP MSS Max: CP MSS VPN Max: CP MSS on High: CP MSS Log Level: CP Auto Clamping: CP Zero Unused ACK: CP Zero Unused URG: CP Option WSOPT: CP Option SACK: me Configuration V System System System Data and Time DNS Arenote Management CO Decestings	1460 1400 Adjust Ignore Ign Log Log Adjust Adj AdjustLog Adj Drop Dro DropLog Dro ValidateLogBad ValidateLogBad ValidateLogBad	Maxim Limits T How to ore g just to comply inst to comply and op the entire pack op and log the pa The W The SA tings s elated to the ICMP proto Second Limit: 500	handle too low M: um allowed TCP N TCP MSS for VPN handle too high N too CF d log ts- tet ds SOPT (Window Sc ACK/SACKPERMIT Cool. Maximum number of ICMP responses that will be sent each second





How long to remember a completed reassembly (watching for old dups )

Reassembly Illegal Limit How long to remember an illegal reassembly (watching for more fragments ) 60

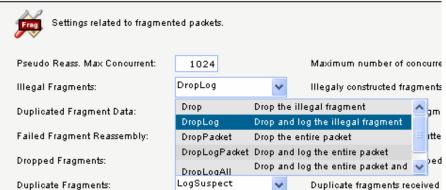
> Cancel OK

E CONDS / IDP 🗄 📆 User Authentication

🗄 🤰 Rules

🗄 🚘 Interfaces 🗄 🛜 Routing

#### Fragmentation Settings

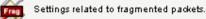


Fragmentation Settings

Settings related to fragmented packets.

Pseudo Re <i>as</i> s. Max Concurrent:	1024	Maximum number of co
Illegal Fragments:	DropLog	Illegaly constructed frag
Duplicated Fragment Data:	Check8	On receipt of duplicate 1
Failed Fragment Reassembly:	None	Nowhere
·	Check/2	in 2-four byte samples (total 8)
Dropped Fragments:	Check 4	in 4-four byte samples (total 16)
Duelle de Deservate	Check8	in 8-four byte samples (total 32)
Duplicate Fragments:	Check16	in 16-four byte samples (total 64)
Fragmented ICMP:	Chedk32	in 32-four byte samples (total 128) s
-	Check 64	in 64-four byte samples (total 256)
Minimum Fragment Length:	Check128	in 128-four byte samples (total 512) t
Reassembly Timeout:	Chedk256	in 256-four byte samples (total 1024) b
r -	Check/512	in 512-four byte samples (total 2048)
Maximum Reassembly Time Limit:	90	Maximum litetime of a r

### Fragmentation Settings



Pseudo Reass. Max Concurrent:	1024	Maximum number of con	cui
Illegal Fragments:	DropLog	V Illegaly constructed fragm	пег
Duplicated Fragment Data:	Check8	<ul> <li>On receipt of duplicate fr.</li> </ul>	agı
Failed Fragment Reassembly:	LogSuspectSubseq	<ul> <li>Failed packet reassembly</li> </ul>	at
Dropped Fragments:	NoLog	Do not log 🔨	
Duplicate Fragments:	LogSuspect	Log "suspect" failures; affected by illegal frags	e
Fragmented ICMP:	LogSuspectSubseq	Log "suspect" failures and all subsequent frags	e:
• • • • • • • • • • • • • • • • • • • •	LogAll	Log normal failures 🛛 🗡	Ł
Minimum Fraoment Lenoth:	8	Minimum allowed length	of

## Fragmentation Settings



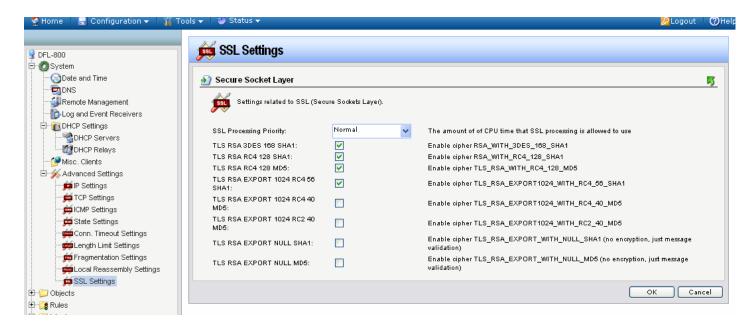
# Free Settings related to fragmented packets.

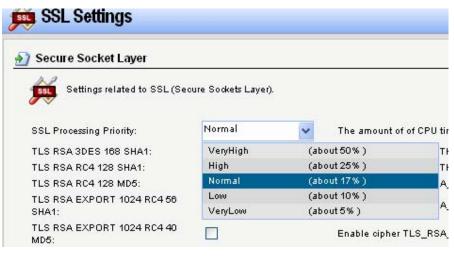
Pseudo Re <i>as</i> s. Max Concurrent:	1024		Maximum number of con-
Illegal Fragments:	DropLog	*	Illegaly constructed fragm
Duplicated Fragment Data:	Check8	*	On receipt of duplicate fra
Failed Fragment Reassembly:	LogSuspectSu	oseq 🔽	Failed packet reassembly
Dropped Fragments:	LogSuspect	*	Fragments of packets drop
Duplicate Fragments:	NoLog [	Do not log	pei
	LogSuspect I	Log if reasse	mbly suspect
Fragmented ICMP:	LogAll I	Log if suspe	ct or if Rules say to log say

### Fragmentation Settings

Settings related to fragment	ted packets.			
Pseudo Reass. Max Concurrent:	1024		Maximum number of	conc
Illegal Fragments:	DropLog	*	Illegaly constructed f	ragme
Duplicated Fragment Data:	Check8	*	On receipt of duplica	te fra
Failed Fragment Reassembly:	LogSuspectSu	bseq 🗸	Failed packet reasser	nbly 2
Dropped Fragments:	LogSuspect	*	Fragments of packets	dropj
Duplicate Fragments:	LogSuspect	*	Duplicate fragments	receiv
Fragmented ICMP:	DropLog	*	Fragmented ICMP m	essag
Minimum Fragment Length:	Ignore	Ignore and p	ass on	th c
Reassembly Timeout:	Log	Log and pas		ly, s
	Drop	Drop the ent		
Ma×imum Reassembly Time Limit:	DropLog	Drop and log	) the packet	rea

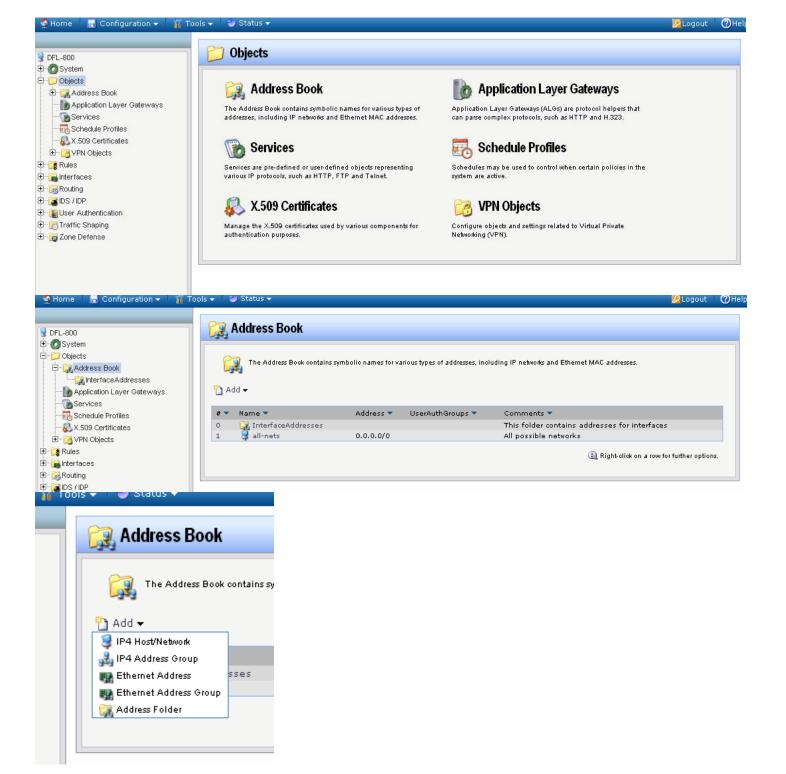
层 Configuration 🗸 🏾 🌇 Tools 🗸 🗳 Status 🔻 🖉 Logout 🛛 🕐 He Local Reassembly Settings 😨 DFL-800 E OSystem 🕤 Date and Time Local Reassembly Settings 5 DNS Rease Parameters use for local fragment reassembly. 剑 Remote Management Log and Event Receivers DHCP Settings Max Concurrent: 256 Maximum number of concurrent local reassemblies BHCP Servers DHCP Relays Max Size: 10000 Maximum size of a locally reassembled packet Misc. Clients Number of large ( >2K) local reassembly buffers ( of the above size ) Large Buffers: 32 E KAdvanced Settings Dir Settings ОК Cancel TCP Settings DicMP Settings 🗯 State Settings 🚎 Conn. Timeout Settings 🗯 Length Limit Settings





🚳 Home

might Fragmentation Settings 🚎 Local Reassembly Settings 🗯 SSL Settings



General User Authentio	100n		l
Use an IP4 Addr Name: Untitled IP Address:	ss item to define a name for a specific	IP4 host, network or range.	
Comments:			
			OK Cance

heral User Authentication	
General	
Groups and user names that belong to this network object. I les section.	Dbjects that filter on credentials can only be used as source nets and destination nets in the
omma-separated list of user names and groups:	
No defined credentials	
	er authentication, but that it has no credentials (user names or groups) defined. This means th gnores any kind of group membership.

eneral User	Authentication							
General								
🛃 An IP4 /	Address Group is 1	used for comb	ining several IP4	4 Address obje	cts for simplif	ied managemen	t.	
Name:	Untitled							
Group members	2		Selected					
	lan_ip lannet	<u>^</u> >	2					
	dmz_ip dmznet							
	wan1_ip wan1net	<	<u>&lt;</u>					
	waninet		, L					
Comments								
Comments:						6		
						4		

ets and destinations nets in the
or groups) defined. This means th
:

🕎 Untitled		
General Use an Name: MAC Address:	Ethernet Address item to define a symbolic name for an Ethernet MAC address.	<u> 5</u>
Comments		<u> 5</u>
		OK Cancel

) General					
An Ethe	rnet Address Group i	s used for combining several Ethe	ernet Address objects for sin	nplified management.	
Name:	Untitled	6			
Group members	: Available	Selected			
) Comments		×> <<			
Comments:					

🧝 Untitle	ed				
🔊 General					呀
Name:	Untitled	to group related addr	ress objects for a better or	rerview.	5
Comments:					
					OK Cancel



	2
800	💘 lan ip
System	
Objects	General User Authentication
· CAldress Book	D Canada
InterfaceAddresses	🔊 General 🐬
	Use an IP4 Address item to define a name for a specific IP4 host, network or range.
Mapplication Layer Gateways	See an in FAddress item to define a name for a specific in Flick, nework of range.
Services	
Schedule Profiles	Name: lan_ip
& X.509 Certificates	IP Address: 192,168,1.1
VPN Objects	
Rules	Comments     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S     S
Interfaces	· · · · · · · · · · · · · · · · · · ·
Routing	Comments: IPAddress of interface lan
IDS / IDP	
User Authentication	
Traffic Shaping	
Zone Defense	
	OK Cancel
Home 🛛 🔚 Configuration 👻 🛛 🚻	Tools 🗸 🖕 Status 👻 😕 🖉
	😼 lan_ip
DFL-800	2 milh
O System	General User Authentication
Dijects	
🖻 🙀 Address Book	🛃 General 🗾
🙀 InterfaceAddresses	
Application Layer Gateways	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:
🗄 🗠 🔀 VPN Objects	
🔁 Rules	
📷 Interfaces	
Routing	
🔂 IDS / IDP	No defined oredentials
Ser Authentication	🚇 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
Traffic Shaping	the network object only requires that a user is authenticated, but ignores any kind of group membership.
🐻 Zone Defense	
-	OK Cancel

💯 Logout 🛛 🕜 Help

		arogoot 🕐
	http://www.communication.com/communication.com/communication.com/communication.com/communication.com/communication.com/communication.com/com/com/com/com/com/com/com/com/com/	
FL-800 System Objects Address Book Address Book Address Book Content of the state of the s	Application Layer Gateways (ALGs) are protocol helpers that can parse complex protocols, such as HTTP and H.323.	
Constant of the second se	# Name *       Type *       Parameters *       Common         0       http-outbound       ALG_HTTP       Strip ActiveX, Strip Java Applets, Strip Scripts       1         1       ftp-inbound       ALG_FTP       Client in active mode allowed       1         2       ftp-outbound       ALG_FTP       Server in passive mode allowed       1         3       if ftp-passthrough       ALG_FTP       Client in active mode allowed, Server in passive m       1         4       if ftp-internal       ALG_FTP       Client in active mode allowed, Server in passive m       1         5       H323       ALG_H323       1       1	ments <b>v</b>
ne El Connguración 🗸 800	In this States	arodoar (4
System Mojects Adplication Layer Gateway: Services Schedule Profiles X.509 Certificates	S Use an HTTP Application Layer Gateway to filter HTTP traffic. Edit the settings for Add → NHTP URL	or this folder
VPN Objects Rules Routing	# ✓ Action ✓ URL ✓ Comments ✓ ① Right-olick on a row for fu	nther options.
General		5
whitelist entries, i.e. r	Ls to deny access to complete sites, to file types by extension, or to URLs with certain words in them. No content filtering is performe no active content stripping, blacklist lookups, etc. g/preventing all access to a whole site	don
example.com/* *.example.com/*		
-	th and double variations to allow/prevent access to "example.com" as well as "www.example.com" without false positives.	
Action: URL:	Blacklist	
Comments		5
Comments:		
	ОК	Cancel

💡 DFL-800	tp-inbound
± 🕐 System	
⊡ 📁 Objects	🔊 General 🐬
E 🙀 Address Book 🍙 Application Layer Gateways	👔 Use an FTP Application Layer Gateway to manage FTP traffic through the system.
Services	Name: fra-inhound
	Name: ftp-inbound
🕹 X.509 Certificates	Data Channel Restrictions
E… 🎦 VPN Objects ⊷ 🌠 Rules	· · · · · · · · · · · · · · · · · · ·
- a Interfaces	Allow client to use active mode (unsafe for client)
Routing	Client data ports: 1024-65535
🚰 IDS / IDP	Allow server to use passive mode (unsafe for server)
🌆 User Authentication	Server data ports: 1024-65535
∽ॡॖॊTraffic Shaping ∽ॡॊ Zone Defense	(1) If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.
	Command Restrictions
	Allow unknown commands
	2 Control Channel Restrictions
	Maximum line length in control channel: 256
	Maximum number of commands per second: 20
	Allow 8-bit strings in control channel
	Ocmments
	Comments:
	OK Cancel
Home 🗆 🔚 Configuration 👻 🛛 🚻	lools → I → Status → ZLogout I ()F
DFL-800	by ftp-passthrough
O System	
" <mark>&gt;&gt;</mark> Objects ≢ <b>;;;;</b> Address Book	👌 General 🐬
Application Layer Gateways	by Use an FTP Application Layer Gateway to manage FTP traffic through the system.
	Name: ftp-passthrough
	tep passunougn
	👔 🛃 Data Channel Restrictions 🗾 🦻
	Data Channel Restrictions
🥞 Rules	Allow client to use active mode (unsafe for client)
🌠 Rules 🚡 Interfaces	
≰ Rules interfaces i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i i	Image: Second system       Image: Second system         Image: Second
i≩ Rules ■ Interfaces i⊗ Routing io / IDP i User Authentication	✓ Allow client to use active mode (unsafe for client) Client data ports: 1024-65535
	Image: Server data ports:       1024-65535         Image: Server data ports:       1024-65535
≩ Rules ■Interfaces ☞ Routing ■IDS / IDP ■User Authentication ऌ Traffic Shaping	<ul> <li>✓ Allow client to use active mode (unsafe for client)</li> <li>Client data ports: 1024-65535</li> <li>✓ Allow server to use passive mode (unsafe for server)</li> <li>Server data ports: 1024-65535</li> <li>④ If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.</li> </ul>
	Image: Server data ports:       1024-65535         Image: Server data ports:       1024-65535
Rules     Interfaces     Routing     DS / IDP     User Authentication     Traffic Shaping	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 ① If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. ② Command Restrictions
Rules       Interfaces       Routing       IDS / IDP       User Authentication       Traffic Shaping	<ul> <li>✓ Allow client to use active mode (unsafe for client)</li> <li>Client data ports: 1024-65535</li> <li>✓ Allow server to use passive mode (unsafe for server)</li> <li>Server data ports: 1024-65535</li> <li>④ If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.</li> </ul>
Rules     Interfaces     Routing     OS / IDP     User Authentication     Traffic Shaping	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 neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.     Ommand Restrictions     Allow unknown commands     Allow SITE EXEC
	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 It neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions Allow unknown commands
<ul> <li>Rules</li> <li>Interfaces</li> <li>Routing</li> <li>IDS / IDP</li> <li>User Authentication</li> <li>Traffic Shaping</li> </ul>	<ul> <li>Allow client to use active mode (unsafe for client)</li> <li>Client data ports: 1024-65535</li> <li>Allow server to use passive mode (unsafe for server)</li> <li>Server data ports: 1024-65535</li> <li>If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.</li> <li>Command Restrictions</li> <li>Allow unknown commands</li> <li>Allow SITE EXEC</li> <li>Control Channel Restrictions</li> </ul>
Rules     Interfaces     Routing     OS / IDP     User Authentication     Traffic Shaping	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 <b>Q</b> If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. <b>Ommand Restrictions Allow unknown commands</b> Allow SITE EXEC <b>Control Channel Restrictions S</b> Maximum line length in control channel: 256
Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction     Construction	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 I or the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions 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
<ul> <li>Rules</li> <li>Interfaces</li> <li>Routing</li> <li>IDS / IDP</li> <li>User Authentication</li> <li>Traffic Shaping</li> </ul>	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 <b>Q</b> If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. <b>Ommand Restrictions Allow unknown commands</b> Allow SITE EXEC <b>Control Channel Restrictions S</b> Maximum line length in control channel: 256
	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 I or the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions 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
<ul> <li>Rules</li> <li>Interfaces</li> <li>Routing</li> <li>IDS / IDP</li> <li>User Authentication</li> <li>Traffic Shaping</li> </ul>	<ul> <li>Allow client to use active mode (unsafe for client)</li> <li>Client data ports: 1024-65535</li> <li>Allow server to use passive mode (unsafe for server)</li> <li>Server data ports: 1024-65535</li> <li>If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.</li> <li>Command Restrictions</li> <li>Allow unknown commands</li> <li>Allow UNTE EXEC</li> <li>Control Channel Restrictions</li> <li>Maximum line length in control channel: 256</li> <li>Maximum number of commands per second: 20</li> <li>Allow 8-bit strings in control channel</li> </ul>
Rules     Interfaces     Routing     TOS / IDP     User Authentication     Traffic Shaping	Allow olient to use active mode (unsafe for olient) Client data ports: 1024-65535 Allow server to use passive mode (unsafe for server) Server data ports: 1024-65535 (1) If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions 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
	Allow olient to use active mode (unsafe for olient) Client data ports: 1024-65535 Allow server to use passive mode (unsafe for server) Server data ports: 1024-65535 (1) If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions 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
<ul> <li>Rules</li> <li>Interfaces</li> <li>Routing</li> <li>IDS / IDP</li> <li>User Authentication</li> <li>Traffic Shaping</li> </ul>	Allow olient to use active mode (unsafe for olient) Client data ports: 1024-65535 Allow server to use passive mode (unsafe for server) Server data ports: 1024-65535 (1) If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode. Command Restrictions 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

😨 DFL-800	tp-internal	
E System		
⊡…© Objects	🛃 General	5
Address Book	use an FTP Application Layer Gateway to manage FTP traffic through the system.	
	Name: ftp-internal	
Schedule Profiles		
&X.509 Certificates 	🛃 Data Channel Restrictions	5
🗈 📴 Rules		
E linterfaces	Allow client to use active mode (unsafe for client) Client data ports: 1024-65535	
E··· 😹 Routing E··· 🚰 IDS / IDP	Allow server to use passive mode (unsafe for server)	
E. Ser Authentication	Server data ports: 1024-65535	
E - ፼ Traffic Shaping E - ፼ Zone Defense	If neccessary, the FTP ALG will do on-the-fly conversion between active and passive mode.	
		_
	Command Restrictions	<u>– 5</u>
	Allow unknown commands Allow SITE EXEC	
		_
	Control Channel Restrictions	<u>, 5</u>
	Maximum line length in control channel: 256	
	Maximum number of commands per second: 20	
	Allow 8-bit strings in control channel	
	n Comments	5
	Comments:	
		OK Cancel
Thomas Countration V 1		Zuguut One
	Н323	
IFL-800 ∰… oo System	1023	
₽ Dijects	🔊 General	5
	Use an H.323 Application Layer Gateway to manage H.323 multimedia traffic.	
b Application Layer Gateways Services		
	Name: H323	
	🕣 TCP data channels	5
⊞ Constant de la	Allow TCP data channels (T.120)	
	Maximum number of TCP data channels per call: 10	
⊕; Bouting ⊕ Compared and the second s	Gatekeeper	ম
User Authentication	Max Gatekeeper Registration Lifetime: 1800 seconds	
⊞; Traffic Shaping ⊞; Zone Defense	(Only used by gatekeeper services)	
		_
	Comments	<u>5</u>
	Comments:	
		OK Cancel

n					
s dress Book plication Layer Gateways		Services are pre-d	efined or use	r-defined objects representing variou	is IP protocols, such as HTTP, FTP and Telnet.
rvices	2	Add 🛨			
hedule Profiles		🔻 Name 🔻	Type 🔻	Parameters 🔻	Comments 💌
509 Certificates	0	Marine - Marine - Mar	Group	all_icmp,all_udp,all_tcp	All ICMP, TCP and UDP services
N Objects	1	all_icmp	ICMP	All	All ICMP services
	2	all_tcp	TCP	0-65535	All TCP services
ces	3	all_udp	UDP	0-65535	All UDP services
3	4	all_tcpudp	Group	all_tcp,all_udp	All TCP and UDP services
P	5	echo	TCP/UDP	- · - ·	Echo service
uthentication	6	Chargen	TCP	, 19	Character generator
Shaping	7	Ssh	TCP	22	Secure shell
efense	8	Ssh-in	TCP	22	Secure shell with SYN flood protection
iciise	9	telnet	TCP	23	Telnet
	1		TCP	25	Simple Mail Transfer Protocol
	1		тср	25	Simple Mail Transfer Protocol with SYN flood protection
	1		TCP/UDP		Legacy time service
	1		тср	53	Domain Name Server via TCP - mainly zone transfers
	1		UDP	53	Domain Name Server via UDP - standard queries
	1		TCP/UDP	53	DNS via TCP and UDP
	1		UDP	67	Bootstrap protocol (also DHCP) server
	1		UDP	68	Bootstrap protocol (also DHCP) client
	1		UDP	69	Trivial File Transfer Protocol
	1		тср	70	Gopher
	2		TCP	79	Finger
	2	1997).	тср	80	World Wide Web HTTP
	2		тср	443	Secure HTTP over SSL/TLS
	2		тср	80	World Wide Web HTTP with SYN flood protection
	2		тср	443	Secure HTTP over SSL/TLS with SYN flood protection
	2		тср	80	HTTP via HTTP ALG "http-outbound" - strips all active conte
	2	6 🔞 pop3	тср	110	Post Office Protocol - Version 3
	2		тср	143	Interactive Mail Access Protocol v2 and v4
	2		ICMP	Echo Request	Outbound ping (also allows traceroute via ICMP)
	2	9 🔞 ping-inbound	ICMP	Echo Request	Inbound ping (does not allow tracerouting)
	31		тср	80,443	HTTP and HTTPS
	3:		UDP	514	Syslog
	3	100 A	тср	3389	Remote Desktop Protocol
	3		тср	111	Sun/Unix Remote Procedure Call
	3		тср	113	Legacy authentication/identification service
	3		тср	119	Network News Transfer Protocol
	3		TCP/UDP	123	Network Time Protocol
	3		TCP/UDP	135	RPC port mapper, used by MS Windows networking

🦉 Home 💷 🔂 Configuration 👻

11

ZLogout (WHel

🛿 Home 🛛 🔂 Configuration 👻	🚻 Tools 🗸	🗧 🥑 Status 👻			🗾 Logout 🛛 🕐
		37 🐚 epmap	TCP/UDP	135	RPC port mapper, used by MS Windows networking
		38 🚡 netbios-name	UDP	137	NetBIOS Name Service
0FL-800		39 🐚 netbios-dam	TCP/UDP	138	NetBIOS Datagram Service
System		40 🔞 netbios-ssn	TCP	139	NetBIOS Session Service - SMB
Objects		41 🔞 microsoft-ds	тср	445	Microsoft-DS - SMB without NetBIOS
Address Book		42 <b>S</b> snmp	UDP	161	Simple Network Management Protocol
- Application Layer Gateways		43 snmp-trap	UDP	162	Simple Network Management Protocol traps (alerts)
		44 🕞 Idap	TCP/UDP		Lightweight Directory Access Protocol
Services		45 Aldaps	TCP	636	Secure LDAP over SSL/TLS
- 📆 Schedule Profiles		46 ke	UDP	500	Internet Key Exchange - key management for IPsec
💫 X.509 Certificates		47 Texec	тср	512	Remote Process Execution
- 🕝 VPN Objects		48 Arlogin	TCP	513	Remote login
Rules			тср	514	Like rexec, but automatic
Interfaces			тср	515	Like rexet, but automatic Line Printer (spooler)
				1433	
Routing			TCP TCP		Microsoft-SQL-Server
IDS / IDP		52 ms-sql-m	TCP/UDP		Microsoft-SQL-Monitor
User Authentication		53 🐚 wins	TCP/UDP		Windows Internet Naming Service
Traffic Shaping		54 👔 12tp-ctl	UDP	1701	Layer Two Tunneling Protocol - control channel
Zone Defense		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	тср	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	тср	21	FTP - protects server against data channel attacks
		65 htp-outbound	тср	21	FTP - protects client against data channel attacks
		66 🕞 ftp-passthroug		21	FTP - unrestricted - allows all transfer modes for client and server
		67 🐚 http-in-all	тср	80,443	HTTP and HTTPS with SYN flood protection
		68 Smb-all		135-139,445	All MS Windows networking ports
				2	
		69 🐚 igmp			Internet Group Management (multicast control)
		70 Tsvp	IPProto	46	Reservation Protocol
		71 gre-encap		47	Generic Routing Encapsulation
		72 jpsec-esp	IPProto	50	IPsec ESP (encrypted and authenticated)
		73 Dipsec-ah	IPProto	51	IPsec AH (authenticated only)
		74 ipsec-natt	UDP	4500	IPsec NAT-traversal (through udp/4500)
		75 jpip-encap	IPProto	94	IP-in-IP encapsulation
		76 jpcomp	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	тср	1723	Point-to-Point Tunneling Protocol - control channel
		80 🐚 H323	TCP	1720	H.323 via H323 ALG - Enables H.323 communication
		81 Batekeeper	UDP	1719	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers
		82 🐚 ftp-internal	тср	21	FTP - protects client and server against data channel attacks
			TOPUPP		n i ii i
Gatekeeper	UDP	1/17		Gatekeepe	ers
: 🐚 ftp-internal	TCP	21		FTP - prote	ects client and server against data channel attacks
3 🛯 🗑 netcon		OP 999		Remote M	

(1) Right-click on a row for further options.

Thome Configuration	11 TOOIS V I Status V
DFL-800 DFL-800 Objects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Dojects Doj	Services are pre-defined
	TCP/UDP Service
	Typ
🗄 🖓 VPN Objects	IP Protocol Service Gro
	Service Group ICN
	2 to all_top TCF
	3 🐚 all_udp 🛛 UDI
	4 🐚 all_tcpudp Gro
	🗌 🔤 5 🦬 echo 🛛 TCI

inne 🛛 🔂 Connigurau		Zuguu
-800	The second secon	
System		
Objects	🔊 🔊 General	
🙀 Address Book		
Application Layer Gat	teways A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.	
Services		
Schedule Profiles	Name: Untitled	
💫 X.509 Certificates	Туре: ТСР 🗸	
🔀 VPN Objects		
Rules	Source: 0-65535	
Interfaces		
Routing	Destination:	
DS / IDP Jser Authentication	🕕 Enter port numbers and/or port ranges separated by commas. For example: 137-139,445	
Fraffic Shaping		
Zone Defense	Pass returned from ICMP error messages from destination SYN flood protection (SYN Relay)	
	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	
	2 Comments	
	Comments:	
	ОК	
🐐 General		
(Time)		
A TCP/	/UDP Service is a definition of an TCP or UDP protocol with sp	
and a second		
Name:	Untitled	
Type:	ТСР	
1984.		
	TCP	
Source:	UDP	
oource.		
Destination:	TCPUDP	
	Inter port numbers and/or port ranges separated by cor	
_		
Туре:	ТСР	
C		
Source:	0-65535	
Destination:		
e counteron.		
	Inter 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	Туре	Comments	
	(None)			
Commonto	🐚 НЗ2З		ALG_H323	
射 Comments	. 👔 ftp-inb	ound	ALG_FTP	
Comments:	👔 ftp-inte	ernal	ALG_FTP	
	👔 ftp-out	bound	ALG_FTP	
	👔 ftp-pas	sthrough	ALG_FTP	
	👔 http-ou	itbound	ALG_HTTP	

2	( Untitled				
ਤੇ DFL-800 ਜੁ⊷@ System	V Onded				
∃ [©] Objects	General ICMP	Parameters			
🗄 🖓 Address Book	約 General				5
Application Layer Gateways	An ICM	P Service is an object definition repre	cepting ICMR traffic wit	h specific parameters	
		r Senice is an object demitton repre	senting former trainion	n specific parameters.	
🖧 X.509 Certificates	Name:	Untitled			
🗄 📴 VPN Objects		Pass returned from ICMP error	messages from destina	tion.	
± <b>≩</b> Rules ± <b>≩ I</b> nterfaces					
	Application	Layer Gateway			5
E IDS / IDP		Layer Gateway (ALG), capable of ma	naging advanced proto	cols, can be specified for this service	
∃ 🌆 User Authentication ∃ 👩 Traffic Shaping					
± 👩 Zone Defense	ALG:	(None)			
	Max Sessions:	1000			
	Comments				5
	Comments:				<u> </u>
	comments.				
					OK Cancel
Application Laura	Cataway				
Application Laye	Galeway				
An Application Layer	Gateway (ALG), capab	le of managing advanced	protocols, can be		
ALG: (N	one) 🗸 🗸				
Max Sessions: N	ame Type	Comments			
	lone)	o o nini cind			
5	а нз23	ALG_H323			
🔰 👌 Comments 👘 📃	ftp-inbound	ALG_FTP			
	a ftp-internal	ALG_FTP			
	ftp-outbound	ALG_FTP			
1	h ftp-passthrough	ALG_FTP			
	http-outbound	ALG_HTTP			
			-		
(					
() Untitled					
General ICMP Paramete	are				
ICMP Parameters					5
Check the ICMP Messa	ge Types applicable to th	s service.			
All ICMP Message					
C ICMP Message Typ	ies				
Type:		Codes:			
Echo Request		0-255			
Destination Ur	nreachable	0-255			
Redirect		1			
		0-255			
Parameter Pro	iorem	0-255			
Echo Reply		0-255			
Source Quenc	hing	0-255	1.1		
Time Exceede	he				
		0-255			
					OK Cancel

General	P Protocol Sen	ice is a definition of	f an IP protocol with specifi	c narameters		
Name:	Untitled					
IP Protocol:						
	(D		1/IP protocol rapidos (copiar	ated by commas) applicable	to this service.	
			nne protocor langes (sepai.	ated by commas) appricable		
	For example:	1-4, 7				
	For example:	1-4, 7	ssages from destination			
) Applicatio	For example:	1-4, 7 rned ICMP error me				
	For example:	1-4, 7 med ICMP error me <b>way</b>	ssages from destination	tocols, can be specified for t	nis service.	
	For example:	1-4, 7 med ICMP error me <b>way</b>	ssages from destination		nis service.	
An Applicatio	For example: Pass retu on Layer Gate	1-4,7 med ICMP error me way way (ALG), capable o	ssages from destination of managing advanced prot		nis service.	
An Applicatio	For example: Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu	1-4, 7 med ICMP error me way way (ALG), capable o (None)	ssages from destination of managing advanced prot		nis service.	
An Applicatio ALG: Max Sessions	For example: Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu Pass retu	1-4, 7 med ICMP error me way way (ALG), capable o (None)	ssages from destination of managing advanced prot		nis service.	

General A Service Group is a collection of service objects, which can then be used by different policies in the system	
Name: Untitled	
Available Selected	
Comments:	

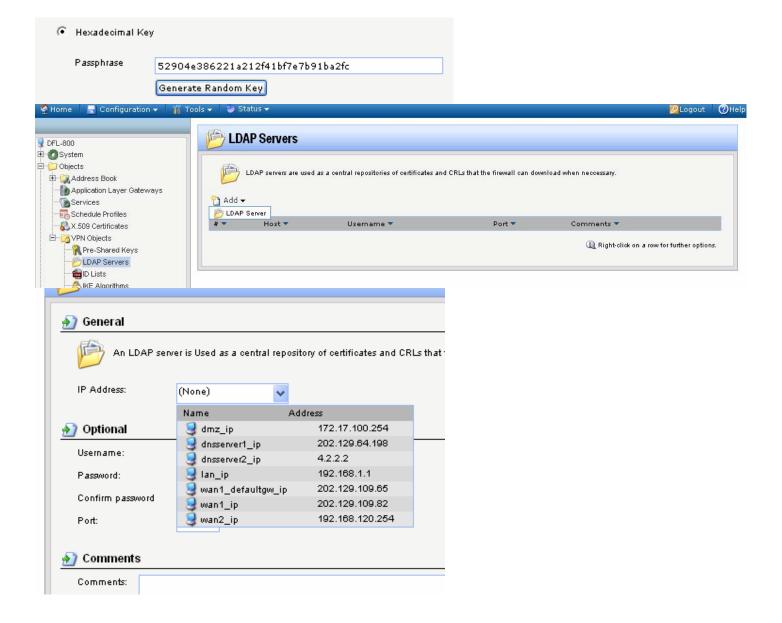
Home 🗆 🔂 Con	figun	ation	- I	- 00	10019			status																	<u>2</u>	Logout	0
FL 000			_	_			Sc	hed	lule F	Profi	es																
FL-800 System Objects Address Book Services Schedule Prot Schedule Prot Sc	ayer G files	≆atew	ays				Add Sche	Sche edule F ame V We Wo Nor	edules r Profile ekday rkingH nWorki ekend	may be s lours ingHou	e used t		trol whe		ain pol			system ndDa		C d Mi Al	omments 💙 onday to Friday, 00: onday to Friday, 08: I hours, except Mon aturday and Sunday,	00-17:0 day to F	00 Friday		17:00		
BDS / IDP User Authentication Traffic Shaping	on																					I F	Right-cl	lick on a	ow for fu	rther option	ns.
Jone Defense																											
Beneral																											5
AS OF	cheo	tule	Prof	ile d	efine	es da	ys ar	nd da	ites ar	nd are	e ther	n use	d by t	the v.	ariou	s poli	cies	in th	e syst	em.							
Name:		/eek	day:												_												
	0	-	-	3	-		6	_	9			12		1:			18	-		21							
Monday												<b>V</b>															
Tuesday		Image: A start of the start	<ul> <li>Image: A start of the start of</li></ul>	<ul> <li>Image: A start of the start of</li></ul>												]		<ul> <li>Image: A start of the start of</li></ul>									
Wednesday	<ul> <li>Image: A start of the start of</li></ul>	<b>&gt;</b>	<b>v</b>	<b>V</b>	<ul> <li>Image: A start of the start of</li></ul>	<b>V</b>	<b>v</b>		• •		<b>V</b>	<b>~</b>					<ul> <li>Image: A start of the start of</li></ul>	<b>V</b>	<b>v</b>	•							
Thursday	•	•	<b>&gt;</b>	•	•				•			•					•	<b>~</b>		•							
Friday	~		<b>v</b>	<b>v</b>	~		<		~ ~			~					~	<b>V</b>	☑	•							
Saturday																]											
Sunday																]											
Start Date:								-																			
End Date:		F						-																			
🄊 Commen	nts																										
Comments:	-	lond	au ti	o Fri	dau.	. 00:	00-2	23(5	9																		2
					-74				5%).																		
																							6	ок		Canc	el
																							-				

Saturday			1 htt	p://	192.	168	(		
Sunday				4	Ju	ne 20	05		$\triangleright \!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!\!$
			Mo	Τu	We	Th	Fr	Sa	Su
Start Date:			30	31	1	2	3	4	5
			6	7	8	9	10	11	12
End Date:			13	14	15	16	17	18	19
-			20	21	22	23	24	25	26
2 Comment	ts		27	28	29	30	1	2	з
Comments:	Monday to Friday, 00:00-2	:3:5	Tim	e: 1	3:55	:43			
				1	) Inte	ernet			

Pome Configuration (100	iis 🗸 T 🔵 30				Zeogoue	
DFL-800     DFL-System     Delcts	💫 X.50	09 Certificates				
Address Book     Application Layer Gateways     Services     Schedule Profiles	⊶⊶	Certificate	rious components for authentication purposes.			
	# 🔻	Name 🔻	Type 🔻	Comments 🔻		
표 🖓 VPN Objects	0	💫 AdminCert	Local			
B- <mark>C</mark> Rules B-				(1) Right-click on a row f	or further option:	IS.
🖭 🖓 IDS / IDP						

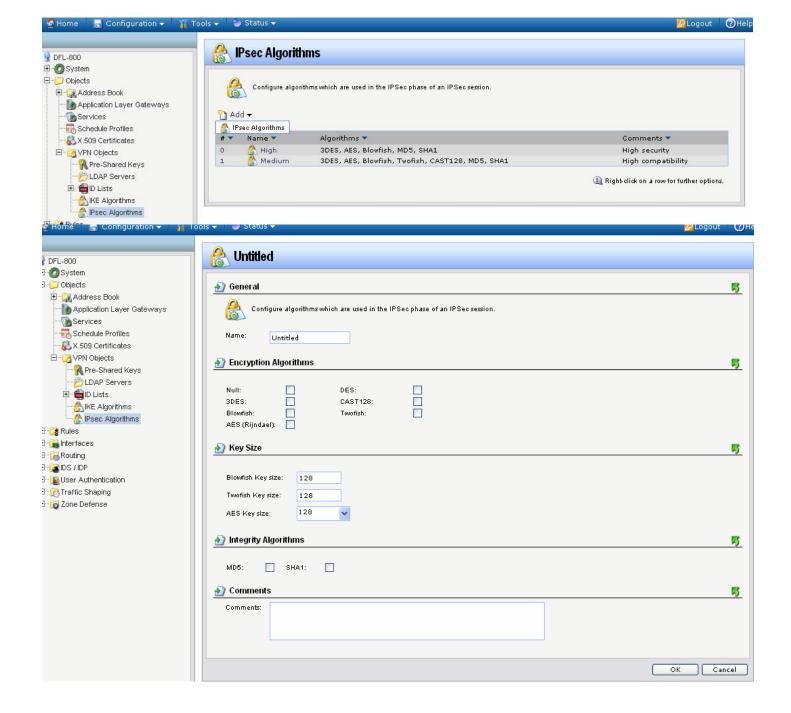
🔮 Home 🗧 Configuration 👻 🌃	Tools 👻  Status 🕶	🙎 Logout 🕜 H
🔮 DFL-800	& AdminCert	
Objects     O	General     An X. 509 certificate is used to authenticate a VPN client or gateway when establishing an IPSec tunnel.	<b>1</b> 5
Schedule Profiles     Schedule Profiles     X,509 Certificates     VPN Objects     Rules	Name: AdminCert	<b>15</b>
Interfaces     Routing     Jos / IDP     User Authentication	Certificate type: Local	<b>1</b> 5
⊞-127 Traffic Shaping ⊞-127 Zone Defense	<ul> <li>Don't upload anything</li> <li>Don't upload anything right now</li> <li>Upload self-signed X.509 Certificate</li> </ul>	
	Upload a remote certificate     Upload a certificate     Upload a certificate     Upload a certificate	
	Comments	<u>5</u>
		OK Cancel

🦉 Home 🛛 🚽 Configuration 👻 🎢 To	ools 👻 🤍 Status 👻	ZLogout OHel
繴 DFL-800	🔗 VPN Objects	
E-COSystem		
E-D Objects		
E Address Book	🙀 Pre-Shared Keys	🖄 LDAP Servers
Application Layer Gateways		
Services	Add, remove and modify Pre-Shared Keys, which are used for IPSec authentication purposes.	LDAP servers are used as a central repositories of certificates and CRLs that the firewall can download when neccessary.
		,
X.509 Certificates	A	
	iD Lists	😤 IKE Algorithms
R Pre-Shared Keys	ID lists contains IDs, which are used within the authentication	Configure algorithms which are used in the IKE phase of an
	process when establishing an IPSec tunnel.	IPSec session.
	🙈 IPsec Algorithms	
Rsec Algorithms		
🗄 📴 Rules	Configure algorithms which are used in the IPSec phase of an	
🗄 🚰 Interfaces	IP Sec session.	
E. Souting		
E DS / IDP		
E Ser Authentication		
Home Configuration - 11 Too	ols 🗸 🔰 🤯 Status 🗸	😕 Logout 💷 🕐 He
	Dra Oharrad Maria	
💡 DFL-800	💦 Pre-Shared Keys	
± OSystem		
	Add, remove and modify Pre-Shared Keys, which are used	for IPSec authentication numbers
🗄 🖓 Address Book		for resectadurentication purposes.
	Add -	
Schedule Profiles	R Pre-Shared Key	
	# 🔻 Name 🔻 Type	<ul> <li>Comments</li> </ul>
E VPN Objects		(1) Right-click on a row for further options.
Pre-Shared Keys		
DAP Servers		
ME Algorithms		
R Untitled		
M Olided		
Conoral		
A General		<u>5</u>
PSK (Pre-Shared Key) .	authentication is based on a shared secret that is known o	nly by the parties involved.
00		
Name: Uptitled		
Name: Untitled		
Shared Secret		馬
C Passphrase		
Shared Secret:		
Confirm Secret:		
Hexadecimal Kev		
Hexadecimal Key		
Passphrase		
Genera	ate Random Key	
🕕 🤃 Since regular words and ph	rases are vulnerable to dictionary attacks, do not use them	as shared secrets.
Comments		5
- comments		2
Comments:		
		OK Cancel
		OK Cancel



🔮 Home 🛛 🚽 Configuration 👻	11 Tools → 🕘 Status 🗸		22Logout	Он
DFL-800 DFL-800 DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOSystem DOS DOS DOS DOS DOS DOS DOS DOS	ID Lists ID lists contains IDs, which are used within the authentica	tion process when establishing an IPSec tunnel.		
Schedule Profiles	Add ▼	Comments 🔻	(1) Right-click on a row for further option:	5,
IDAP Servers				
General			Ŗ	Ľ
An ID list contain	IDs, which are used within the authentication process when es	tablishing an IPSectunnel.		
Comments			<b>.</b>	L
Comments:				
			OK Cancel	

💁 Home 🛛 🚍 Configuration 👻 🍟 Tools 👻  Status 👻	🖉 Logout 🛛 🖉 He
DFL-800	
Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithms which are used in the IKE phase of an IPSecsed         Image: Objects       Image: Configure algorithmsecsed <td>ssion.</td>	ssion.
Schedule Profiles	
↓ X.509 Certificates     # ▼ Name ▼ Algorithms ▼       □ → WPN Objects     0 ↔ High 3DES, AES, Blowfish, MD5, SHA1	Comments 💌 High security
Ress and the second secon	
	(1) Right-click on a row for further options.
KE Algorithms	
Psec Algorithms	
😤 Untitled	
O Constal	
Seneral	<u>R</u>
A Configure algorithms which are used in the IKE phase of an IPSec session.	
Configure algorithms windin are used in the Inc. phase of an in Secsession.	
Name: Untitled	
Encryption Algorithms	5
	<u>v</u>
Null: DES:	
3DES: CAST128:	
Blowfish: Twofish:	
AES (Rijndael):	
Mey Size	<b>5</b>
Step 1	
Blowfish Key size: 128	
Biowish Key size.	
Twofish Key size: 128	
AES Key size:	
🔬 Integrity Algorithms	<b></b>
MD5: SHA1:	
A Commente	-
2) Comments	ন
Comments:	
	OK Cancel

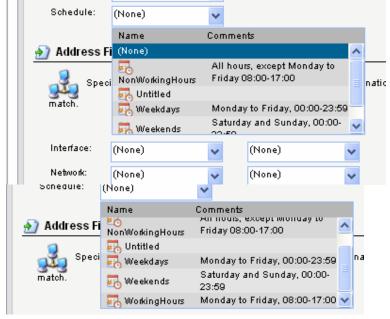


Se Home	🔡 Config	uration 👻 🔰	🖥 Tools 🗸 🛛 🥹	Status 🔫					💯 Logout	()He
				-						
3 DFL-800			🛛 🔁 🥵 R	lles						
E OSystem										
Rules			3	IP Rules			Access			
Ð 🖁 IP R				ules are used to filter IP-base			Add, remove and modify IP spoofing t	ilters that regulates which		
E Interfac				provide means for address ti I Balancing.	ranslation as well as Serve	er	IP addresses the system will accept as			
E Routing										
E CONDS / IDI										
E Subser Al										
🗄 🕝 Zone D	efense									
🔮 Home	🚽 Configu	iration 👻 🎽 🧃	Tools 👻 🙂 S	Status 👻					🖉 Logout	ЮНе
			\$ IP	Rules						
DFL-800			8	Nules						
Dijects			•							
🗏 📑 Rules	a transfer		8	IP Rules are used to filter	IP-based network traffic. I	n addition, the	ey provide means for address translation	n as well as Server Load Bala	ncing.	
E- 💈 IP Ru			bbA 🚰	•						
Acce	an_to_wan1 ess		S IP R							_
🗄 📊 Interface			📴 IP R	ule Folder Action	🔹 SourceInterface 🔻	SourceNet	twork 👻 DestinationInterface 💌	DestinationNetwork 🔻	Service 🔻	
E SRouting				lan_to_wan1 ping_fw Allow	lan	lannet	core	lan_ip	ping-inbour	nd
± GalDS / IDP ± GalUser Aut								12		
E 🔂 Traffic S								(1) Right-click on a row	for further optior	ns.
🗄 👩 Zone De	fense									
Gene Gene	eneral	settings		SAT Server Load Ba						<u>5</u>
1	An IP	rule specifie	s what action to	perform on network t	raffic that matches t	he specifie	d filter criteria.			
		P	12							
Nar	ne:	Untitled								
Acti	ion:	Drop	~							
Ser	vice:	(None)	~							
Sch	nedule:	(Mana)	10.00							
001	readie.	(None)	*							
🄊 A	ddress Fi	ilter								5
mat	3	ify source inte	erface and source	e network, together w	ith destination inter	face and d	estination network. All parame	ters have to match for	the rule to	
		Source		Destination						
Inte	erface:	(None)	~	(None)	~					
Net	work:	(None)	~	(None)	~					
		******								
n Co	omments	5								5
Cor	nments:									
-										
								ОК	Cano	el

Name:	Untitled		
Action:	Drop	✓	
Service:	😡 Drop	Drop the packet silently	
	📥 Reject 🛛	Drop the packet and respond with an ICMP error or TCP reset	
Schedule:	🟦 FoodFast 🔅	Stateless packet forwarding	
	👬 Allow 🔅	Stateful connection creation	
約 Address Fi	EP	Static Address Translation	
	SLB_SAT :	Server Load Balancing using Static Address Translation	
Speci	👬 NAT 🔤	Dynamic Address Translation (hide) tior	
match.			
Service:	(Nana)		
000000	(None)	×	
Schedule:	Name	Comments	
	M323	H.323 via H323 ALG - Enables H.323 communication	~
衸 Address Fi	1323-	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers	
	Gatekeeper	Valencepels	
Speci			.ll par
<u></u>	() Untitled		
match.	() Untitled		=
	all_icmp	All ICMP services	
Interface:	all_services	All ICMP, TCP and UDP services	
	🔞 all_top	All TCP services	
Network:	🐚 all_tcpudp	All TCP and UDP services	
	🐚 all_udp	All UDP services	
Comments	bootpc 👔	Bootstrap protocol (also DHCP) client	
	bootps 👔	Bootstrap protocol (also DHCP) server	
Comments:	() chargen	Character generator	
	Mins-all	DNS via TCP and UDP	
	Mans-tep	Domain Name Server via TCP - mainly zone transfers Domain Name Server via UDP - standard queries	
	())) dns-udp ())) echo	Echo service	
	Cono Con 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-passthrou	gh FTP - unrestricted - allows all transfer modes for client and server	
	🐚 gopher	Gopher	
	🐚 gre-encap	Generic Routing Encapsulation	
	Ministry http	World Wide Web HTTP	
	http-all	HTTP and HTTPS	
	Man http-in	World Wide Web HTTP with SYN flood protection	
	http-in-all	HTTP and HTTPS with SYN flood protection  HTTP via HTTP ALG "http://withound", string all active content	~
	Mile http://www.	A BILLE WART LE ALLS "DOD.OUDO". STUDS ALL ACTIVE CONTENT	

Service: (†	None)	¥	
Schedule:	Name	Comments	
1	🚡 http-outbound	HTTP via HTTP ALG "http-outbound" - strips all active content	1
Addroop Fi	🚡 https	Secure HTTP over SSL/TLS	
Address Fi	🚡 https-in	Secure HTTP over SSL/TLS with SYN flood protection	
	🚡 ident	Legacy authentication/identification service	
Speci 🕜	🚡 igmp	Internet Group Management (multicast control)	
match.	🚡 ike	Internet Key Exchange - key management for IPsec	
(	🐚 imap	Interactive Mail Access Protocol v2 and v4	
(	🚡 ipcomp	IP Payload Compression Protocol	
Interface: (	🚡 ipip-encap	IP-in-IP encapsulation	
	🚡 ipseo-ah	IPsec AH (authenticated only)	
Network:	🚡 ipseo-esp	IPsec ESP (encrypted and authenticated)	
	🚡 ipseo-natt	IPsec NAT-traversal (through udp/4500)	
Comments	🚡 ipseo-suite	The IPsec+IKE suite	
(	🚡 l2tp-ctl	Layer Two Tunneling Protocol - control channel	
Comments:	🚡 l2tp-encap	Layer Two Tunneling Protocol - encapsulation	
(	🚡 l2tp-ipsec	L2TP using IPsec for encryption and authentication	
(	🚡 l2tp-raw	L2TP control and transport, unencrypted	
(	🚡 Idap	Lightweight Directory Access Protocol	
(	🚡 Idaps	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-top	NFS (Network File System) server via TCP	
(	🚡 nfs-udp	NFS (Network File System) server via UDP	
(	nntp	Network News Transfer Protocol	

	Name mercen	Comments	
	🚡 nfs-all	NFS (Network File System) server via TCP/UDP	1
👌 Address Fi 🔇	🚡 nfs-top	NFS (Network File System) server via TCP	
Address	🚡 nfs-udp	NFS (Network File System) server via UDP	
Speci Speci	nntp	Network News Transfer Protocol	
STS Obec	🚡 ntp	Network Time Protocol	
match.	🚡 ping-inbound	Inbound ping (does not allow tracerouting)	
2	🚡 ping-outbound	Outbound ping (also allows traceroute via ICMP)	
2	🚡 рорЗ	Post Office Protocol - Version 3	
Interface:	pptp-ctl	Point-to-Point Tunneling Protocol - control channel	
Network:	🚡 pptp-suite	PPTP control and transport	
Newson.	🚡 radius	Remote Authentication Dial In User Service	
2	🚡 radius-acct	RADIUS Accounting	
👌 Comments 🐧	🚡 rom d	Like rexec, but automatic	
	🚡 rdp	Remote Desktop Protocol	
Comments:	🚡 rexec	Remote Process Execution	
9	🚡 rlogin	Remote login	
2	🚡 rsvp	Reservation Protocol	
2	🚡 smb-all	All MS Windows networking ports	
2	🚡 smtp	Simple Mail Transfer Protocol	
2	🚡 smtp-in	Simple Mail Transfer Protocol with SYN flood protection	
2	🚡 snmp	Simple Network Management Protocol	
2	🚡 snmp-trap	Simple Network Management Protocol traps (alerts)	
2	🚡 ssh	Secure shell	
2	🚡 ssh-in	Secure shell with SYN flood protection	
2	🚡 sun-rpc	Sun/Unix Remote Procedure Call	
2	🚡 syslog	Syslog	
2	🚡 telnet	Teinet	
2	🚡 tftp	Trivial File Transfer Protocol	
5	🚡 time	Legacy time service	
5	🚡 traceroute-udp	Outbound traceroute via UDP	
9	wins	Windows Internet Naming Service	~



match.	cify source interface	and sou	rce network, to	gether with	ı destin
	Source		Destinatio	n	
Interface:	(None)	*	(None)		~
Network:	Name	Comr	nents		~
	📷 any				
	core 📷				
) Commen	🕻 🏢 dmz				
Comments:	🌉 lan				
	🌉 wan1				
	🌉 wan2				
🛃 Spec	ify source interface a	nd sourc	e network, tog	ether with	destina
Spec match.	ify source interface a Source	nd sourc	e network, tog Destination	ether with a	destina
<u>So</u>		nd sourc		ether with a	destin <i>a</i>
match.	Source	nd sourc	Destination	ether with	destina V
match. Interface:	Source (None)	*	Destination (None)	ether with	destina V
match. Interface: Network:	Source (None) (None) Name	*	Destination (None) (None)	eth er with	destinat
match. Interface: Network: Comment	Source (None) (None) Name	*	Destination (None) (None) dress		destina V
match. Interface: Network:	Source (None) (None) Name all-nets	*	Destination (None) (None) dress 0.0.0.0/0	).254	v v
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip	*	Destination (None) (None) dress 0.0.0.0/0 172.17.100	1.254 1.0/24	v v
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet	*	Destination (None) (None) dress 0.0.0.0/0 172.17.100 172.17.100	1.254 1.0/24	destina V
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dmznet	*	Destination (None) (None) dress 0.0.0.0/0 172.17.100 172.129.64	0.254 0.0/24 1.198	destina V
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dmsserver1_ip dnsserver2_ip	*	Destination (None) (None) dress 0.0.0.0/0 172.17.100 202.129.64 4.2.2.2	0.254 0.0/24 4.198 1	destina V
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dnsserver1_ip dnsserver2_ip lan_ip	× × Ad	Destination (None) (None) dress 0.0.0.0/0 172.17.100 202.129.64 4.2.2.2 192.168.1.	1.254 1.0/24 4.198 1 0/24	destina V
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dnsserver1_ip alserver2_ip lan_ip lannet	× × Ad	Destination (None) (None) dress 0.0.0.0/0 172.17.100 202.129.64 4.2.2.2 192.168.1. 192.168.1.	0.254 0.0/24 0.198 1 0/24 09.65	destina V
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dnsserver1_ip lan_ip lan_ip wan1_defaultg	× × Ad	Destination (None) (None) dress 0.0.0.0/0 172.17.100 172.17.100 202.129.64 4.2.2.2 192.168.1. 192.168.1. 202.129.10	0.254 0.0/24 4.198 1 0/24 19.65 19.82	destina
match. Interface: Network: Comment	Source (None) (None) Name all-nets dmz_ip dmznet dnsserver1_ip lan_ip lan_ip lan_net wan1_defaultg wan1_ip	× × Ad	Destination (None) (None) dress 0.0.0.0/0 172.17.100 202.129.64 4.2.2.2 192.168.1. 192.168.1. 202.129.10 202.129.10	0.254 0.0/24 4.198 1 0/24 19.65 19.82 19.82	destina V

Untitled		
General Log Settings NAT SAT SAT Server		
) General		L,
Select log receiver(s) and severity to enable log Enable logging: Severity: Notice	.ct.	
Log to:		
All receivers		
C Specific receiver(s):		
Available Selected		
	ОК	Cance

Enable logging:  Severity: Notice  Debug	
Debug	
Log Receivers Info	
Log to: Wasting	
Warning	
Spe Critical	
Available Alert	
MemLog gency	

Gene	eral Cog Setting: eneral	S NAT SAT	SAT Server	Load Balancing				5
00	Use Interface Ad Specify Sender /	10110						
	New IP Address:	(None)	~					
							ОК	ancel

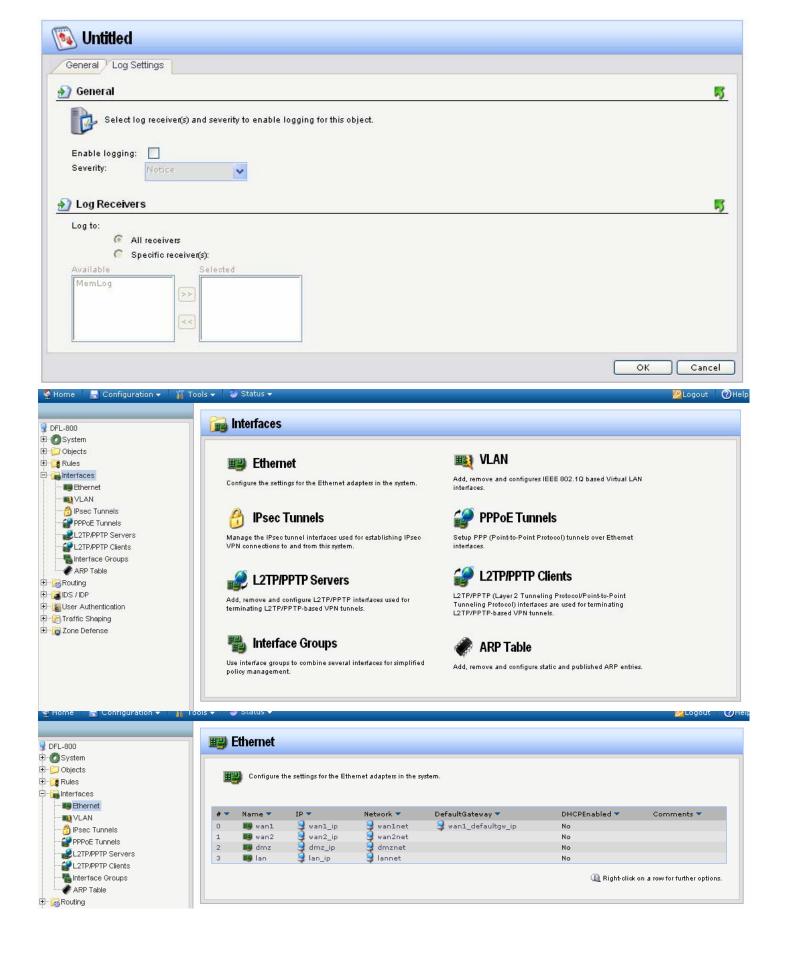
General Log Settings	NAT SA	T SAT Ser	ver Load	d Balanci	ing									
General														
Translate the C Source IP A C Destination														
To:														
New IP Address: New Port:	(None)	*												
gaps		👌 This value	nay only	y be appli	lied on T	CP/UDP	services (	with port:	set to eitl	ner a singl	e port nu	mber or a	port range	e without
All-to-One Mappi	na: rewrite all	lectination IP	s to a sin	ale IP										

General Log Settings NAT SAT SAT Server Load Balancing	
) General	<u>ज</u>
Server Addresses:     Available     Selected       Ian_ip dmz_ip wan2_ip wan2_ip wan2_ip dnsserver1_ip     Image: Selected       Monitoring	5
Monitoring using ICMP Ping packets: Use Shared IP: Ping Interval: 10000 milliseconds Ping Max Loss: Monitoring using TCP packets: Use Shared IP: TCP Interval: 10000 milliseconds TCP Max Loss: TCP Ports: 0-65535 Distribution	
Method: © Round Robin © Connection Rate Window Time: 10 seconds ) Stickiness	5
Stickiness:     None       Idle Timeout:     30 seconds       Max Slots:     2048       Net Size:     24	
	OK Cancel

	An ID Dula falder ann ha	used to an	un IP Pular into Iogia	al around for hottor o	verview and simplified mana	asmost	
ן ק	- <b>8</b> ∖dd <del>-</del>	u.c.t.o.g.		u goop in one o			ings for this folder
# 👻	Name 🔻	Action 🔻	SourceInterface 🔻	SourceNetwork 🔻	DestinationInterface 🔻	DestinationNetwork 🔻	Service 🔻
)	💈 drop_smb-all	Drop	lan	lannet	wan1	all-nets	smb-all
L.	allow_ping-outbound	NAT	lan	lannet	wan1	all-nets	ping-outbound
	8 allow_ftp-	NAT	lan	lannet	wan1	all-nets	ftp- passthrough
2	passthrough						

🔞 Acce	ess					
Add <del>•</del>	Rule					
		Action -	incrisce -	HELIOIR -	Right-click on a row for	r further optior
	→ bbA	Add -	Add ▼	1 Add ▼ S Access Rule	The Add ▼	Add ▼ Add ▼ Access Rule # Name ★ Action ★ Interface ★ Network ★ Comments ★

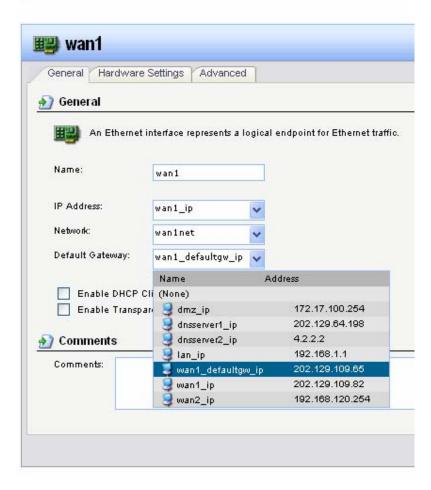
실 Untitle	ed						
General Lo	og Settings						
) General							
	an access rule to al	low or block specifi	r source IP addresses	on a specific interface	8		
103e	an access fulle to a	row of brook specifi	coulde in addresses	on a specific intenace	•		
Name:	Untitled						
Action:	Drop	~					
Interface:	(None)	~					
Network:	(None)	~					
	1	10000					
) Commen	ts						
Comments:							
					5.11		
						_	OK Canc



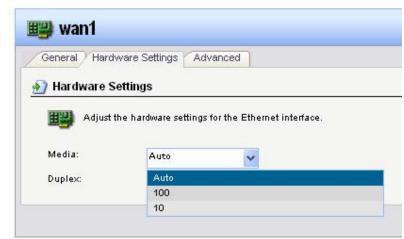
🕮 wan1								
General Hardware	e Settings Advanced	1						
🛃 General	10							5
🕮 An Ethernet	t interface represents a l	ogical end	point for Ef	thernet traffic.				
Name:	wan1							
IP Address:	wan1_ip	~						
Network:	wan1net	~						
Default Gateway:	wan1_defaultgw_ip	*						
Enable DHCP	Client							
Enable Transp	arent Mode							
🛃 Comments						 		5
Comments:								
							ок	Cancel
						19		

) General				
ocheral				
H Ethernet in	terface represents a logic	al endpoint for Ethernet		
Name:		1		
Hame.	wan1			
IP Address:				
IF Addless.	wan1_ip 💙			
Network:	Name	Address		
	🧕 dmz_ip	172.17.100.254		
2	aurz-ib			
Default Gateway:	dnsserver1_ip	202.129.64.198		
Default Gateway:				
	dnsserver1_ip dnsserver2_ip	202.129.64.198		
Enable DHCP Cli	dnsserver1_ip dnsserver2_ip lan_ip	202.129.64.198 4.2.2.2 192.168.1.1		
	dnsserver1_ip dnsserver2_ip lan_ip	202.129.64.198 4.2.2.2 192.168.1.1		

General	nterface represents a logica	
An Ethernet i	nterface represents a logica	
		Il endpoint for Ethernet
Name:	wan1	
IP Address:	wan1_ip 🗸	
Network:	waninet 🗸	
Default Gateway:	Name )	Address
	🤤 all-nets	0.0.0.0/0
Enable DHCP C	🧧 😏 dmz_ip	172.17.100.254
	dmznet	172.17.100.0/24
Enable Transpa	🖞 🧕 dnsserver1_ip	202.129.64.198
	🧕 dnsserver2_ip	4.2.2.2
Comments	🧕 😏 lan_ip	192.168.1.1
Comments:	🧕 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
		192,168,120,254
	🔡 wan2_ip	182.100.120.204



🕮 wan1			
General Hard	dware Settings	anced	
釣 Hardware S	Settings		<b>N</b>
🕮 Adjust	the hardware settings	or the Ethernet interface.	
Media:	Auto	~	
Duplex:	Auto	~	
			OK Cancel



Seneral Hard	ware Settings Ad	vanced	
Hardware S	ettings		
		······ · ·····························	
📺 Adjust f	the hardware settings	for the Ethernet interface	
Media:	the hardware settings Auto	for the Ethernet interface	

👺 wan1	
General Hardware Settings Advanced	
Automatic Route Creation	
Automatically add commonly used routes related to this interface	
<ul> <li>Add route for interface network</li> <li>Add default route if default gateway is specified</li> </ul>	
Route Metric: 100	
	ОК Са

	<b>III VLAN</b>						
00							
/stem ojects							
iles	🔛 Add, reme	ove and configures IEI	EE 802.1Q based Virt	ual LAN interfa	ices.		
erfaces							
Ethernet	🗧 🎦 Add 🗸						
VLAN	NU VLAN						
IPsec Tunnels	# 🔻 Name 🔻	Ethernet 🔻	VLANID 🔻	IP 💌	Network 🔻	DefaultGateway 🔻	Comments 🔻
PPPoE Tunnels						(D	t-click on a row for further opt
L2TP/PPTP Servers						Call Righ	n-click on a row for further opt
L2TP/PPTP Clients							🍌 Modify advanced setti
Interface Groups	4						
ARP Table							
ام التقاريل							
Untitled 👔							
General Advanced							
Selleral Auvaliceu							
General							
) General							
Name:	a fore a systematic						
Name:	Untitled						
Name: Interface:	Untitled (None)	~					
Interface:	(None)	~					
	and the second s	~					
Interface:	(None)	¥					
Interface: VLAN ID: ) Address Settings	(None)						
Interface: VLAN ID: Address Settings IP Address:	(None)	•					
Interface: VLAN ID: ) Address Settings	(None)						
Interface: VLAN ID: Address Settings IP Address: Network:	(None) 0 (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address:	(None) 0 (None)	×					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway:	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network:	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transpare	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transpared	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transpared	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transparer Comments	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transparer Comments	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transpare Comments	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transparer Comments	(None) 0 (None) (None) (None)	<b>v</b>					
Interface: VLAN ID: Address Settings IP Address: Network: Default Gateway: Enable Transparer Comments	(None) 0 (None) (None) (None)	<b>v</b>					OK Can

🛐 Untitled		
General Advanced		
Automatic Route	Creation	5
Automatically add co	mmonly used routes related to this interface	
Add route for in		
	te if default gateway is specified	
Route Metric:	100	
		OK Cancel
me 🛛 🚽 Configuration	🗸 🎢 Tools 🗸 🚽 🥹 Status 🗸	😕 Logout 🛛
-800	👸 IPsec Tunnels	
System Objects		
Rules Interfaces	Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.	
🖷 Ethernet	Add -	
💐 VLAN 😚 IPsec Tunnels	👩 IPsec Tunnel # 🔻 Name 🔻 LocalNetwork 🔻 RemoteNetwork 🔻 RemoteEndpoint 👻	AuthMethod 🔻 Comments 🔻
PPPoE Tunnels 212TP/PPTP Servers		(1) Right-click on a row for further options.
L2TP/PPTP Clients		🐝 Modify advanced settings
🐁 Interface Groups 🖋 ARP Table		
An IPsec tun	nel 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		孯
IKE Algorithms:	(None)	
IKE Life Time	0 seconds	
IPsec Algorithms:	(None)	
IPsec Life Time	0 seconds	
IPsec Life Time	0 kilobytes	
🛐 Comments		5
Comments:		
		OK Cancel

(None)	*					
(None)	*					
Available		Selected				
AdminCert						
	>>					
	<<					
(None)	*					
	(None) Available AdminCert	(None)	(None)	(None)	(None)	(None) Available Selected AdminCert

KE X			tication (XAuth)	Routing	IKE Settings	Keep-alive	Advanced	
	rann -							
🖲 of	f							
C Re	quire IKE XAuth u	ser authentication f	or inbound IPsect	unnels				
C Pa	ass username and p	assword to peer via	IKE XAuth, if the	remote gat	teway requires i	£.		
	Username:	-						
	Password:							
	Confirm Password	1:						

General	Authentication	Extended A	Authentication (XA	uth) Routing	IKE Settings	Keep-alive	Advanced	
) Automa	atic Routing							
	w DHCP over IPSe amically add route			tunnel is estab	lished			
Packet	Sizes							
Specify th	e size at which to	1	aintext packets (rat	her than fragme	nting IPsec).			
	e size at which to	1	aintext packets (rat	her than fragme	nting IPsec).			
Specify th	e size at which to MTU: 1424	1	aintext packets (rat	her than fragme	nting IPsec).			
Specify th Plaintext	e size at which to MTU: 1424	]	22	her than fragme	nting IPsec).			
Specify th Plaintext ) IP Addr IP address • Auto	e size at which to MTU: 1424 resses s to use as source omatically pick the	IP of the tuni	nel					
Specify th Plaintext IP Addr IP address IP address IP address IP address IP address	e size at which to MTU: 1424 Iesses s to use as source	IP of the tuni	nel					 

General Authentication	Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced	
) ike		
C Aggressive		
Perfect Forward Se		
PFS None	DH Group	
7 Security Association		
Per Net     Compatibility Flags	°er Host	
Do not verify paddir	a	
) NAT Traversal	·	
<ul> <li>○ Off</li> <li>○ On if supported and</li> <li>○ On if supported</li> </ul>	NATed	
		OK Canc
Untitled		
General Authentication	Extended Authentication (XAuth) Routing IKE Settings Keep-alive Advanced	
Keep-alive		1
IPseckeep-alives makes s	ire that an IPsec tunnel stays established at all times by continuosly sending ICMP pings through the tun ill only work on LAN to LAN tunnels, i.e. where the remote gateway is a single IP address.	
Disabled		
C Auto		
Manually configured Source IP Address:	IP addresses (None)	
Destination IP Addre		

General	Authentication	Extended Authentication (XAuth)	Routing	IKE Settings	Keep-alive	Advanced	
🛃 Auton	natic Route Cre	ation					<b>5</b>
Automat	tically add route fo	or remote network.					
🗹 Ad	d route for remote	network					
Route M	letric:	90					
							OK Cancel

🔮 Home 👘 🚽 Configuration 👻	🔻 🌃 Tools 👻 🥹 Status 👻	🖉 Logout 🛛 🕜 He
🚽 DFL-800	PPPoE Tunnels	
🗈 👩 System		
⊞∽ <mark>C</mark> i Objects ∄∽ <mark>Cis</mark> Rules	Setup PPP (Point-to-Point Protocol) tunnels over Ethernet interfaces.	
⊡‴ <b>ig</b> Rules ⊟‴ <b>ig</b> Interfaces		
Ethernet	P Add 🗸	
	PPPoE Tunnel	
- 👸 IPsec Tunnels	# 🔻 Name 🔻 EthernetInterface 👻 Network 🗶 ServiceName 💌 Username 💌 DialOnDemand	<ul> <li>Comments</li> </ul>
PPPoE Tunnels	D Biakt al	ck on a row for further options.
L2TP/PPTP Servers	angerer angere	at on a low for failurer ophons.
L2TP/PPTP Clients		
ARP Table		
E Parting		
🔐 Untitled		
General Authenticati	ation Dial-on-demand Advanced	
🔊 General		5
A PPPoE inte	erface is a PPP (point-to-point protocol) tunnel over an existing physical Ethernet interface. Its IP address is dynamical	ly assigned.
Name:	Untitled	
Physical Interface:	(None)	
Remote Network:	(None)	
Service Name:		
Authentication		<u>5</u>
Username:		
Password:		
Confirm Password:		
Comments		5
Comments:		1.5
		OK Cancel
🏈 Untitled		
General Authenticati	tion Dial-on-demand Advanced	
Authentication		<u> </u>
Allow No Authen	ntication	
🔽 Unencrypted Pas	assword (PAP)	
Challenge Hands	dshake Authentication Protocol (CHAP)	
Mircosoft CHAP (	(MS-CHAP)	
Microsoft CHAP \	Version 2 (MS-CHAP v2)	
		OK Cancel

😭 Untitled	
General Authentication Dial-on-demand Advanced	
🛃 Dial-on-demand	<b>5</b>
Enable dial-on-demand to delay connection until traffic is sent on the interface. Idle tir in activity.	neout specifies the time to wait before disconnecting due to
Enable Dial-on-demand	
Activity Sensing: BiDirectional	
Idle Timeout: 3600 seconds	
	OK Cancel

🚅 Untitled							
General Authentication	Dial-on-demand Adv	anced					
🔬 Automatic Route Cre	ation						5
Automatically add route fo	or remote network.						
Add route for remote	: network						
Route Metric:	90						
						C	OK Cancel
Home 💂 Configuration 🗸	🌃 Tools 👻 🌍 Status 🗸						💋 Logout
DFL-800	L2TP/PPT	^o Servers					
Ø∫System ⊃Objects	6						
🚦 Rules	Add, remov	ve and configure L2TP/PPTP i	nterfaces used	for terminating L2T	P/PPTP-based VP	N tunnels.	
Interfaces	🔶 Add 🗸						
VLAN	L2TP/PPTP Serv	er TunnelProtocol 🔻	IP 💌	Interface 🔻	IPPool 🔻	UseUserAuth 🔻	Comments 🔻
Prec Tunnels     PPPoE Tunnels	# Name •		The c	Interface •	199001		
L2TP/PPTP Servers							ick on a row for further options. ¾ Modify advanced settings
ARP Table							

E 😹 Routing

🤗 Untitled						
General PPP Parameter	s Add Route					
🛐 General						
A PPTP/L2TP se	ver interface term	inates PPP (Point	t to Point Protocol) tun	nels set up over existir	g IP networks.	
Name:	Untitled	N				
Inner IP Address:	(None)	~				
Tunnel Protocol:	PPTP	~				
Outer Interface Filter:	(None)	~				
Server IP:	(None)	*				
) Comments						
Comments:						
						OK Canc
						OK Canc
) Untitled						OK Cano
	s Add Route					OK Canc
General PPP Parameter	s Add Route					
General ) PPP Parameter ) General						
General PPP Parameter			and the encryption str	engths allowed. Also sp	ecify the IP address ass	
General PPP Parameter General General Specify if User A server informatic	uthentication Rule n to hand out to c		and the encryption str	engths allowed. Also s	ecify the IP address ass	
General PPP Parameter General Specify if User A server informatic Use User Authentica	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also sj	recify the IP address ass	
General PPP Parameter General General Specify if User A server informatic	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also s	ecify the IP address ass	
General PPP Parameter General Specify if User A server information Use User Authentica Microsoft Point-to-P None	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also sj	ecify the IP address ass	ignment and the DNSAVINS
General PPP Parameter General Specify if User A server information Use User Authentica Microsoft Point-to-P None RC4 40 bit	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also s	ecify the IP address ass	ignment and the DNSAVINS
General PPP Parameter General Specify if User A server information Use User Authentica Microsoft Point-to-P None RC4 40 bit RC4 56 bit	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also s	ecify the IP address ass	ignment and the DNSAWINS
General PPP Parameter General Specify if User A server information Use User Authentica Microsoft Point-to-P None RC4 40 bit RC4 56 bit RC4 128 bit	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also s	recify the IP address ass	ignment and the DNSAWINS
General PPP Parameter General Specify if User A server information Use User Authention Microsoft Point-to-P None RC4 40 bit RC4 56 bit RC4 128 bit IP Pool	uthentication Rule n to hand out to c tion Rules D <b>int Encryption</b>	onneced clients.	and the encryption str	engths allowed. Also s	ecify the IP address ass	ignment and the DNSAWINS
General PPP Parameter General Specify if User A server informatic Use User Authentica Microsoft Point-to-P None RC4 40 bit RC4 56 bit RC4 128 bit	uthentication Rulo n to hand out to c tion Rules	onneced clients.	and the encryption str	engths allowed. Also s	recify the IP address ass	ignment and the DNSAWINS
General PPP Parameter General Specify if User A server informatic Use User Authentica Microsoft Point-to-P None RC4 40 bit RC4 56 bit RC4 128 bit IP Pool IP Pool: (None)	uthentication Rule n to hand out to c tion Rules D <b>int Encryption</b>	onneced clients.	and the encryption str	engths allowed. Also s	ecify the IP address ass	ignment and the DNSAWINS
General PPP Parameter General Specify if User A server information Use User Authention Microsoft Point-to-P None RC4 40 bit RC4 56 bit RC4 128 bit IP Pool	uthentication Rule n to hand out to c tion Rules D <b>int Encryption</b>	onneced clients.	and the encryption str	engths allowed. Also s	recify the IP address ass	ignment and the DNSAWINS

ок

Cancel

eneral PPP Parameters	YAdd Route				
Filter					5
Restricts networks fo	or which routes may automa	ically be added.			
Allowed Networks: all-r	nets 💌				
Proxy ARP					
Walls:					
dmz Ian Untitled Untitled	erfaces, including new ones.			OK Can	cel
dmz Ian Untitled Untitled Intitled Intitled Intitled				OK Can	

RemoteNetwork 👻 Username 💌 DialOnDemand 👻 Comments 💌

1 Right-click on a row for further options.

- NLAN PPPoE Tunnels

L2TP/PPTP Servers

ARP Table 

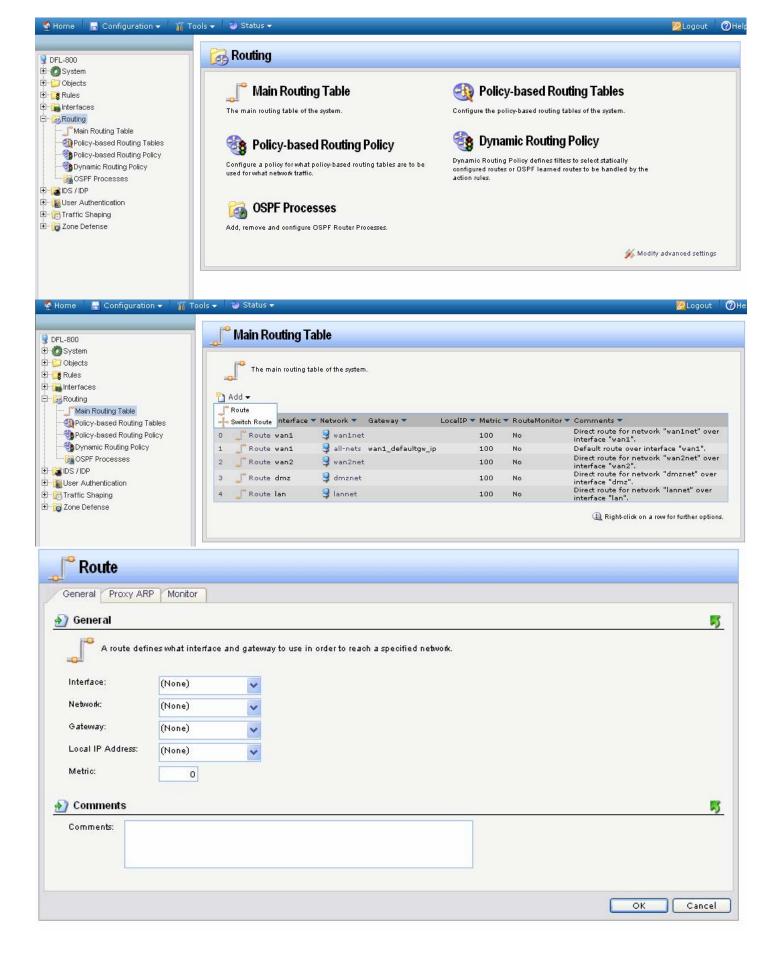
L2TP/PPTP Client
 # 
 Name 
 TunnelProtocol 
 RemoteEndpoint

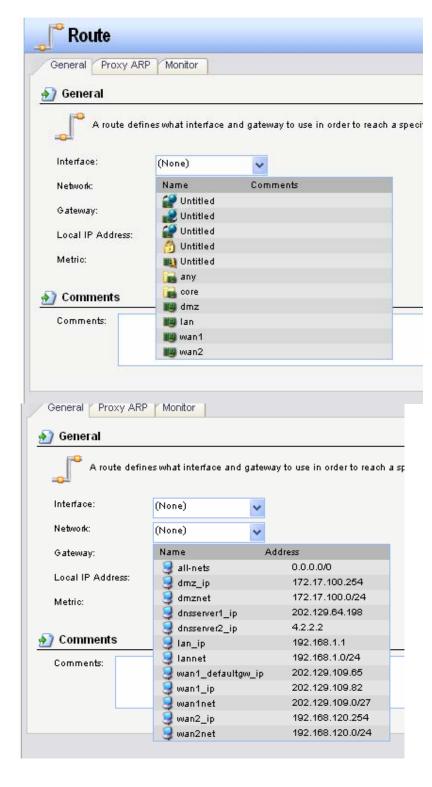
General Security D	al-on-demand Advance	ed		
) General				
A PPTP/L2TP of assigned.	lient interface is a PPP (I	°oint-to-Point Protocol) tunn	el over an existing IP network. Its IP address a	and DNS servers are dynamically
Name:	Untitled			
Tunnel Protocol:	PPTP	~		
Remote Endpoint:	(None)	*		
Remote Network:	(None)	~		
Authentication				
Username:				
Password:				
Confirm Password:				
7 Comments				
Comments				1
Comments				
·				
Comments:				
Comments:	al-on-demand Advance	ed		
Comments: Untitled General Security D	al-on-demand Advanc	ed		OK Canc
Comments: Untitled General Security D Authentication		ed		OK Canc
Comments: Untitled General Security Di Authentication	cation	ed		OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw	cation			OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw Challenge Handsh Microsoft CHAP (M	cation vord (PAP) ake Authentication Proto S-CHAP)			OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw Challenge Handsh Microsoft CHAP (M	cation vord (PAP) ake Authentication Proto			OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw Challenge Handsh Challenge Handsh Microsoft CHAP (M Microsoft CHAP Ve	cation vord (PAP) ake Authentication Proto S-CHAP)	901 (CHAP)		
Comments: Untitled General Security D Authentication Allow No Authentic Unencrypted Passw Challenge Handsh Microsoft CHAP (M Microsoft CHAP Vecon	cation vord (PAP) ake Authentication Proto S-CHAP) rision 2 (MS-CHAP v2)	901 (CHAP)		OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw Challenge Handsh Challenge Handsh Microsoft CHAP (M Microsoft CHAP Ve	cation vord (PAP) ake Authentication Proto S-CHAP) rision 2 (MS-CHAP v2)	901 (CHAP)		OK Canc
Comments: Untitled General Security D Authentication Allow No Authenti Unencrypted Passw Challenge Handsh Microsoft CHAP (M Microsoft CHAP (M Microsoft Point-to- Microsoft Point-to-	cation vord (PAP) ake Authentication Proto S-CHAP) rision 2 (MS-CHAP v2)	901 (CHAP)		OK Canc

P Untitled	
General Security Dial-on-demand Advanced	
🧿 General	
Enable Dial-on-demand	
Enable Dial-on-demand	
Activity Sensing: BiDirectional  Idle Timeout: 3600 seconds	
	OK Cance
P Untitled	
General Security Dial-on-demand Advanced	
General       Security       Dial-on-demand       Advanced         Automatic Route Creation         Automatically add route for remote network.	
General       Security       Dial-on-demand       Advanced         Automatic Route Creation         Automatically add route for remote network.         Image: Creation of the second	
General       Security       Dial-on-demand       Advanced         Automatic Route Creation       Automatically add route for remote network.	

💁 Home 🛛 🔒 Configuration 👻 🗌	🌃 Tools 👻 🔮 Status 👻	🖉 Logout 🔞 H
DFL-800	Interface Groups	
E OSystem		
Ð Öjects ∃- <mark>⊈</mark> Rules	Use interface groups to combine several interfaces for simplified policy	/ management.
⊐ <b></b> Interfaces		
B Ethernet	Add 🗸	
	Sinterface Group	
👸 IPsec Tunnels	# 🔹 Name 💌 Members 💌	Comments 🔻
PPPoE Tunnels		(1) Right-click on a row for further options.
L2TP/PPTP Servers		Cag regimenta on a room of returner options.
L2TP/PPTP Clients		
HEREN		
The Untitled		
		_
魡 General		<b>5</b>
ment		
Use an interface g	group to combine several interfaces for a simplified security policy.	
Name: Untitle		
Name: Untitle	d	
🖌 Se	curity/Transport Equivalent	
🎻 Interfaces		<b>5</b>
	2220000	and the second
Available	Selected	
wan1 wan2 dmz lan		
dmz		
lan 🤤	0	
Untitled	<<	
Untitled		
Comments		15 日
Comments:		
		OK Cancel

	1000						🖉 Logout 🕜
OFL-800 OgSystem	A rest	RP Table					
Dijects				-1-1			
<b>8</b> Rules		Add, remove and configure :	static and published ARP e	ntries.			
interfaces	bbA 🐴	•					
- NI VLAN	ARF	° Entry					
- 👸 IPsec Tunnels 	# -	Mode 🔻 🛛 In	terface 🔻	IP 🔻 MAG	CAddress 🔻	Comments	•
L2TP/PPTP Serve	ers					(1) Right-click on a	row for further options.
L2TP/PPTP Clients						🍌 Мо	dify advanced settings
ARP Table							
🎻 ARP Ent	ay						
🔊 General							5
Use an .	ARP entry to publish addition	al IP addresses and/or M	AC addresses on a sp	ecified interface.			
Mode: p	Publish						
Interface: (f	None) 💙						
IP Address: (†	None) 🔽						
MAC: 0	0-00-00-00-00-00						
Comments							5
Comments:							
						ОК	Cancel
			Use a	n ARP entry to pu	blish additional IP	addresses and/or M.	
			₩qr'		blish additional IP	addresses and/or M.	
			Mode:	n ARP entry to pu Publish	blish additional IP .	addresses and/or M.	
			₩qr'			addresses and/or M.	
			Mode:	Publish		addresses and/or M.	
			Mode: Interface: IP Address:	Publish (None)	<b>*</b>	addresses and/or M.	
			Mode: Interface:	Publish (None) Name Untitled	<b>*</b>	addresses and/or M.	
			Mode: Interface: IP Address: MAC:	Publish (None) Name Untitled Untitled Untitled	<b>*</b>	addresses and/or M.	
Use an AF	RP entry to publish additional	IP addresses and/or M;	Mode: Interface: IP Address:	Publish (None) Name Untitled Untitled Untitled Untitled	<b>*</b>	addresses and/or M.	
Use an AF	RP entry to publish additional	IP addresses and/or M/	Mode: Interface: IP Address: MAC:	Publish (None) Name Untitled Untitled Untitled	<b>*</b>	addresses and/or M.	
<b>V</b> \$7'	RP entry to publish additional blish	IP addresses and/or M.	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled	<b>*</b>	addresses and/or M.	
Mode: Pub		IP addresses and/or M/	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Suntitled Core	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: Sta	blish 💌 atic ublish	IP addresses and/or M;	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: Stu IP Address: XP	blish 🗸	IP addresses and/or M/	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Suntitled Core	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: Stu IP Address: XP	blish 💌 atic ublish	IP addresses and/or M,	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: Stu IP Address: XP	blish 🗸	IP addresses and/or M.	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00-	blish v atic ublish Publish -00-00-00-00 v	IP addresses and/or M/	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	<b>*</b>	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00- Mode:	blish v atic ublish Publish -00-00-00-00 v Publish	IP addresses and/or M.	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	*	addresses and/or M.	
Mode: Pub Interface: Sta IP Address: XP MAC: 00- Mode: Interface:	blish v tatic ublish -00-00-00-00 v Publish (None) (None)		Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	*	addresses and/or M.	
Mode: Pub Interface: Sta IP Address: XP MAC: 00- Mode: Interface: IP Address:	blish v tatic ublish -00-00-00-00 v Publish (None) (None)	× ×	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	*	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00- Mode: Interface: IP Address: MAC:	blish v tatic ublish Publish -00-00-00-00 v Publish (None) Name dmz_ip dmsserver1_ip	Address 172.17.100.254 202.129.64.198	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitl	*	addresses and/or M.	
Mode: Pub Interface: Sta IP Address: XP MAC: 00- Mode: Interface: IP Address:	blish v tatic ublish Publish -00-00-00-00 v Publish (None) (None) Name dmz_ip dmsserver1_ip dmsserver2_ip	Address 172.17.100.254 202.129.64.198 4.2.2.2	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle U	*	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00- Mode: Interface: IP Address: MAC:	blish v tatic ublish Publish -00-00-00-00 v Publish (None) (None) Name dmz_ip dnsserver1_ip dnsserver2_ip lan_ip	Address 172.17.100.254 202.129.64.198 4.2.2.2 192.168.1.1	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle U	*	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00- Mode: Interface: IP Address: MAC: MAC:	blish v atic ublish Publish -00-00-00-00 v Publish (None) (None) Name dmz_ip dnsserver1_ip dnsserver2_ip lan_ip wan1_defaultgw_ip	Address 172.17.100.254 202.129.64.198 4.2.2.2 192.168.1.1 202.129.109.65	Mode: Interface: IP Address: MAC: <u>MAC:</u>	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle U	*	addresses and/or M.	
Mode: Pub Interface: St. IP Address: XP MAC: 00- Mode: Interface: IP Address: MAC: MAC:	blish v tatic ublish Publish -00-00-00-00 v Publish (None) (None) Name dmz_ip dnsserver1_ip dnsserver2_ip lan_ip	Address 172.17.100.254 202.129.64.198 4.2.2.2 192.168.1.1	Mode: Interface: IP Address: MAC: <u>MAC:</u> Comments:	Publish (None) Name Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitled Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle Untitle U	*	addresses and/or M.	





• • •	dress	Interface: Network: Gateway: Local IP Address:	(None) (None) (None) (None)	▼ ▼ ▼
× × Add	dress	Gateway: Local IP Address:	(None)	~
× × Add	dress	Local IP Address:		~
<mark>∼</mark> Add	dress	Local IP Address:		×
Add	dress		(None)	*
		Metric:	Name	Address
	172.17.100.254		(None)	
ip	202.129.64.198	A Comments	🧕 dmz_ip	172.17.100.254
ip	4.2.2.2		💶 🧕 dnsserver1_ip	202.129.64.198
	192.168.1.1	 Comments:	🧕 dnsserver2_ip	4.2.2.2
ultgw_ip	202.129.109.65		🧕 lan_ip	192.168.1.1
	202.129.109.82		😔 wan1_defaultgw	
	192.168.120.254		— 🧕 wan1_ip	202.129.109.82
	102.100.120.204		🤤 wan2_ip	192.168.120.254
				a wanz_ip

Proxy ARP		
MANAGES IN SECOND DESC	Alex - added	
Interface to ARP publis	the added route on.	
Available	Selected	
wan1 wan2		
dmz		
lan Untitled		
Untitled		
Always select ALL	interfaces, including new ones.	

Route	
General Proxy ARP Monitor	
🔊 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	

🔮 Home 🔰 🛃 Con	nfiguration 👻	🚺 Tools 🗸	🚽 Status 👻					Logout 🕜
		6	Policy-base	ed Routing Tables				
DFL-800 DFL-800			A loney buoc	a notating rabios				
🗄 📁 Objects			Configure the	e policy-based routing tables o	if the most of			
E 🥞 Rules			Configure the	2 policy-based routing tables o	of the system.			
E 🕞 Interfaces			add -					
- GRouting	Toblo		ີ່ Add ▾ ૱ Policy-based Routir	ng Table				
Main Routing			# Vame Vame	Ordering 🔻	RemoveInterface	IPRoutes 🔻	Comments 💌	
Policy-based								
Bynamic Rout	ting Policy						(I) Right-click on a row for fu	rther options.
CSPF Proces	ses							
] 😭 IDS / IDP								
- 👔 User Authenticati - 🕝 Traffic Shaping	1011							
- Tone Defense								
<b>60</b> 11. ea								
🕘 Untitle	ed							
🔬 General								5
A p	olicy-based i	routing table	is used to define a	an alternate routing tab	le.			
-								
Name:	Untitled							
Ordering:	Only							
	Omy		*					
	Rem	ove Interface	IP Routes					
	(make	firewall tota	illy transparent)					
Comment	nts							
Comments:								
	10					25		
							ОК	Cancel
🕘 Untit	fled							
	uvu							
約 Genera	al							
					-			
A 🚯 🔍	policy-base	ed routing t	able is used to d [,]	efine an alternate rou	r			
		Ť						
Name:	Untitl	ed						
Ordering:	Only		*					
ľ			×					
	Defau	ult						
	First							
	Only							
約 Comm	ents							
Comment	<b>B</b> :							

🧐 Home 🛛 🔚 Configurati	on 👻 🎢 Tools 👻	🕘 Stati	JS ▼				💆 Logout 🛛 🕐 H
	a	Dalla	- kasad Dauffun I	) all av			
3 DFL-800		S Polic	y-based Routing I	olicy			
E OSystem							
🗄 📁 Objects		🚱 Co	nfigure a policy for what poli	cv-based routing tabl	es are to be used for what network	traffic.	
E Rules		<b>38</b>		.,			
E Interfaces		add -					
E Routing		Add 🔫	sed Routing Rule				
Main Routing Table			<ul> <li>SourceInterface</li> </ul>	SourceNetwork *	<ul> <li>DestinationInterface </li> </ul>	DestinationNetworl	Service Comments
E - M Policy-based Routing	Tables	Hanne	outernenate	obdicentection	Destinationaliterrate	Destinationnetwon	Comments -
						Œ	Right-click on a row for further options.
OSPF Processes	У						
E-CONTROCCSSCS	3						
E User Authentication							
🗄 👸 Traffic Shaping							
2 Zana Dafanan							
🕰 II.ea. i							
Constituted 🛛 🗞							
🛃 General							<u>5</u>
A Policy-t	based Routing Rule	forces th	e use of policy-based i	outing tables in	the forward and/or return d	lirection of traffic on	a connection. The 'ordering'
parameter of the p	olicy-based routing	table de	termines if the router i	s consulted befo	re or after the main routing	table.	
		5.0920.0990.0				·	
Name:	Untitled	î					
	Untitled						
Forward Table:	(None)	*					
Return Table:	(Marca)	11000					
Retuin rable.	(None)	*					
Service:	(None)	v					
Schedule:	(None)	1710					
	((10112)	*					
🎒 Address Filter	r.						5
-							
Specify se	ource interface and	source no	etwork, together with th	e destination int	erface and destination net	twork. All parameters	have to match for the rule to
3-3						<i>.</i>	
match.							
12.112.12	Source	-	Destination				
Interface:	(None)	*	(None)	*			
Network:	(None)	*	(None)	*			
	No No Control - Cont	-					
O Commente							
Comments							5
Comments:							
-							
							OK Cancel
🔰 🯹 👸 A Policy	r-based Routing R	ule force	s the use of policy-b	ased routing [.]			
	nation based out	tina tabl	. dataminan itita e				
parameter of the	policy-based lod	ung taon	e determines if the r	outer is consu			
			_				
Name:	Untitled						
Forward Table:	(None)	1	,				
Return Table:	Name	Co	mments				
	[®] <main></main>						
Service:	Untitled						
Schedule:	(None)	~	*				

Service:	(None)	*	
Schedule:	Name	Comments	
	😘 НЗ23	H.323 via H323 ALG - Enables H.323 communication	-
👌 Address Filte	Gatekeeper	H.323 RAS via H323 ALG - Enables communication with H.323 Gatekeepers	
-	Shekeeper M Untitled		
Specify s	1.022		
Ser .	Chilled Untitled		
match.	Chilled (Chilled		
	all_icmp	All ICMP services	
	all_services	All ICMP. TCP and UDP services	
Interface:		All TCP services	
Network:	Mail_tep	All TCP and UDP services	
	Mail_tcpudp	All UDP services	
	Mall_udp		
👌 Comments	M bootpc	Bootstrap protocol (also DHCP) client	
	– 🀚 bootps	Bootstrap protocol (also DHCP) server	
Comments:	Chargen	Character generator	
	Ma dns-all	DNS via TCP and UDP	
	M dns-tcp	Domain Name Server via TCP - mainly zone transfers	
	🐚 dns-udp	Domain Name Server via UDP - standard queries	
	Minimizer 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	
🔰 Address Filte	https	Secure HTTP over SSL/TLS	
	🐚 https-in	Secure HTTP over SSL/TLS with SYN flood protection	
🏹 Specifys	° 🦬 ident	Legacy authentication/identification service	
match.	🐚 igmp	Internet Group Management (multicast control)	
	🐚 ike	Internet Key Exchange - key management for IPsec	
	🐚 imap	Interactive Mail Access Protocol v2 and v4	
Interface:	( ipcomp	IP Payload Compression Protocol	
	🐚 ipip-encap	IP-in-IP encapsulation	
Network:	🐚 ipseo-ah	IPsec AH (authenticated only)	
	🐚 ipseo-esp	IPsec ESP (encrypted and authenticated)	
Comments	🐚 ipseo-natt	IPsec NAT-traversal (through udp/4500)	
- commenta	🦬 ipseo-suite	The IPsec+IKE suite	
Comments:	🐚 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	
	🐚 Idap	Lightweight Directory Access Protocol	
	Maps	Secure LDAP over SSL/TLS	
	m Ipr	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-top	NFS (Network File System) server via TCP	V

Return Table:	(None)	×	
Service:	(Nama)		
Selvice.	(None)	<u>×</u>	
Schedule:	Name	Comments	
	Minifs-top	NFS (Network File System) server via TCP	
衸 Address Filter	Manfs-udp	NFS (Network File System) server via UDP	
	🛛 🐚 nntp	Network News Transfer Protocol	
Specify s	Mintp	Network Time Protocol Inbound ping (does not allow tracerouting)	
يعي	⁰ () ping-inbound () ping-outbound	Outbound ping (also allows traceroute via ICMP)	
match.	pop3	Post Office Protocol - Version 3	
	popo pptp-ctl	Point-to-Point Tunneling Protocol - control channel	
Interface:	pptp-suite	PPTP control and transport	
internation.	Tadius	Remote Authentication Dial In User Service	
Network:	Tadius-acct	RADIUS Accounting	
	rem d	Like rexec, but automatic	
🏹 Comments	rdp 🚮	Remote Desktop Protocol	
	- 🦬 rexec	Remote Process Execution	
Comments:	🐚 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)	
	M ssh	Secure shell	
	Ssh-in	Secure shell with SYN flood protection	
	sun-rpc	Sun/Unix Remote Procedure Call	
	Syslog	Syslog Telnet	
	teinet	Trivial File Transfer Protocol	
	Mittp (Mittine)	Legacy time service	
	Traceroute-udp	Outbound traceroute via UDP	
	( wins	Windows Internet Naming Service	
Keturn Ladie:	(None)	-	
	(Home)		
Service:	(None)	~	
Schedule:	(None)		
	(None)	×	
_	Name	Comments	
約 Address Filte	(None)		
	20	All hours, except Monday to Friday 08:00-17:00	
🕺 Specifys	o NonWorkingHours	hation	
match.	Weekdays	Monday to Friday, 00:00-23:59	
		Saturday and Sunday, 00:00-	
	🐺 Weekends		
Interface:	(None)	V (None) V	
Network:	(None)	(None)	
	(Holle)		
-			
約 Comments			
Comments:			

💁 Home 👘 👼 Configuration	👻 🎽 Tools 👻	🥹 Status 👻				💯 Logout (	ОНе
DFL-800		훩 Dynamic Rou	ting Policy				
🗄 🕜 System		<b>v</b> ·					-
E 📁 Objects							
E 🙀 Rules		Dynamic Routir	ng Policy defines filters	to select statically configured	routes or OSPF learned routes to be h	andled by the action rules.	
E 🔒 Interfaces							
3- 😹 Routing		🔁 Add 👻					
Main Routing Table		🐴 Dynamic Routing Rule	2				
E Opicy-based Routing Tak	oles	# 🔹 Name 🔻	From 🔻	OSPFProcess 🔻	RoutingTable 🔻	Comments 💌	
Policy-based Routing Poli						_	
Dynamic Routing Policy						(1) Right-click on a row for further options.	
I- 🚰 IDS / IDP							
🍓 Untitled							
General More Para	meters Log :	Settings					
🔊 General						5	
-							•
A Dynamic F	Routing Policy r	ule creates a filter to	catch statically co	onfigured or OSPF lear	rned routes. The matched rou	es can be controlled by the action	
rules to be either exp	orted to USPF (	processes or to be ac	ided to one or mo	re routing tables.			
2							
Name: Untitl	ed						
From OSPF Pro	ocess: Availabl	•	Selected				
		>	2				
		6	-				
		0	-				
		<	<u> </u>				
0.5 St. 16 Sec. 16							
From Routing 1	able: Availabl	e	Selected				
	Routes						
	Untitle	d	>				
		3	<				
	1						
Destination interface		1000					
Destination intenace	· (None)	~					
Destination Network	work					5	
	96					~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	-
Exactly Matches:	(None)	*					
0.1		1000					
Or is within:	(None)	*					
	As a second s						
約 Comments							
Comments						5	-
Comments:							
						OK Cancel	
							-

🦉 Home 🛛 🚽 Configuration 👻 🁔	Tools 🗸 🛛 🥶 Status 🗸	2Logout 🕐 H
DFL-800 DFL-800 Dobjects Rules Rules Rules Routing Main Routing Table Dobject-based Routing Tables Policy-based Routing Policy Dopamic Routi	General     Metric:     to     OSPF Specific     Router ID:   OSPF Route Type:   OSPF Tag:     to	<u>5</u>
		OK Cancel

			🥞 Untitled		
			General More Para	neters Log Settings	
🍓 Untitled	1		🋃 General		
General More	e Parameters Log Setting	IS	Next Hop: (None)	*	
衸 General			Metric:	to	
	(None)		OSPF Specific		
Metric:	Name Ad (None)	dress	Router ID:	(None) 🗸	
OSPF Spec	😡 dmz in	172.17.100.254	OSPF Route Type:	Name Ad	dress
OSPF Spec	🧕 dnsserver1_ip	202.129.64.198	_	(None)	
Router ID:	🤤 dnsserver2_ip	4.2.2.2	OSPF Tag:	🛃 dmz_ip	172.17.100.254
0005 0	🧕 lan_ip	192.168.1.1		dnsserver1_ip	202.129.64.198
OSPF Route 1	🧕 wan1_defaultgw_ip	202.129.109.65		dnsserver2_ip	4.2.2.2
OSPF Tag:	🧕 wan1_ip	202.129.109.82		lan_ip	192.168.1.1
	🤤 wan2_ip	192.168.120.254		wan1_defaultgw_ip	202.129.109.65
				wan1_ip	202.129.109.82

🍓 Untitled	
General More Par	ameters Log Settings
Seneral	
Next Hop: (Non	e) 🗸
Metric:	to
🔊 OSPF Specific	
Router ID:	(None)
OSPF Route Type:	(None)
OSPF Tag:	1
	2
🍓 Untitled	
	ameters / Log Settings
Seneral	
Select log i	eceiver(s) and severity to enable logging for this object.
Enable logging:	✓
Severity: N	łotice 🔽
I	Debug
Log Receivers	Info Notice
Log to:	Warning
( All	Error
	Critical
Available	Alert
inchized a	jency

Home 🗧 Configuration 👻	🌃 Tools 👻 🥪 Status 🕶		😕 Logout 🛛 🥑
DFL-800	OSPF Processes		
Ø System ➢ Objects ⅔ Rules ☜ Interfaces	Add, remove and configure (	)SPF Router Processes.	
BROUTING ──Main Routing Table	Add →	RouterID 💌	Comments 🔻
Policy-based Routing Tables     Policy-based Routing Policy     Donanic Routing Policy     OSPF Processes     DS / IDP     User Authentication	# Vame Vame V	KoutenD *	Comments •
🗞 Untitled			
	ntication Advanced Log Settings		_
約 General			<u> </u>
Router ID: (None) Reference Bandwidth: RFC 1583 Compatibil	1 Gbps 💙		<b>1</b>
Comments:			
			OK Cancel
🌏 Untitled			
General Debug Authen	tication Advanced Log Settings	Thitled	
🛃 General		General Debug Authentication	Advanced Log Settings
	ocess defines a group of routers exchangir		ines a group of routers exchanging routing information via th
Name: Untitled			

Name:

Router ID:

Comments

Comments:

Reference Bandwidth:

Router ID:

Reference Ba (None)

RFC 158

Comments

Comments:

(None)

Name

4

dmz_ip dnsserver1_ip dnsserver2_ip

wan1_defaultgw_ip

lan_ip

🧕 wan1_ip 🧕 wan2_ip ¥

Address

172.17.100.254

202.129.64.198

202.129.109.65

202.129.109.82

192.168.120.254

192.168.1.1

4.2.2.2

Untitled

(None)

RFC 1583 Compatibility Mode

~

1 Gbps

bps

Kbps

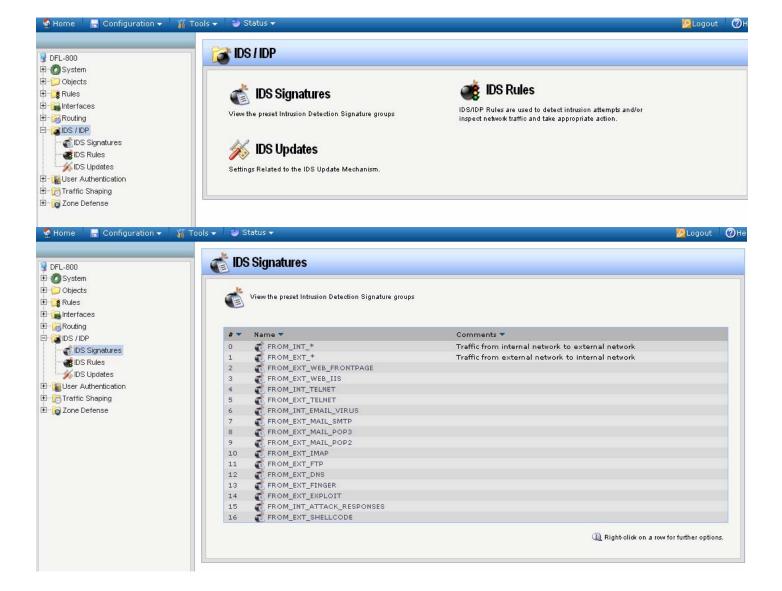
Mbps Gbps *

neral / Debug / Authentic	ation Advanced	Log Settings
	1	
General		
🗿 To assist in troublesho	oting routing proble	ms, log messag
General:	Off	~
Hello Packets:	Off	~
Database Description Packets:	Off	~
	Off	~
Exchange Packets:		
Exchange Packets: Internal LSA Logic:	Off	*
	off Off	*

## General Debug Authentication Advanced Log Settings 艩 General -To assist in troubleshooting routing problems, log messages may be generated General: Off Y Hello Packets: Low Database Description Packets: Medium High Exchange Packets: Internal LSA Logic: Off SPF Calculations: Off Routing Table Manipulation: Off

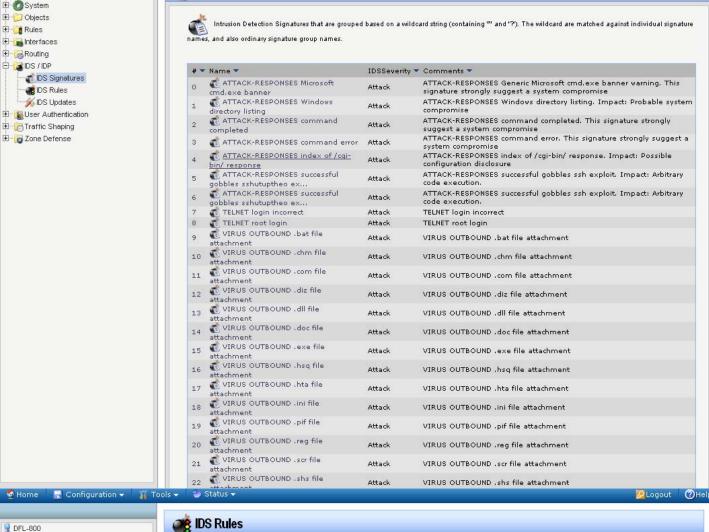
General	Debug Authentic	ation Advanced	Log Settings	
🟹 Gener	al			
-			NA 1011 81 82 93	
	All OSPF protocol ex/	changes can be authe	nticated via s simple passv	word or cryptograhp
100				
• No				
	(null) Authentication sphrase			
	(null) Authentication	1		
C Pas	(null) Authentication	]		
C Pas	(null) Authentication sphrase	]		

General	Debug A	uthentication Advanced Log Settings
) Time	Settings	
SPE Ho	ld Time:	
	lay Time:	10 Seconds
	oup Placing:	5 Seconds
	Holdtime:	10 Seconds
) Memo	огу	
Max RA	M usage for pi	rocess:
		Kilobytes
	r specified, th	e live database for each Router Process may use up to 1% of total RAM.
	n specified, th	e live database for each Router Process may use up to 1% of total RAM.
	n specineu, m	e live database for each Router Process may use up to 1% of total RAM.
	n speanea, th	e live database for each Router Process may use up to 1% of total RAM.
		e live database for each Router Process may use up to 1% of total RAM.
Dunt 👌	itled	
Dunt 👌	itled	e live database for each Router Process may use up to 1% of total RAM.
	itled Debug A	
General General	<b>itled</b> Debug A ral	uthentication Advanced Log Settings
General General	<b>itled</b> Debug A ral	
General General General Enable	<b>ittlect</b> Debug A ral Select log rec logging:	uthentication Advanced Log Settings reiver(s) and severity to enable logging for this object.
General General	<b>ittlect</b> Debug A ral Select log rec logging:	uthentication Advanced Log Settings
General General General Ceneral Ceneral Ceneral Severity	<b>ittlect</b> Debug A ral Select log rec logging:	uthentication Advanced Log Settings reiver(s) and severity to enable logging for this object.
General General General Ceneral Ceneral Ceneral Severity	ittlect Debug A ral Select log rec logging: r: No ecceivers	uthentication Advanced Log Settings reiver(s) and severity to enable logging for this object.
General General General General Control General Severity Severity	ittlect Debug A ral Select log rec logging: r: ro ecceivers	uthentication Advanced Log Settings reiver(s) and severity to enable logging for this object.
General General General General Control General Severity Severity	ittlect Debug A ral Select log rec logging: r: Ro ecceivers	uthentication Advanced Log Settings reiver(s) and severity to enable logging for this object.
General General General Content General Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Content Conten	ittlect Debug A ral Select log rec logging: c No ecceivers ecceivers	elivers receiver(s) and severity to enable logging for this object.
General General General Coston Severity Log to: Availab	ittlect Debug A ral Select log rec logging: c No ecceivers ecceivers	uthentication Advanced Log Settings eviver(s) and severity to enable logging for this object.



💡 DFL-800

## FROM_INT_*



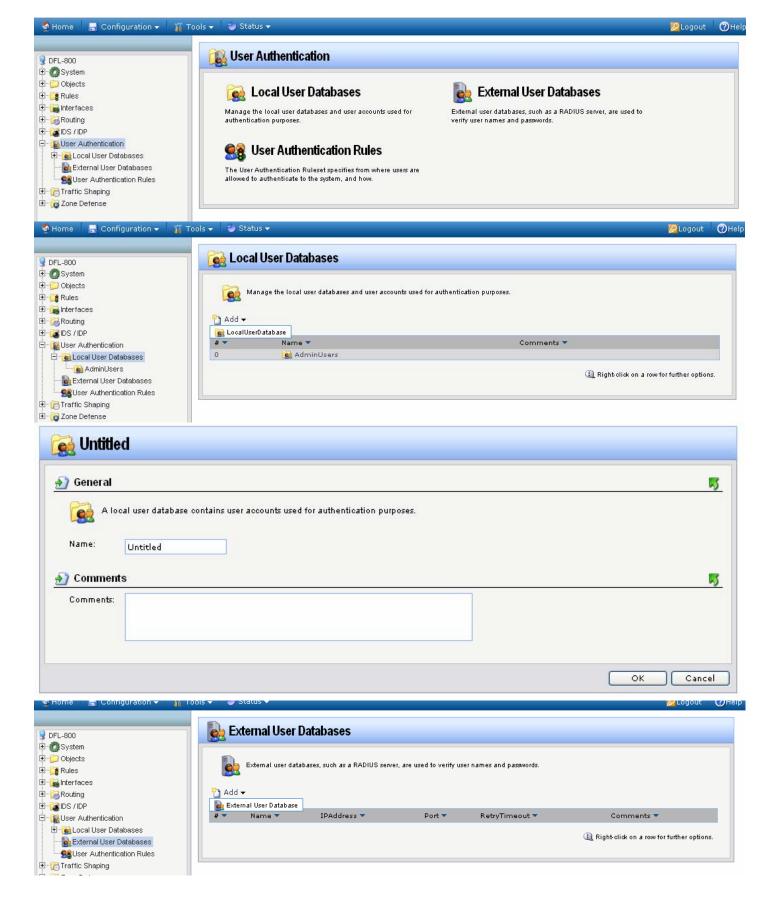
3 DFL-800 E OSystem 🗄 📁 Objects IDS/IDP Rules are used to detect intrusion attempts and/or inspect network traffic and take appropriate action. E- 8 Rules 🗄 🚘 Interfaces E BRouting 👌 Add 👻 💣 IDS/IDP Rule 🖻 🔂 IDS / IDP SourceInterface 🔻 SourceNetwork 🔻 DestinationInterface 🔻 DestinationNetwork 🔻 Service 💌 Name 💰 IDS Signatures IDS Rules Right-click on a row for further options. 🚿 IDS Updates 🗄 📓 User Authentication 🗄 📆 Traffic Shaping 🗄 👩 Zone Defense

eneral Lo	og Settings			
General				
at IDS/	/IDP Rules are used t	to detect intrusion attemp	and/or inspect network traffic and take appropriate action.	
Name:	Untitled			
Service:	(None)	~		
Schedule:	(None)	~		
🖌 Also in	spect dropped packe	ts		
		ts		
Also in Address		ts		
Address	Filter		erwith destination interface and destination network. All parameters ha	
Address	Filter		er with destination interface and destination network. All parameters ha	
Address	Filter cify source interface	and source network, toge	er with destination interface and destination network. All parameters ha	
Address Spe	Filter :cify source interface Source	and source network, toge Destination		
Address Spe natch.	Filter cify source interface Source (None)	and source network, toge Destination (None)	~	
Address Spe	Filter :cify source interface Source	and source network, toge Destination		
Address Spe natch. Interface: Network:	Filter crify source interface Source (None) (None)	and source network, toge Destination (None)	~	ve to match for the rule to
Address Spe natch.	Filter crify source interface Source (None) (None)	and source network, toge Destination (None)	~	
Address Spe natch. Interface: Network:	Filter crify source interface Source (None) (None)	and source network, toge Destination (None)	~	ve to match for the rule to
Address Spe natch. Interface: Network: Commen	Filter crify source interface Source (None) (None)	and source network, toge Destination (None)	~	ve to match for the rule to

Name:	Untitled		
Service:	(None)	~	
Schedule:	Name	Comments	
Schedule.	(The H323	H.323 via H323 ALG - Enables H.323 communication	
Alex is a	Ma H323.	H.323 RAS via H323 ALG - Enables communication with H.323	
Also hisp	Gatekeeper	Gatekeepers	
	Montitled		
🧃 Address Fi	M Untitled		
	Montitled		
💢 Speci	🐚 Untitled		
match.	[] all_icmp	All ICMP services	
	() all_services	All ICMP, TCP and UDP services	
	🀚 all_top	All TCP services	
Interface:	🀚 all_tcpudp	All TCP and UDP services	
	🀚 all_udp	All UDP services	
Network:	🀚 bootpc	Bootstrap protocol (also DHCP) client	_
	🀚 bootps	Bootstrap protocol (also DHCP) server	
Comments	🀚 chargen	Character generator	
- connente	🐚 dns-all	DNS via TCP and UDP	
Comments:	🐚 dns-top	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	
	M 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	

General Cog Settings		
General		
R. Select log receiver's) and severith	to enable logging for this object.	
	to enable logging for this object.	
Enable logging:		
Coveritor		
Log Receivers		
Logitoconors		
All receivers		
<ul> <li>All receivers</li> <li>Specific receiver(s):</li> </ul>		
All receivers     Specific receiver(s):     Available     Selected		
All receivers     Specific receiver(s):  Available  MemLog		
All receivers     Specific receiver(s):     Available     Selected		
All receivers     Specific receiver(s):  Available  MemLog		
C Specific receiver(s): Available Selected MemLog		

🙅 Home 🛛 🚽 Configuration 👻 👔	Tools 🗸 🕘 Status 🗸	💆 Logout 🛛 🕐 Heli
DFL-800	🕺 IDS Updates	
± → ⑦ System → ♡ Objects	DS Updates	R.
Ð∽ <mark>ig</mark> Rules Ð∽ing Interfaces Ð∽igg Routing	Settings Related to the IDS Update Mechanism.	
DS / IDP	Enable Updates	
DS Rules MDS Updates User Authentication	Update Server: http://dflupdate.dlink.co.uk/ids/	
T and the file an	Interval: Monthly 🗸	
	Specific Day in Each Week:	
	Pattern Update Time: : (HH:MM)	
		OK Cancel
🛃 IDS Updates		
Settings Relate	d to the IDS Update Mechanism.	
🖌 Enable Updates		
Update Server:	http://dflupdate.dlink.co.uk/ids/	
Interval:	Monthly 🖌	
Specific Date in Each N	Ionth: Daily Daily Updates Weekly Weekly Updates	
Specific Day in Each W		
Pattern Update Time:	: (HH:MM)	



) General					ļ
External user d.	tabases, such as a RADIUS s	server, are used to verify	user names and password	ts.	
Name: Unti	led				
Type: Radi					
IP Address: (Non					
	12				
Retry Timeout:	2 seconds				
Shared Secret:	2 Seconds				
Confirm Secret:					
) Comments					
Comments:					
at the second			-		
					OK Cance
					10
me 🛛 🛃 Configuration 👻	🌃 Tools 👻 🥥 Status 👻				2Logout
-800	Ser Auth	nentication Rules			
System Objects					
Rules	The User /	Authentication Ruleset specifie	s from where users are allowed to	) authenticate to the system, a	nd how.
Interfaces					
	🗕 bha 🕰				
Routing	*``_ Add <del>↓</del> Sig User Authenticat	tion Rule			
Routing IDS / IDP User Authentication	T Add ▼ S User Authenticat # ▼ Name ▼		AuthSource 🔻	Interface 🔻	Comments 🔻
Routing IDS / IDP User Authentication @Local User Databases	🥞 User Authenticat		AuthSource 🔻	Interface 🔻	
Routing IDS / IDP User Authentication Local User Databases Local User Databases	🥞 User Authenticat		AuthSource 🔻	Interface 🔻	Comments 💌
Routing IDS / IDP User Authentication Local User Databases Local User Databases Siguser Authentication Rules	🥞 User Authenticat		AuthSource 🔻	Interface 💌	
Routing DS / IDP User Authentication Local User Databases External User Databases So User Authentication Rules Traffic Shaping	🥞 User Authenticat		AuthSource 🔻	Interface 🔻	
Routing DS / IDP Jser Authentication Local User Databases External User Databases GUser Authentication Rules Traffic Shaping Zone Defense	🕵 User Authenticat # 🔻 Name 🕈		AuthSource 🔻	Interface 🔻	
Routing DS / IDP Jser Authentication Local User Databases External User Databases User Authentication Rules Traffic Shaping Zone Defense	User Authenticat # Varne V	<ul> <li>Agent</li> </ul>			
Routing DS / IDP User Authentication Local User Databases External User Databases External User Databases Traffic Shaping Zone Defense	User Authenticat # Varne V			Interface   Restrictions	
Routing IDS / IDP User Authentication Local User Databases External User Databases Suser Authentication Rules Traffic Shaping Zone Defense Untitled General Log Settings	User Authenticat # Varne V	<ul> <li>Agent</li> </ul>			
Routing DS / IDP Jser Authentication Local User Databases External User Databases User Authentication Rules Traffic Shaping Zone Defense Untitled General Log Settings General	User Authenticat # Varne V	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	I Right-click on a row for further option
Routing DS / IDP Jeer Authentication Cocal User Databases Cocal User Databases Source Authentication Rules Traffic Shaping Zone Defense Cone Defense Cone Defense Cone Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal Cocal C	Authentication Options	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	I Right-click on a row for further option
Routing DS / IDP User Authentication Cocal User Databases External User Databases Conser Authentication Rules Traftic Shaping Zone Defense <b>Untitled</b> General Log Settings <b>General</b> <b>General</b> Name:	Authentication Options	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	I Right-click on a row for further option
Routing IDS / IDP User Authentication Local User Databases Local User Databases Local User Databases Surver Authentication Rules Traftic Shaping Zone Defense <b>Untitled</b> General Log Settings <b>General</b> <b>General</b> Name: Agent:	Authentication Options	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	( Right-click on a row for further option
Routing IDS / IDP User Authentication Local User Databases Subser Authentication Rules Traffic Shaping Zone Defense <b>Untitled</b> General Log Settings <b>General</b> <b>General</b> Mame: Agent: Authentication Source:	Authentication Options	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	( Right-click on a row for further option
Routing IDS / IDP User Authentication Cacal User Databases External User Databases Suser Authentication Rules Traffic Shaping Zone Defense <b>Untitled</b> General Log Settings <b>General</b> <b>General</b> Mame: Agent: Authentication Source: Interface:	Authentication Options P Authentication Options P Intication Ruleset specifies free Untitled HTTP V Radius V (None) V	Agent  Agent  HTTP(s) Agent Option:	s PPP Agent Options	Restrictions	( Right-click on a row for further option
Routing IDS / IDP User Authentication Local User Databases Local User Databases User Authentication Rules Untitled General Log Settings General Log Settings General Agent: Agent: Authentication Source: Interface: Originator IP:	Authentication Options Authentication Options ntication Ruleset specifies fro Radius (None) (None)	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options	Restrictions	( Right-click on a row for further option
Routing DS / IDP User Authentication External User Databases Suser Authentication Rules Traffic Shaping Zone Defense <b>Untitled</b> General Log Settings <b>General</b> <b>General</b> Name: Name: Agent: Authentication Source: Interface:	Authentication Options	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options wed to authenticate to the	Restrictions	( Right-click on a row for further option
Routing IDS / IDP User Authentication Local User Databases Subser Authentication Rules Traffic Shaping Zone Defense Untitled General Log Settings General General Mame: Agent: Authentication Source: Interface: Originator IP: Terminator IP:	Authentication Options	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options wed to authenticate to the	Restrictions	( Right-click on a row for further option
Routing IDS / IDP User Authentication Local User Databases User Authentication Rules User Authentication Rules Untitled General Log Settings General Cog Settings The User Authentication Name: Agent: Authentication Source: Interface: Originator IP: Terminator IP:	Authentication Options	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options wed to authenticate to the	Restrictions	Right-click on a row for further option
Routing DS / IDP User Authentication External User Databases Subser Authentication Rules Traffic Shaping Zone Defense Ceneral Log Settings Controlled Constantion Name: Agent: Authentication Source: Interface: Originator IP: Terminator IP: Comments	Authentication Options	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options wed to authenticate to the	Restrictions	Right-click on a row for further option
Routing DS / IDP User Authentication External User Databases Subser Authentication Rules Traffic Shaping Zone Defense Ceneral Log Settings Controlled Constantion Name: Agent: Authentication Source: Interface: Originator IP: Terminator IP: Comments	Authentication Options	Agent      Agent      Agent      orn where users are allow	s PPP Agent Options wed to authenticate to the	Restrictions	Right-click on a row for further option

General Log Settings	Authentication Options HTTP(s) Agent Options PPI	
約 General		
C	ication Ruleset specifies from where users are allowed to .	
<b>₩</b>		
Name:	Untitled	
Agent:	нттр	
Authentication Source:	HTTP	
Interface:	HTTPS	
	XAuth PPP	
Originator IP:	Example 1 For XAuth and PPP, this	
Terminator IP:	(None)	
Comments.		
Comments		
Comments:		
	and the state of t	
🔰 General		
C	cation Ruleset specifies from where users are allowed to a	
<b>∞</b> 8		
Name:	Untitled	
Agent:	нттр	
Authentication Source:	Radius	
Interface:	Disallow	
	Radius	
Originator IP:	Local his	
Terminator IP:	(None)	
C		
) Comments		
Comments:		
🔒 Untitled		
General Log Settings Au	hentication Options HTTP(s) Agent Options PPP Agent Options Restrictions	
) General		
<b>B</b>		
Select log receiver(s)	and severity to enable logging for this object.	
Enable logging:		
Severity: Notice	▼	
_		
) Log Receivers		
Log to:		
G Specific receivers	er(\$):	
Available	Selected	
MemLog		
<		
and the second s		
		ОК

neral Log Setting	Authentication Options	HTTP(s) Agent Options	PPP Agent Options	Restrictions	
General					
Select one o	r more authentication servers	Also select the authentica	tion method, which is u	ed for encrypting the us	er password.
adius Server(s):	Available	Selected			
iaido deixel(o).	Untitled				
		>>			
		<			
adius Method:	PAP	,			
cal User DB:	The second				
ical oser DD.	(None)	/			

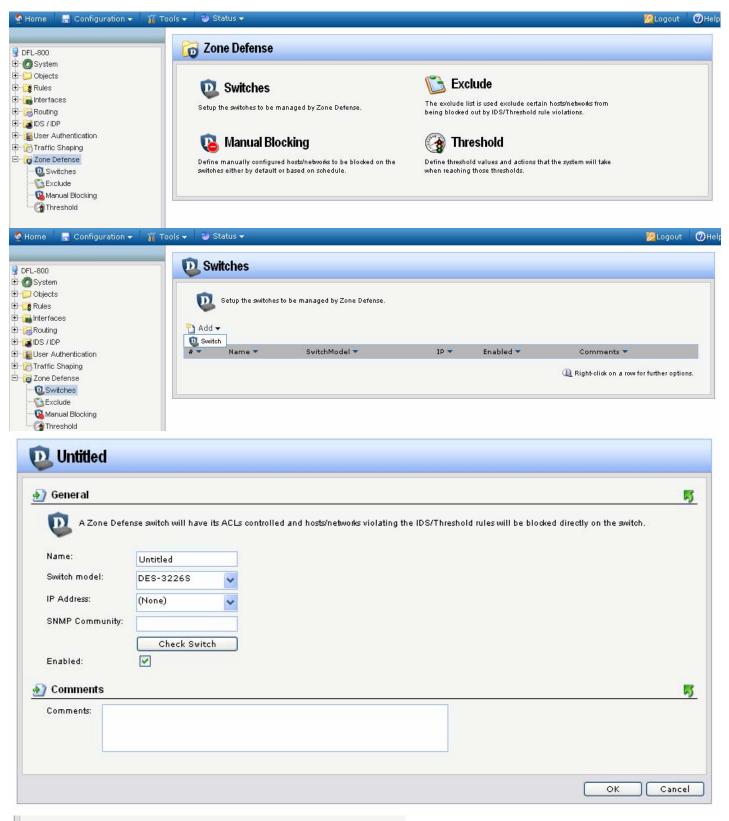
🍓 Untitled					
General Log Settings	Authentication Options	HTTP(s) Agent Options	PPP Agent Options	Restrictions	
釣 General					5
Login Type: Realm String:	HTMLForm	~			
Certificates Host Certificate:	(None)	~			<b>F</b>
Root Certificate:	(March)	*			
					OK Cancel

General Log Settings Authentication Options HTTP(s) Agent Options PPP Agent Options Restrictions	
🛐 General	
Allow Unauthenticated Users	
Unencrypted Password (PAP)	
Challenge Handshake Authentication Protocol (CHAP)	
Microsoft CHAP (MS-CHAP)	
Microsoft CHAP Version 2 (MS-CHAP v2)	
	OK Cano
A	
R Untitled	
Openeral VI as Sattienes Authentication Options (UTTD/a) (work Options (DDD (work Options ) Doctointic )	
General Log Settings Authentication Options HTTP(s) Agent Options PPP Agent Options Restrictions	
General Log Settings Authentication Options HTTP(s) Agent Options PPP Agent Options Restrictions	
Timeouts	
Timeouts	
Timeouts         Idle Timeout:       1800 seconds         Session Timeout:       seconds	
Timeouts         Idle Timeout:       1800 seconds         Session Timeout:       seconds         Use timeouts received from the authentication server.	
Timeouts         Idle Timeout:       1800 seconds         Session Timeout:       seconds	
Timeouts         Idle Timeout:       1800 seconds         Session Timeout:       seconds         Use timeouts received from the authentication server.	
Timeouts Idle Timeout: IBOD seconds Session Timeout: Seconds Use timeouts received from the authentication server. IN Note that if no timeouts are received, OR if this checkbox is unchecked, the above settings will be used. Multiple Username Logins	
Session Timeout: 1800 seconds Session Timeout: Use timeouts received from the authentication server. Use 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	
Session Timeout: 1800 seconds Session Timeout: Use timeouts received from the authentication server. 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.	
Session Timeout:   1800 seconds   Session Timeout: seconds   Session Timeout: seconds   Use timeouts received from the authentication server.   Image: Construction of the seconds of the second of the se	
Session Timeout: 1800 seconds Session Timeout: Use timeouts received from the authentication server. 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.	
Timeouts          Idle Timeout:       1800 seconds         Session Timeout:       seconds         Use timeouts received from the authentication server.	
Timeouts          Idle Timeout:       1800 seconds         Session Timeout:       seconds         Use timeouts received from the authentication server.	OK Can

🔮 Home	🗌 🔒 Configuration	🔹 🎢 Tools 🗸 🥹 Status 🗸	🖉 Logout 🗌 🕐 He	elp
E-Corrati	em cts s faces ng IDP Authentication ic Shaping ipes ipe Rules	Pipes       Pipes are used as regulators for network traffic flowing through the system.       Pipe Rules		
o Home	🗌 🛃 Configuration	🗸 🕌 🌃 Tools 🗸 😌 Status 🗸	🛛 🖉 Logout 🖉 P	Hel
	em ects faces faces (IDP - Authentication fic Shaping Pipes	Pipes Pipes are used as regulators for network traffic flowing through the system. Add - Pipe # Name Grouping GroupingNetworkSize LimitKbpsTotal Comme Bight-click on a row f		
	Untitled			1
N N <u>1</u> Us	ame: U Pipe Limits se pipe limits to spe	nes basic traffic shaping parameters. The pipe rules then determines which traffic goes through which pipes. Intitled ecify bandwidth limits per precedence in the pipe. If traffic in one precedence exceeds its limits, additional traffic will be pushed cedence (usually precedence 'Low').	S down to the	
F	Note that, for b Precedences: Highest: High: Medium:	andwidth, 'kilo' and 'mega' are multiples of 1000, not 1024 kilobits per second kilobits per second kilobits per second kilobits per second		
	Grouping	kilobits per second	5	
		er-port/IP/network static bandwidth limits as well as dynamic balancing between groups.	~	
<u>.</u>		None Maximum bandwidth per group: kilobits per second  Enable dynamic balancing of groups	<u>=5</u>	
				1000
		ОК	Cancel	4

ne 🔡 Confi	iguration 🔻 🛛 🏭 🤇	Tools 👻 🚭	) Status 🔻								2 Logout
300			ipe Rules								
/stem											
bjects		0									
ules		(	👌 Define a traffic shap	ping policy by	y specifying what ne	twork traffic st	ould flow through v	vhat pipes			
terfaces		6									
outing		👌 Ad	d 🕶								
S/IDP			pe Rule								
ser Authenticatio	n	# 🕶	Name 🔻 SourceInt	erface 🔻	SourceNetwork *	<ul> <li>Destin</li> </ul>	ationInterface 🔻	Destinati	onNetwork 🔻	Service 🔻	Comments <
affic Shaping									(II) Ria	ht-click on a row fo	r further option
Pipes									(2 <u>17</u> 1118	ine circa on a root re	in runner opnom
Pipe Rules											
one Defense											
👌 Untitle	ed										
0											
General Tr	raffic Shaping										
Comment											
7 General											
Service:	(None)	*									
Schedule:	(None)	*									
) Address	Filter										j
Spe	cify source interfa	ace and net	work, together with	destinatio	on interface and	d destinatio	n network.				
See.3											
	Source		Destination								
Interface:	(None)	*	(None)	~	•						
Network:	(None)	*	(None)	~	•						
) Commen	**										
Comments:											
	4										
										ОК	Canc

eneral Traffi	c Shaping				
		matching this rule through on	e or more pipes in order to perfo	rm traffic shaping on the particular traffic.	
Forward Chain	Available	Selected			
	Untitled				
Return Chain	Available	Selected			
	Untitled				
Precedence					
Ticcouches	16				
Map IP DS	CP (ToS)				
C Use Fixed I	Precedence				
(None)	~				



Name:	Untitled	
Switch model:	DES-3226S	*
IP Address:	DES-3226S	(R4.02-B14 or above)
	DES-3250TG	(R3.00-B09 or above)
SNMP Community:	DES-3326S	(R4.01-B39 or above)
	DES-3350SR	(R1.02.035 or above)
	DES-3526	(R3.01-B23 or above)
Enabled:	DES-3550	(R3.01-B23 or above)
	DGS-3324SR	(R4.10-B15 or above)
魡 Comments		
Comments:		

🔮 Home 🛛 🔒 Configuration 👻	🚺 Tools 🔻	🕘 Status 👻		💋 Logout	(2)Help
Home Configuration DFL-800 System Objects Rules Frances Second System Frances Second System Frances Second System Second System Frances Second System Second System Frances Second System Second System S		General General The exol	Iude list is used exclude certain hosts/networks from being blocked out by IDS/Threshold rule violations.         Available       Selected         Iannet       Image: Selected         dmanet       Image: Selected         wan1_ip       Image: Selected		<u>85</u>
				OK Can	cel

🔮 Home	🗌 🔂 Configurat	iion 👻 🛛 🌃 Tools 👻	🥹 Status 👻				22Logout	ЮНе
			4					
3 DFL-800			🏅 Manual Blocking	9				
E OSyste	em		<b>-</b>	70:				
🗄 📁 Objec			-					
E Rules			Define manually cor	nfigured hosts/networks to be block	ed on the switches either by	default or based on scl	hedule.	
E 🔒 Interf								
E 🐻 Routin		1	Add 🗸					
E DS /			💫 Manual Block					_
	Authentication		# 🔻 Addresses 🔻	Protocol 💌	Port 🔻	Schedule 🔻	Comments 💌	
🗄 🔂 Traffi							-	
E 👩 Zone	Defense						(1) Right-click on a row for further option	s.
- 🔃 s	witches							
- 🔁 E	xclude							
<b>1</b>	lanual Blocking							
- 🚱 TI	hreshold							
								_
	Manual	lask						
	Manual B	SIOCK						
-								
2	General							5
ST I								
	陷 Manually	configured blocks	are used to block a host	/network on the switches e	ither by default or bas	ed on schedule.		
	9	•						
A	ddresses:	Available	Selected					
		lan_ip	A					
		lannet						
		dmz_ip						
		dmznet	_ <<					
		wan1_ip wan1net						
		Iwanifier						
P	rotocol:	All	*					
	2004 C							
P	ort:	0						
	chedule:	AL						
۲ ۲	cileadie.	(None)	*					
	Comments							
2	comments							<b>N</b>
C	omments:							
	onniene.							
	10							
1								
							OK Cance	el 📄

💁 Home 👘 🛃 Con	nfiguration 👻 🗌 🁔	Tools 👻 🕘 Status 👻					🖉 Logout 👘
DFL-800 OSystem		😽 Threshol	d				
		Define th	reshold values and actions	: that the system will take	when reaching those thresholds	5. No	
- 😹 Routing - 😭 IDS / IDP	1	Threshold	SourceInterface 🔻	SourceNetwork 🔻	DestinationInterface 🔻	DestinationNetwork 🔻	Service 🔻 Action 🔻
- 💽 User Authenticati - 👩 Traffic Shaping	1011						on a row for further options.
Zone Defense							
Called Exclude Called Manual Blocki Called Threshold	ing						
🛞 Untitl	ed						
General	.og Settings A	ction					
🄊 General							5
							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
thr	reshold defines a	i rule matching specific	network traffic. When	the rule criteria is	πet, the thresholds are e	valuated and possible ac	tions taken.
Name:	Untitled						
Service:	(None)	~					
Schedule:	(None)	~					
1		Terror Control of Cont					
Address	Filter						5
match. Spi	ecify source inter	face and source network	, together with destir	nation interface and	l destination network. All	parameters have to mat	ch for the rule to
	Source	Destin	ation				
Interface:	(None)	V (None) 🗸				
Network:	(None)	V (None) 🖌				
Comment Comment	nts						5
Comments:							
							OK Cancel

🗿 Untitled	
General Log Settings Action	
🧿 General	5
Select log receiver(s) and severity to enable logging for this object. Enable logging: Severity: Notice	
Dog Receivers	ন
Log to: All receivers	
Specific receiver(s):	
Available Selected	
	OK Cancel
l Untitled	
8	
General Log Settings Action	

Action:	ZoneDefense 🗸	
Host-based Threshold:	1000 connections/second	
Network-based Threshol		
Newtork-Dased (Hiteshor)	1. 1000 connectionssecond	

Seneral Log Settings	Action		
Action			
Action:	ZoneDefense	~	
	ZoneDefense		
Host-based Threshold:	Audit	Allow new connections and log.	
Network-based Threshold:		ections/second	