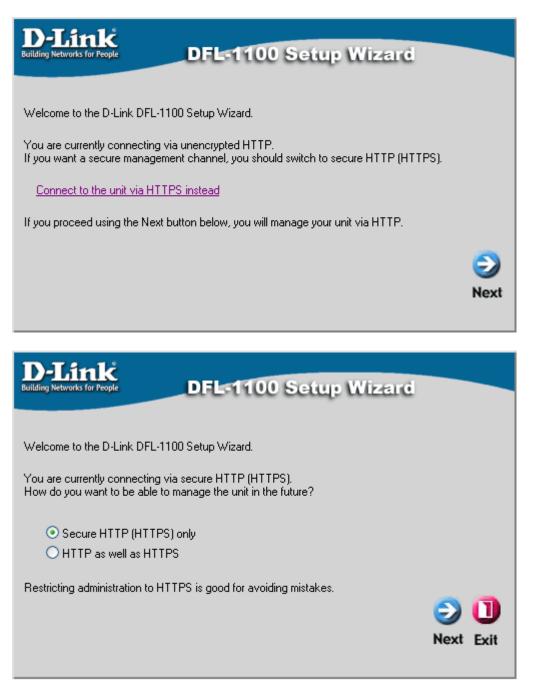
DFL-1100 Screenies

FW-1.20.00

Created By: Scott Howell



D-Link Building Networks for People DFL=1100 Setup Wizard
D-Link DFL-1100 Setup Wizard, Step 1 - Set admin password
Please enter a password for protecting the administrative interface of the unit: Username: admin
Password:
Note that the password is case sensitive, and that you should pick a password that contains upper- and lowercase letters as well as numbers and/or special characters.
Back Next Exit
D-Link
Building Networks for People DEL-1100 Setup Wizard

D-Link DFL-1100 Setup Wizard, Step 2 - Set timezone

Select the appropriate time zone and click Next to continue.	

(GMT+10:00) Canberra, Guam, Port Mo	resby, Vladivostok	*			
Daylight saving time settings:					
 No daylight saving time 					
· · · · · · · · · · · · · · · · · · ·					
Apply daylight saving time from:	Mar 💙 28 💙				
to:	Oct 🔽 28 🔽				
			-	-	-
			(-)	Ð	
				9	9
			Back	Next	Exit
					LAN

DFL-1100 Setup Wizard

D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface

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

Static IP - manual configuration

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

O DHCP - automatic configuration

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

PPPoE - account details needed

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

O PPTP - account details needed

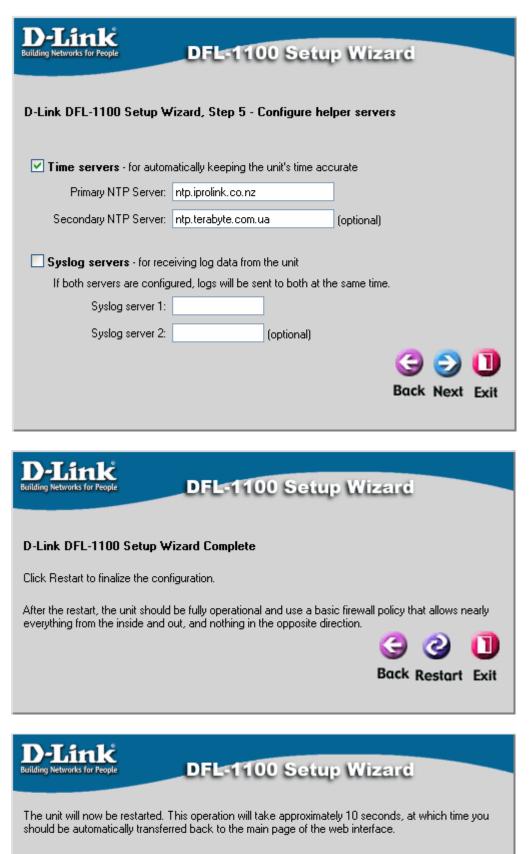
PPTP over Ethernet connection. Used in some DSL and cable modern networks. You need account details, but also IP parameters for the physical interface that the PPTP tunnel runs over.

O Big Pond - account details needed

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



D-Link Building Networks for People DFL-1100 Setup Wizard	
D-Link DFL-1100 Setup Wizard, Step 3 - Configure WAN interface	
PPP over Ethernet connections are used in many DSL and cable modem networks. After authenticating, everything is automatic.	
Username: dlink.comp@ozemail.com.au	
Password:	
Retype Password:	
Service Name: OzEmail (Some ISPs require the Service Name to be filled out.)	
G Sack Next	1 Exit
D-Link Building Networks for People DFL-1100 Setup Wizard	
D-Link DFL-1100 Setup Wizard, Step 4 - Set up built-in DHCP server	
You may enable the built-in DHCP server so that the gateway can hand out IP addresses to c the LAN via the DHCP protocol.	ients on
• Disable DHCP Server	
O Enable DHCP Server	
Enter a range of IP addresses to hand out to DHCP clients:	
IP Range: 192.168.1.0 - 192.168.1.255	
	0



If you are not automatically transferred, you can reconnect to the unit manually.



п

System	Firewall	Servers	Tools	Status	Help
Administration	Settings				
Management v	veb GUI ports				
HTTPF					
HTTPS F	ort: 443				
ports. Also r	note that if web-based	etter to run the mana <u>c</u> d user authentication II has to use other por	is enabled, ports	on non-standard 80 and 443 will be	
				🛛 🚫 🕴	3 🗘
				Apply Car	cel Help
				Appij cu	ice: neip
	-	edit from the below lis			
Note that both the and read-only righ	user settings and the	e interface settings lim ewhere where only re	it what a user ca	n do, so if a user v	vith both admir
Note that both the and read-only righ to log on, but will r	user settings and the ts logs on from a som	e interface settings lim ewhere where only re ess only.	it what a user ca	n do, so if a user v	vith both admin
Note that both the and read-only righ to log on, but will r	user settings and the ts logs on from a som eceive read-only acc	e interface settings lim iewhere where only re cess only. ce <u>(Edit)</u>	it what a user ca	n do, so if a user v	vith both admin
Note that both the and read-only righ to log on, but will r Administrative acc Ping:	e user settings and the ts logs on from a som eceive read-only acc cess via LAN interfac Any address Any address (HT	e interface settings lim iewhere where only re cess only. ce <u>(Edit)</u>	it what a user ca	n do, so if a user v	vith both admin
Note that both the and read-only righ to log on, but will r Administrative acc Ping: Admin:	e user settings and the ts logs on from a som eceive read-only acc esss via LAN interfac Any address Any address (HT e access via: e: <u>WAN</u> , <u>DMZ</u> , <u>ETH</u>	e interface settings lim ewhere where only re cess only. ce [Edit] TPS only)	it what a user ca	n do, so if a user v	vith both admin



н

System	Firewall	Servers	Tools	Status	Help
Administration So	ettings				
Edit administrative a	ccess via the LAN	interface:			
🗹 Ping - standa	rd ICMP echo to th	e IP address of the ir	nterface		
Networks:			Blank = An	ý	
🗹 Admin - Full a	access to web-base	d management			
Networks:			Blank = An	y.	
Protocol:	HTTPS only	*			
📃 Read-only ·	Read-only access (o web-based manag	ement		
Networks:			Blank = An	y	
Protocol:	HTTP and HTTP	S 🗸			
SNMP - Simp	le Network Manage	ement Protocol (read	-only access)		
Networks:	-		Blank = An	v	
Community:				,	
-		orks, e.g. ''192.168.(જ હ	9 🗘
				Apply Can	cel Help
Select the interface	/ user you wish to a	dit from the below lis	st.		
Note that both the u and read-only rights to log on, but will rea	logs on from a some	where where only re			
Administrative acce	ss via LAN interfac	e (Edit)			
Ping: Admin:	Any address Any address (HT	(PS only)			
Add administrative a	access via:				
	: <u>WAN, DMZ, ETH</u>	4			
VPN Tunnel					



ystem	Firewall	Servers	Tools
ninistration S	ettings		
administrative	access via the WAN	interface:	
Ping - stand	lard ICMP echo to th	e IP address of the i	nterface
Networks			Blank = Any
Admin - Ful	access to web-base	d management	
Networks			Blank = Any
Protocol	HTTP and HTTP	S 🗸	
Read-only	- Read-only access (o web-based manag	gement
Networks			Blank = Any
Protocol	HTTP and HTTP	S 🔽	
SNMP - Sin	nple Network Manage	ement Protocol (read	d-only access)
Networks			Blank = Any
Community			
that both the read-only right	e / user you wish to e user settings and the s logs on from a some eceive read-only acc	e interface settings li ewhere where only r	mit what a user can
inistrative acc	ess via LAN interfac	e [<u>Edit]</u>	
	Any address		
Ping: Admin:	Any address (HT	[PS only]	
_	Any address (HT	[PS only]	



н.

System	Firewall	Servers	Tools	Status	Help
Administration S	ettings				
Edit administrative a	access via the DMZ	interface:			
Ping - stand	ard ICMP echo to the	e IP address of the ir	nterface		
Networks:			Blank = An	ŷ.	
🔲 Admin - Full	access to web-base	d management			
Networks:			Blank = An	ý	
Protocol:	HTTP and HTTP	S 🗸			
Read-only	Read-only access t	o web-based manag	iement		
Networks:			Blank = An	U	
Protocol:	HTTP and HTTP	5.		,	
	ple Network Manage	ement Protocol (read			
Networks:			Blank = An	У.	
Community:					
Note that both the and read-only rights	user settings and the	dit from the below lis interface settings lin where where only re ess only.	nit what a user car	Apply Cane	th both admi
Administrative acce	ess via LAN interfac	e [<u>Edit]</u>			
Ping: Admin:	Any address Any address (HT1				
Add administrative	access via:				
Interface VPN Tunne VLAN Interface		4			



н.

System	Firewall	Servers	Tools	Status	Help
Administration S	ettings				
Edit administrative a	ccess via the ETH	4 interface:			
🔲 Ping - standa	ard ICMP echo to th	e IP address of the ir	nterface		
Networks:			Blank = Any	,	
🔲 Admin - Full	access to web-base	ed management			
Networks:			Blank = Any	,	
Protocol:	HTTP and HTTP	S 🔽			
🔲 Read-only -	Read-only access	to web-based manag	ement		
Networks:	_		Blank = Any	J	
Protocol:	HTTP and HTTP	s 🗸			
_		ement Protocol (read	-only access)		
Networks:	_		Blank = Any	J	
Community:					
				🦰 💦	
Note that both the u	user settings and the logs on from a some	edit from the below lis e interface settings lin ewhere where only re ess only.	nit what a user car	Apply Cane	th both admir
Note that both the u and read-only rights	iser settings and the logs on from a som ceive read-only acc	e interface settings lin ewhere where only re ess only.	nit what a user car	do, so if a user wi	th both admir
Note that both the u and read-only rights to log on, but will re	iser settings and the logs on from a som ceive read-only acc	e interface settings lin ewhere where only re ess only. e <u>[Edit]</u>	nit what a user car	do, so if a user wi	th both admir
Note that both the u and read-only rights to log on, but will re Administrative acce Ping: Admin:	user settings and the logs on from a some ceive read-only acc ss via LAN interfac Any address Any address (HT	e interface settings lin ewhere where only re ess only. e <u>[Edit]</u>	nit what a user car	do, so if a user wi	th both admir
Note that both the u and read-only rights to log on, but will re Administrative acce Ping: Admin:	user settings and the logs on from a some ceive read-only acc ss via LAN interfac Any address Any address (HT	e interface settings lin ewhere where only re ess only. e <u>[Edit]</u> TPS only)	nit what a user car	do, so if a user wi	th both admir



н

00000	System	Firewall	Servers	Tools	Status	Help
	Interface Settin	gs				
Administration	Pick an interface to	o edit from the below	list:			🛟 Help
mendces	Available interface	\$				netp
VLAN	LAN WAN (PPPol DMZ	[Edit]				
Routing	ETH4	[E dit]				
HA						
Logging						
Time						



L.

00000	System	Firewall	Servers	Tools	Status	Help
	Interface Settir	igs				
Administration	Edit settings of the	LAN interface:				
Interfaces	IP Addres Subnet Mas		- 256 hosts (/24) 💉	•		
VLAN					💋 🔮 Apply Can	cel Help
Routing	Available interface	25				
НА	LAN WAN (PPPo DMZ	(<u>Edit)</u> E) (<u>Edit)</u> (<u>Edit)</u>				
Logging	ETH4	(<u>Edit)</u>				
Time						



I

System	Firewall	Servers	Tools	Status	
Interface Settin	igs				
Edit settings of the	WAN interface:				
Change WA	N Type: PPPoE	Apply Chang	ge 🛛		
PPP over Ethernel After authenticatin	t connections are us g, everything is autor	ed in many DSL and matic.	cable modem net	works.	
	Username:	dlink.comp@ozemail	.com.au		
	Password:				
	Retype Password:				
	Service Name:	DzEmail			
	services provide DI		n. A few do not.	o be filled out.)	
	case, you can fill out imary DNS Server: [ourseir. optional)		
	ndary DNS Server:		optional)		
In order to d needs to kn these speed These settin Up	ping - interface spee o traffic shaping bey ow what the maximu ls. If the limits are se ugs should match the stream bandwidth: stream bandwidth:	ond simple limits, suo m bandwidth is. Th et too high, traffic sh	roughput through t aping will not work	his interface will be	
Normally, yo	erface MTU Confi u do not need to cha sical media supports. MTU: F	ange the MTU settin	gs. By default, the		
	MTU:	1432 bytes.	Upper limit: 1492.	*	
				V 🗳	2
				Apply Can	cel
Available interface	8				
LAN WAN (PPPo	(<u>Edit)</u> E) (Edit)				
DMZ	[Edit]				
ETH4	[Edit]				



I

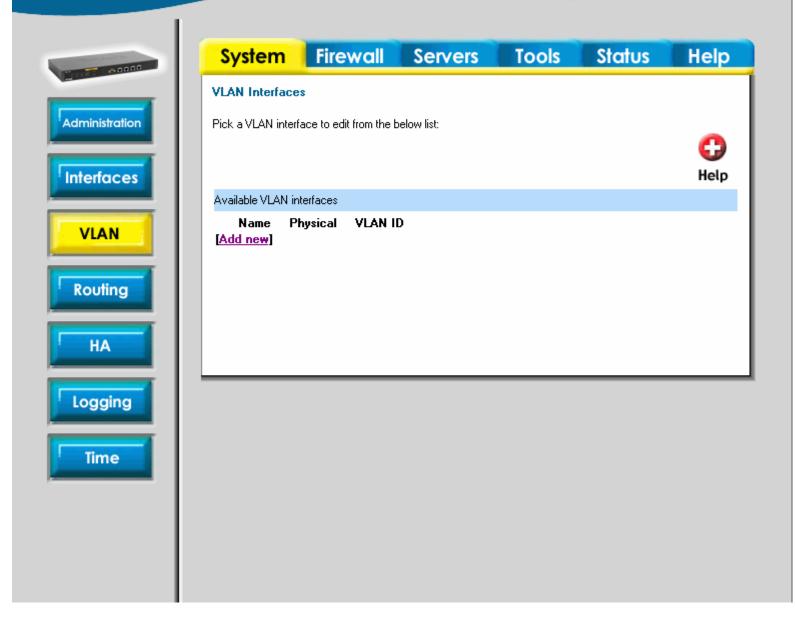
00000	System	Firewall	Servers	Tools	Status	Help
	Interface Settir	igs				
Administration	Edit settings of the	DMZ interface:				
Interfaces	IP Addres					
	Subnet Mas	k: 255.255.255.0	- 256 hosts (/24) 🕚	*		
VLAN					🤣 🙆) 🛟
Routing					Apply Can	el Help
	Available interface	es [Edit]				
HA	WAN (PPPc DMZ					
Logging	ETH4	[Edit]				
Time						



E

0000	System	Firewall	Servers	Tools	Status	Help
	Interface Settin	gs				
Administration	Edit settings of the	ETH4 interface:				
Interfaces	IP Addres	s: 127.0.0.1				
mendces	Subnet Masi	k: 255.255.255.0	- 256 hosts (/24) 📘	•		
VLAN					🧭 😆) 🗘
Routing					Apply Can	cel Help
Kooling	Available interface	28				
НА	LAN WAN (PPPo DMZ	[<u>Edit]</u> E) [<u>Edit]</u> [<u>Edit]</u>				
Logging	ETH4	[<u>E dit</u>]				
Time						







System	Firewall	Servers	Tools	Status	Help
VLAN Interfac	es				
Edit settings of th	e new VLAN:				
Nar	ne:				
Physic	al: LAN 💌				
VLAN	ID: 0	(0-4095)			
IP Addre	\$\$:				
Subnet Ma	sk: 255.255.255.0	- 256 hosts (/24) 💊			
				🧭 🔮) 🕄
				Apply Can	cel Help
Available VLAN i	nterfaces				
	Physical VLAN I	D			
Add new					



I

 Routing Table					
Pick a route to edit	t from the below list:				
Note that routing ta	able ordering does not	matter; smaller route	es are always picked	above larger ones.	
					0
					•
					He
Routing table					
Interface	Network	Gateway	Additional IP	Proxy ARP	,
LAN	192.168.1.0/24				(Ec
WAN	0.0.0/0				Ec
WAN	0.0.0/0				Ec
DMZ	127.0.0.0/24				(Ec
 ETH4	127.0.0.0/24				(Ec
Add new					



н.

	System	Firewall	Servers	Tools	Status	Help
B	outing Table					
Ed	lit 192.168.1 .0	0 7255.255.255.0 re	ute:			
No	ote that this is th	e local network route	for the interface; you	I can only change	the Proxy ARF	^o setting.
	Interfa	ce: LAN 💌				
	Netwo	ork: 192.168.1.0				
	Subnet Ma	sk: 255.255.255.0	- 256 hosts (/24)	*		
	Gatew	vay: Network is I 0.0.0.0	pehind remote gatev	vay		
	Proxy AF	RP: 🔲 Publish net	vork on all other inte	rfaces via Proxy Al	RP	
	Additional	IP: 📃 Additional fi	rewall IP address that	at hosts can use as	: gateway:	
		0.0.0.0				
					3	8 A
					Mpply C	3 🕄 ancel Help
B	outing table				Ø	3 🔂 ancel Help
B	Interface	Network	Gateway	Additional II		y ARP
B		192.168.1.0/24		Additional II		y ARP (Edit)
B	Interface LAN			Additional II		y ARP (Edit) (Edit)
B	Interface LAN WAN	192.168.1.0/24 0.0.0.0/0		Additional II		y ARP (Edit) (Edit) (Edit)
B	Interface LAN WAN WAN	192.168.1.0/24 0.0.0.0/0 0.0.0.0/0		Additional II		y ARP [Edit [Edit [Edit
B	Interface LAN WAN WAN DMZ ETH4	192.168.1.0/24 0.0.0.0/0 0.0.0.0/0 127.0.0.0/24		Additional II		y ARP (Edit)



	System	Firewall	Servers	Tools	Status	
	Routing Table					
L.	Edit 0.0.0.0/0.0	.0.0 route:				
	Note that this is th	e local network route f	or the interface; you	ı can only change tl	he Proxy ARP set	ting.
L	Interfa	ce: 🛛 🛛 💙				
	Netwo	ork: 0.0.0.0				
	Subnet Ma	isk: 0.0.0.0	- 4G hosts (/0)	*		
	Gatew		behind remote gatev	1911		
		0.0.0.0		vay		
	Proxy Al	RP: 📃 Publish netw	ork on all other inte	rfaces via Proxy AR	IP	
	Additional	ID —				
		😳 🔛 Additional fin	ewall IP address that	at nosts can use as	gateway:	
		0.0.0.0				
ī 🗌		0.0.0.0				
		0.0.0.0				
		0.0.0				
		0.0.0			S (2	
		0.0.0			ॐ	el
		0.0.0			Mapply Cana	cel
	Routing table	0.0.0			ॐ	cel
	Routing table	0.0.0.0 Network	Gateway		🕥 😢 Apply Cane	
	_				🕥 😢 Apply Cane	
	Interface	Network			🕥 😢 Apply Cane	
	Interface LAN	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0			🕥 😢 Apply Cane	
	Interface LAN WAN	Network 192.168.1.0/24 0.0.0.0/0			🕥 😢 Apply Cane	
	Interface LAN WAN WAN	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0			🕥 😢 Apply Cane	



System	Firewall	Servers	Tools	Status	H
Routing Table					
Edit 127.0.0.0/2	55.255.255.0 route	e:			
Note that this is the	e local network route	for the interface; you	u can only change t	the Proxy ARP se	etting.
Interfac	ce: DMZ 💌				
Netwo	rk: 127.0.0.0				
Subnet Ma	sk: 255.255.255.0	- 256 hosts (/24)	*		
Gatew					
	0.0.0	behind remote gatev	vay		
Proxy AF	P: 🔲 Publish net	work on all other inte	erfaces via Proxy AF	3P	
Additional					
Additional	IP: 📃 Additional fi	irewall IP address th			
Additional					
Additional	IP: 📃 Additional fi				
Additional	IP: 📃 Additional fi				
Additional	IP: 📃 Additional fi				3
Additional	IP: 📃 Additional fi				3 Incel
	IP: 📃 Additional fi			: gateway:	3 Incel
Routing table	IP: Additional f	irewall IP address th	at hosts can use as	gateway:	
Routing table	IP: Additional f	irewall IP address th 		gateway:	
Routing table Interface LAN	IP: Additional f 0.0.0.0 Network 192.168.1.0/24	irewall IP address th 	at hosts can use as	gateway:	
Routing table Interface LAN WAN	IP: Additional fi 0.0.0.0 Network 192.168.1.0/24 0.0.0.0/0	irewall IP address th 	at hosts can use as	gateway:	
Routing table Interface LAN WAN WAN	IP: Additional f 0.0.0.0 Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0	irewall IP address th 	at hosts can use as	gateway:	
Routing table Interface LAN WAN WAN DMZ	IP: Additional f 0.0.0.0 Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0 127.0.0.0/24	irewall IP address th 	at hosts can use as	gateway:	
Routing table Interface LAN WAN WAN	IP: Additional f 0.0.0.0 Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0	irewall IP address th 	at hosts can use as	gateway:	



Routing table Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 [E] WAN 0.0.0.0/0 [E] WAN 0.0.0.0/0 [E] DMZ 127.0.0.0/24 [E]		System	Firewall	Servers	Tools	Status	Hel
Note that this is the local network route for the interface; you can only change the Proxy ARP setting. Interface: DMZ Network: 127.00.0 Subnet Mask: 255.255.255.0 Gateway: Network is behind remote gateway 0.0.0 0 Proxy ARP: Publish network on all other interfaces via Proxy ARP Additional IP: Additional firewall IP address that hosts can use as gateway: 0.0.0 0 Note table Export Enterface: Network Gateway: 0.0.0 Q.0.0 0 Mathing IP: Additional firewall IP address that hosts can use as gateway: 0.0.0 0 Reputy Cancel Here Note table Interface: Network Max 0.0.0/0 WAN 0.0.0/0 WAN 0.0.00/0 WAN 0.0.00/0 Max 0.0.00/0 Max 0.0.00/0 Max 0.0.00/24 ETH4 127.0.00/24	F	Routing Table					
Interface: DMZ Network: 127.0.0.0 Subnet Mask: 255.255.255.0 - 256 hosts (/24) Gateway: Network is behind remote gateway 0.0.0 0.0.0 Proxy ARP: Publish network on all other interfaces via Proxy ARP Additional IP: Additional firewall IP address that hosts can use as gateway: 0.0.0 0.0.0 Proxy ARP: 0.0.0 Proxy ARP: 0.0.0 Additional IP: Additional firewall IP address that hosts can use as gateway: 0.0.0 0.0.0 Routing table Ketwork Gateway: Additional IP Proxy ARP: Image: Network Cancel Hetwork MAN 0.00.0/0 WAN 0.00.0/0 WAN 0.00.0/0 WAN 0.00.0/0 WAN 0.00.0/0 WAN 0.00.0/2 MA 0.00.0/2 MA 0.00.0/2 WAN 0.00.0/2	E	dit 127.0.0.0/2 !	55.255.255.0 route	e:			
Network: 127.0.00 Subnet Mask: 255.255.255.0 - 256 hosts (/24) Gateway: Network is behind remote gateway 0.0.0	M	lote that this is the	local network route	for the interface; yo	u can only change (the Proxy ARP :	setting.
Subnet Mask: 255.255.255.0 -256 hosts (/24) Image: Constraint of the state of the sta		Interfac	e: DMZ 💌				
Gateway: Network is behind remote gateway 0000 Proxy ARP: Proxy ARP: Publish network on all other interfaces via Proxy ARP Additional IP: Additional firewall IP address that hosts can use as gateway: 0000 0000 Quertication Quertication Proxy ARP: Additional firewall IP address that hosts can use as gateway: Quertication Quertication Quertication Quertication Quertication Quertication Routing table Interface Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 Image: Cancel		Netwo	rk: 127.0.0.0				
Proxy ARP: Publish network on all other interfaces via Proxy ARP Additional IP: Additional firewall IP address that hosts can use as gateway: 0000 0000 WAN Gateway Additional IP Proxy ARP: Interface Network Gateway Additional IP Proxy ARP: Proxy ARP: Additional firewall IP address that hosts can use as gateway: 0000 Outing table Interface Network Gateway Additional IP Proxy ARP: LAN 192.168.1.0/24 E WAN 0.00.0/0 E DM2 127.0.0.0/24 E ETH4 127.0.0.0/24 E E		Subnet Mas	sk: 255.255.255.0	- 256 hosts (/24)	*		
Proxy ARP: Publish network on all other interfaces via Proxy ARP Additional IP: Additional firewall IP address that hosts can use as gateway: 0.0.0 Image: Concelement of the second		Gatewa		behind remote gate	vay		
Additional inewall in address that hosts can use as gateway. 0.0.0 Apply Cancel He Routing table Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 WAN 0.00.0/0 WAN 0.00.0/0 DMZ 127.0.0.0/24 ETH4 127.0.0.0/24		Proxy AR	_	work on all other inte	erfaces via Proxy AF	RP	
Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 E WAN 0.0.0/0 E WAN 0.0.0/24 E DMZ 127.0.0/24 E		Additional I	P: 📃 Additional fi	rewall IP address th	at hosts can use as	gateway:	
Routing tableInterfaceNetworkGatewayAdditional IPProxy ARPLAN192.168.1.0/24EWAN0.0.0.0/0EWAN0.0.0.0/0EDMZ127.0.0.0/24EETH4127.0.0.0/24E							
Routing table Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 E WAN 0.0.0.0/0 E WAN 0.0.0.0/2 E DMZ 127.0.0.0/24 E ETH4 127.0.0.0/24 E			0.0.0.0				
Routing tableInterfaceNetworkGatewayAdditional IPProxy ARPLAN192.168.1.0/24EWAN0.0.0.0/0EWAN0.0.0.0/0EDMZ127.0.0.0/24EETH4127.0.0.0/24E			0.0.0.0			.	2
Interface Network Gateway Additional IP Proxy ARP LAN 192.168.1.0/24 [E] WAN 0.0.0.0/0 [E] WAN 0.0.0.0/0 [E] DMZ 127.0.0.0/24 [E] ETH4 127.0.0.0/24 [E]			0.0.0.0			ى 20	3 C
LAN 192.168.1.0/24 [E] WAN 0.0.0.0/0 [E] WAN 0.0.0.0/0 [E] DMZ 127.0.0.0/24 [E] ETH4 127.0.0.0/24 [E]			0.0.0			ى 20	3 🕻 Incel Hel
WAN 0.0.0/0 E WAN 0.0.0/0 E DMZ 127.0.0/24 E ETH4 127.0.0/24 E						🍼 🄇 Apply Ca	
WAN 0.0.0/0 E DMZ 127.0.0/24 E ETH4 127.0.0/24 E	F	Interface	Network	Gate w ay		🍼 🄇 Apply Ca	ARP
DMZ 127.0.0/24 E ETH4 127.0.0/24 E		Interface LAN	Network 192.168.1.0/24	Gate w ay		🍼 🄇 Apply Ca	ARP E
ETH4 127.0.0.0/24		Interface LAN WAN	Network 192.168.1.0/24 0.0.0.0/0	Gate w ay		🍼 🄇 Apply Ca	ARP
		Interface LAN WAN WAN	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0	Gate w ay		🍼 🄇 Apply Ca	ARP
		Interface LAN WAN WAN DMZ	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0 127.0.0.0/24	Gate w ay		🍼 🄇 Apply Ca	ARP E E
		Interface LAN WAN WAN DMZ ETH4	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0 127.0.0.0/24	Gate w ay		🍼 🄇 Apply Ca	
		Interface LAN WAN WAN DMZ ETH4	Network 192.168.1.0/24 0.0.0.0/0 0.0.0.0/0 127.0.0.0/24	Gate w ay		🍼 🄇 Apply Ca	



Stand Sy	stem Firewo	II Servers	Tools	Status	Help
and the second	Availability				
on	Error:		1 5 51		
	High Availability s connections.	etups may only be config	ured on units with	static WAN	



System	Firewall	Servers	Tools	Status	Help
Logging Setting	s				
Syslog - ser	nd log data via the sy	vslog protocol to one	or two servers		
If both serve	ers are configured, lo	ogs will be sent to bot	h at the same time	9.	
Sys	log server 1:				
Sys	log server 2:	(option	al)		
Sj	vslog facility: Loca	10 🗸			
🗌 Enable aud	lit logging				
The firewall	normally logs denied	l packets. With audit	logging enabled,	it will also log when	allowed
connections	s open and close.				
📃 Enable E-n	ail alerting for IC				
	Sensitivity: High	×			
Sh	MTP Server:				
	Sender:				
E-Ma	il Address 1:				
E-Ma	il Address 2:				
E-Ma	il Address 3:				
				o 😒 🖸	
				Apply Can	cel Help



System	Firewall	Servers	Tools	Status	Не	elp
Time Settings						
Current time and d	ate					
🔲 Set the sy						
	04 🔽 Aug 🔽 : 01:02:20 (24 hour l					
nme.	01:02:20 [24 hour)	limej				
	ylight saving time set					
Time zone:	(GMT+10:00) Canbe	erra, Guam, Port Mor	esby, Vladivostok	*		
	ight saving time	om; Jan 🔽 01	~			
🤍 Αρρίγ α	aylight saving time fro 	to: Jan 🔽 01				
Automatic time syr	nchronization					
🗹 Enable NT						
	NTP Server: <u>ntp.ipro</u> NTP Server: <u>ntp.tera</u>		(and invertibuted)			
Secondary r	arr Server, http://eia	byte.com.ua	(optional)			
Note: The Curre	nt time and date	and Time zone sett	ings above			
will be applied inst	antly, and do not req	uire Activate Char	iges.			
				🍼 🧕	3 6	3
					ncel He	elp





0000	System	Firewall	Servers	Tools	Status	Help
cy	Firewall Policy Edit global policy p					
	Fragme Minimum T		agmented packets			
					💋 🥴 Apply Cana	el Help
l						



Firewall	Policy						
Show poli	sy: <u>LAN->W</u> WAN->L			Z <u>LAN->ETH4 M</u> N <u>ETH4->LAN</u> J		->ETH4 4->DMZ	
Settings fo	r LAN->WAN	policy:					
NA		ource addresses \T - requires publ		NAT) s on LAN network.			
					A		
Select "Ad	id New'' belo	w, or select a rule	from the list to) edit it:	Mapply Co	incel H	C) Help
LAN->WA						incel H	() Help
LAN->WA Name	N Policy	Action	Source	Destination	Service		C) Help
LAN->WA Name #1 drop_	N Policy smb-all	Action Drop	Source Any	Destination Any	Service smb-all	[Edit]	1
LAN->WA Name #1 drop_ #2 allow	N Policy smb-all _ping-outbour	Action Drop id Allow	Source Any Any	Destination Any Any	Service smb-all ping-outbound	(Edit) (Edit)	1
LAN->WA Name #1 drop_ #2 allow	N Policy smb-all _ping-outbour _ftp-passthrou	Action Drop id Allow	Source Any	Destination Any	Service smb-all	[Edit]	C) Help

Add New rule:

Name: Position:	Unnamed_1]	1-1
	Drop	given position. Blank :	= last.
Action:	ыор	· ·	
Source Nets:			
Users/Groups:			"Any" = Any authenticated
Destination Nets:			
Users/Groups:			"Any" = Any authenticated
	Leave source and/or o	destination blank to ma	tch everything.
Service:	All		
	Custom source ports:		Blank = any port
	destination ports:		
Schedule:	- Always - 💙		
Intrusion Detec	tion / Prevention:		
Mode:	Inspection only		
Alerting:	Enable IDS/IDP a	alerting via email for thi	s rule
Traffic shaping	- limits and guarantees		
Upstream:	Limit Guar	antee kbit/s	
Downstream:	kbit/s	kbit/s	
	Normal Guarantee	- KDI(7'S	
Priority:	Note that priorities and	guarantees will only w	ork if the traffic limits for the WAN
			ts will however always work.
Policy routing ·	reroute traffic via norma	al routing or address tra	anslation
Gateway:	0.0.0.0]	
Method:	 Redirect via routir 	— ng (make gateway nex	t hop)

 \bigcirc Via address translation (rewrite destination IP in packet)





ю

System	Firewall	Servers	Tools	Status	Help
Firewall Policy					
Show policy: <u>LAN-</u> WAN	<u>>wan</u> <u>Lan->dm</u> I->lan <u>dmz</u> ->la			AN->ETH4 DMZ-> H4->WAN ETH4->	
Note: Hosts on the private addresses wi		ATed. Writing rule	s that allow traffic I	from the Internet to I	hosts with
Select "Add New" b	elow, or select a rule	e from the list to e	dit it:		
WAN->LAN Policy	tion Sourc		nation	Service	
[Add new]					
If no rule matches, th	ne connection will be	e denied and logg	ed.		



н.

Firewall Policy Show policy: LAN-SWAN LAN-SDMZ WAN-SDMZ LAN-SETH4 WAN-SETH4 DMZ-SETH4 WAN-SLAN DMZ-SLAN DMZ-SWAN ETH4-SLAN ETH4-SWAN ETH4-SDMZ Settings for LAN-SDMZ policy: NAT: Hide source addresses (many-to-one NAT) No NAT Ward State Ward State Ward State No NAT Setect "Add New" below, or select a rule from the list to edit it: LAN-SDMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound Edit #2 allow_ftp-passthrough Allow Any Any All Protocols Edit #3 allow_standard Allow Any Any All Protocols Edit Add new] Inow Any Any All Protocols Edit
WAN->LAN DMZ->LAN DMZ->WAN ETH4->LAN ETH4->WAN ETH4->DMZ Settings for LAN->DMZ policy: NAT: Hide source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: No NAT Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one NAT) Image: Conceler to the source addresses (many-to-one to the source addresses (many-to-
Settings for LAN->DMZ policy: NAT: Hide source addresses (many-to-one NAT) No NAT No NAT Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination #1 allow_ping-outbound Allow Any Hilde allow_standard Allow Any Allow Any All Protocols
NAT: O Hide source addresses (many-to-one NAT) No NAT No NAT Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any Any Any Any Any All Protocols Edit) #3 allow_standard Allow Any Any Any Any Any Any All Protocols Edit)
 No NAT No NAT Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound Edit #2 allow_ftp-passthrough Allow Any Any All Protocols Edit #3 allow_standard Allow Any Any All Protocols Edit
 No NAT Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ftp-passthrough Allow Any Any All Protocols Edit) #3 allow_standard Allow Any Any All Protocols Edit)
Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [E dit] #2 allow_ftp-passthrough Allow Any Any All Protocols [E dit]
Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [Edit] #2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [Edit] #2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
Select "Add New" below, or select a rule from the list to edit it: LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [Edit] #2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
LAN->DMZ Policy Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [Edit] #2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
Name Action Source Destination Service #1 allow_ping-outbound Allow Any Any ping-outbound [Edit] #2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
#1 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#2 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#3 allow_standardAllowAnyAnyAll Protocols[Edit]
#2 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit]
#3 allow_standard Allow Any Any All Protocols [Edit]
[Add new]
If no rule matches, the connection will be denied and logged.



System	Firewall	Servers	Tools	Status	Help
	->WAN LAN->DMZ N->LAN DMZ->LA		LAN->ETH4 WA ETH4->LAN ETH		
Settings for DMZ->I					
	ide source addresses o NAT	(many-to-one NA	T)		•
				🏏 🔰 Apply Car	9 😈 ncel Help
Select "Add New" DMZ->LAN Policy	below, or select a rule	e from the list to ea	dit it:		
Name Ac [<u>Add new]</u>	tion Sourc	e Desti	nation	Service	Order of evaluation
					aluation
If no rule matches, I	the connection will be	e denied and logge	ed.		•



System	Firewall	Servers	Tools	Status	Help
Firewall Policy Show policy: LAN- WAN	<u>>wan</u> <u>Lan->dmz</u> ->lan dmz->lan		LAN->ETH4 WAN ETH4->LAN ETH		
Note: Hosts on the private addresses w		ATed. Writing rul	es that allow traffic fr	om the Internet to h	nosts with
Select "Add New" b	elow, or select a rule	e from the list to e	dit it:		
-	tion Sourc	e Desti	nation	Service	
					Order of evaluation
					/aluation
If no rule matches, t	he connection will be	e denied and logg	ed.		ţ



н.

Firewall Policy Show policy: LAN->WAN_LAN->DMZ WAN->DMZ LAN->ETH4 WAN->ETH4 DMZ->ETH4 Settings for DMZ->WAN policy: NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy: Name Action Source Drop Any Any Smb-all Edit) #2 allow_fitp-passthrough Allow Any Any All Protocols Edit) The passthrough Allow Any Any All Protocols Edit) Edit)	Show policy: LAN-> WAN LAN-> DMZ WAN-> DMZ LAN-> ETH4 WAN-> ETH4 DMZ-> ETH4 Settings for DMZ->WAN policy: NAT: Image: Hide source addresses (many-to-one NAT) Image: Wan-> Eth4 Image	Show policy: LAN->WAN LAN->DMZ WAN->DMZ LAN->ETH4 WAN->ETH4 DMZ->ETH4 WAN->LAN DMZ->LAN DMZ->WAN ETH4->LAN ETH4->WAN ETH4->DMZ Settings for DMZ->WAN policy: NAT: Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: Settings for DMZ->WAN policy: Image: Addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addresses (many-to-one NAT) Image: Addresses (many-to-one NAT) Image: No NAT - requires public IP addresses on DMZ network. Image: Addrese (many-to-one NAT) Image: A		rewall	Servers	Tools	Status	
WAN->LAN DMZ->WAN ETH4->LAN ETH4->WAN ETH4->DMZ Settings for DMZ->WAN policy: NAT: Hide source addresses (many-to-one NAT)	WAN>LAN DMZ>LAN DMZ>WAN ETH4>LAN ETH4>WAN ETH4>DMZ Settings for DMZ>WAN policy: NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Setect "Add New" below, or select a rule from the list to edit it: Mame Action Source Destination Service #1 drop_smb-all Drop Any Any mig-outbound Edit #2 allow_ping-outbound Allow Any Any Any All Protocols Edit #4 allow_standard Allow Any Any All Protocols Edit 	WAN-SLAN DMZ-SLAN DMZ-SWAN ETH4-SLAN ETH4-SWAN ETH4-SDMZ Settings for DMZ-SWAN policy: NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Setect "Add New" below, or select a rule from the list to edit it: DMZ-SWAN Policy Name Action Source Destination Service Edit 2 allow, ping-outbound Edit 2 allow Any Any ming-outbound Edit 2 allow, and and and and and any Any All Protocols Edit 2 allow, standard Edit 2 allow, and and and any Any All Protocols Edit 2 allow, and and and any Any All Protocols Edit 2 allow, and and allow Any Any All Protocols Edit 2 allow, and and allow Any All Protocols Edit 2 allow, and and allow Any All Protocols Edit 2 allow, and allow Any All Protocols Edit 3 allow, flap-passthrough Edit 3 allow	Firewall Policy					
NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit) #2 allow_ping-outbound Allow Any Any ftp-passthrough Edit) #4 allow_standard Allow Any Any All Protocols Edit)	NAT: Hide source addresses (many-to-one NAT) No NAT - requires public IP addresses on DMZ network. Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit #2 allow_ping-outbound Allow Any Any Itp-passthrough Edit #4 allow_standard Allow Any Any All Protocols Edit Add new] Allow Any Any All Protocols Edit						
No NAT - requires public IP addresses on DMZ network. Image: Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	No NAT - requires public IP addresses on DMZ network. Image: Select "Add New" below, or select a rule from the list to edit it. DMZ->WAN Policy Name Action Source If drop_smb-all Drop Any Any If drop_smb-all Drop Any Any Edit If allow_ping-outbound Allow Any Any Edit If allow_ftp-passthrough Allow Any Any Edit If allow_standard Allow Any Any All Protocols Edit	No NAT - requires public IP addresses on DMZ network. Image: Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit #2 allow_ping-outbound Allow Any Any ftp-passthrough Edit #3 allow_ftp-passthrough Allow Any Any All Protocols Edit #4 allow_standard Allow Any Any All Protocols Edit Add new] Any Any All Protocols Edit	Settings for DMZ->WAN	policy:				
Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough [Edit] #3 allow_standard Allow Any Any All Protocols [Edit] #4 allow_standard Allow Any Any All Protocols [Edit] [Add new] Any Any All Protocols [Edit]						
Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit] #2 allow_ping-outbound Allow Any Any ftp-passthrough Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit] #4 allow_standard Allow Any Any All Protocols [Edit] [Add new] Allow Any Any All Protocols [Edit]	No NA	F - requires public	e IP addresses	on DMZ network.		
Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit] #2 allow_ping-outbound Allow Any Any tip-passthrough Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols Edit] #4 allow_standard Allow Any Any All Protocols Edit] Add new] Any Any All Protocols Edit]					- 🍼 🎈	×
Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	Select "Add New" below, or select a rule from the list to edit it: DMZ->WAN Policy Name Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all Edit] #2 allow_ping-outbound Allow Any Any tip-passthrough Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols Edit] #4 allow_standard Allow Any Any All Protocols Edit] Add new] Any Any All Protocols Edit]						_
DMZ->WAN Policy Action Source Destination Service #1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any All Protocols [Edit]	DMZ->WAN PolicyNameActionSourceDestinationService#1 drop_smb-allDropAnyAnysmb-allEdit#2 allow_ping-outboundAllowAnyAnyping-outboundEdit#3 allow_ftp-passthroughAllowAnyAnyAll ProtocolsEdit#4 allow_standardAllowAnyAnyAll ProtocolsEdit	DMZ->WAN PolicyNameActionSourceDestinationService#1 drop_smb-allDropAnyAnysmb-allEdit#2 allow_ping-outboundAllowAnyAnyping-outboundEdit#3 allow_ftp-passthroughAllowAnyAnyftp-passthroughEdit#4 allow_standardAllowAnyAnyAll ProtocolsEditAdd new					Apply Co	incel
NameActionSourceDestinationService#1 drop_smb-allDropAnyAnysmb-all[Edit]#2 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#3 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#4 allow_standardAllowAnyAnyAll Protocols[Edit]	NameActionSourceDestinationService#1 drop_smb-allDropAnyAnysmb-all[Edit]#2 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#3 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#4 allow_standardAllowAnyAnyAll Protocols[Edit]	NameActionSourceDestinationService#1 drop_smb-allDropAnyAnysmb-all[Edit]#2 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#3 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#4 allow_standardAllowAnyAnyAll Protocols[Edit][Add new]AnyAnyAnyAll Protocols[Edit]					Apply Co	incel
#1 drop_smb-allDropAnyAnysmb-all[Edit]#2 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#3 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#4 allow_standardAllowAnyAnyAll Protocols[Edit]	#1 drop_smb-all Drop Any Any smb-all [Edit] #2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit]	#1 drop_smb-allDropAnyAnysmb-all[Edit]#2 allow_ping-outboundAllowAnyAnyping-outbound[Edit]#3 allow_ftp-passthroughAllowAnyAnyftp-passthrough[Edit]#4 allow_standardAllowAnyAnyAll Protocols[Edit][Add new]		, or select a rule	from the list to	edit it:	Αρριγ Co	incel
#2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit]	#2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit]	#2 allow_ping-outbound Allow Any Any ping-outbound [Edit] #3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit] [Add new] Any Any Any All Protocols [Edit]		, or select a rule	from the list to	edit it:		incel
#3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit]	#3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit]	#3 allow_ftp-passthrough Allow Any Any ftp-passthrough [Edit] #4 allow_standard Allow Any Any All Protocols [Edit] [Add new] Allow Any Any All Protocols [Edit]	DMZ->WAN Policy Name	Action	Source	Destination	Service	
#4 allow_standard Allow Any Any All Protocols [Edit]	#4 allow_standard Allow Any Any All Protocols [Edit]	#4 allow_standard Allow Any Any All Protocols [Edit] [Add new]	DMZ->WAN Policy Name #1 drop_smb-all	Action Drop	Source Any	Destination Any	Service smb-all	(<u>E dit</u>)
		[Add new]	DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbourd	Action Drop I Allow	Source Any Any	Destination Any Any	Service smb-all ping-outbound	(<u>E dit</u>) (<u>E dit</u>)
	[Add new]		DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbound #3 allow_ftp-passthroug	Action Drop I Allow h Allow	Source Any Any Any	Destination Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
		If no rule matches, the connection will be denied and logged.	DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbourd #3 allow_ftp-passthroug #4 allow_standard	Action Drop I Allow h Allow	Source Any Any Any	Destination Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
		If no rule matches, the connection will be denied and logged.	DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbourd #3 allow_ftp-passthroug #4 allow_standard	Action Drop I Allow h Allow	Source Any Any Any	Destination Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
		If no rule matches, the connection will be denied and logged.	DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbourd #3 allow_ftp-passthroug #4 allow_standard	Action Drop I Allow h Allow	Source Any Any Any	Destination Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
			DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbourd #3 allow_ftp-passthroug #4 allow_standard	Action Drop I Allow h Allow	Source Any Any Any	Destination Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
If no rule matches, the connection will be denied and logged.	If no rule matches, the connection will be denied and logged.		DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbound #3 allow_ftp-passthroug #4 allow_standard [Add_new]	Action Drop I Allow h Allow Allow	Source Any Any Any Any	Destination Any Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)
If no rule matches, the connection will be denied and logged.	If no rule matches, the connection will be denied and logged.		DMZ->WAN Policy Name #1 drop_smb-all #2 allow_ping-outbound #3 allow_ftp-passthroug #4 allow_standard [Add_new]	Action Drop I Allow h Allow Allow	Source Any Any Any Any	Destination Any Any Any Any	Service smb-all ping-outbound ftp-passthrough	(E dit) (E dit) (E dit)



Syst	em <mark>Fir</mark> e	ewall Se	ervers	Tools	Statu	JS I	Help
Firewall	Policy						
Show poli		LAN->DMZ WA DMZ->LAN DM			<u>N->ETH4 [</u> 14->WAN [
Settings fo	or LAN->ETH4 po	blicy:					
NA	T: 🔘 Hide sou 💿 No NAT	rce addresses (man	y-to-one NAT)				
					🍼 Apply	Cancel	C) Help
Select "A	dd New'' below, (or select a rule from	the list to edit it:				
LAN->ET							
LAN->ET Name [Add ne	Action	Source	Destinatio	'n	Service		1
Name	Action	Source	Destinatio	'n	Service		
Name	Action	Source	Destinatio	'n	Service		
Name	Action	Source	Destinatio	'n	Service		
Name	Action	Source	Destinatio	'n	Service		
Name [<u>Add ne</u>	Action			'n	Service		
Name [<u>Add ne</u>	Action	Source nection will be deni		'n	Service		



Sys	tem	Firewall	Servers	Tools	Stat	us I	lelp
Firewal	l Policy						
Show po		->WAN LAN->DMZ ->LAN DMZ->LAN			WAN->ETH4 ETH4->WAN		
Settings	for ETH4->l	AN policy:					
N	AT: 🔿 Hid 💿 No	de source addresses) NAT	: (many-to-one N	AT)			
					🍼 Apply	Cancel	C) Help
Select "/	Add New'' b	elow, or select a rule	e from the list to	edit it:			
ETH4->I	AN Policy						
	Act	tion Sourc	e Des	tination	Service		
Name [<u>Add n</u>	Act ew]	tion Sourc	e De:	tination	Service		
Name		ion Sourc	e De:	tination	Service		
Name		ion Sourc	e De:	tination	Service		OT det of evol
Name		ion Sourc	e De:	tination	Service		
Name		tion Sourc	e De:	tination	Service		OT LIEF OF EVALUATION
Name [Add m	ew]	t ion Sourc			Service		
Name [<u>Add n</u>	ew]				Service		



Syst	em <mark>F</mark> i	rewall	Servers	Tools	Status	Help
Firewall	Policy					
Show pol	icy: <u>LAN->WA</u> <u>WAN->LA</u>			AN->ETH4 WAN TH4->LAN ETH4		<u>>ETH4</u> >DMZ
Select "A	dd New'' below	v, or select a rule I	from the list to ed	lit it:		
WAN->E	TH4 Policy					
Name	Action	Source	e Desti	nation	Service	
[Add ne						
lf no rule	matches, the c	onnection will be	denied and looge	ed		



System	Firewa	Servers	Tools	Status	Help
Firewall Poli	су				
Show policy:		DMZ <u>WAN->DMZ</u> •LAN <u>DMZ->WAN</u>			
Settings for ET	H4->WAN policy:				
		esses (many-to-one NA : public IP addresses c			
				🍼 🥸 Apply Cane) 🛟 cel Help
Select "Add N	ew'' below, or select	a rule from the list to e	dit it:		
ETH4->WAN	Policy				
Name [Add new]	Action S	ource Dest	ination	Service	
					9
					Ğ
					- 1
If no rule matc	hes, the connection	will be denied and logg	ged.		



System	Firewall	Servers	Tools	Status	Help
	, <u>AN->WAN LAN->DM</u> /AN->LAN DMZ->L/				
Settings for DMZ	->ETH4 policy: Hide source address				
۲	No NAT			💋 🄇 Apply Ca	3 🔂 ncel Help
Select "Add New	v" below, or select a r licu	ule from the list to edi	t it:		
	Action Sou	rce Destin	ation	Service	
If no rule matche	s, the connection will	be denied and logge	d.		



Syste	em Fire	wall	Servers	Tools	Status	Help
Firewall F	Policy					
Show polic					->ETH4	
Settings fo	rETH4->DMZ po	blicy:				
NAT	: 🔘 Hide sour 💿 No NAT	ce addresses (m	any-to-one NAT)	I		
					🍼 🔮 Apply Can) 🛟 cel Help
Select "Ad	d New'' below, c	r select a rule fro	om the list to edit	it:		
ETH4->DM	IZ Policy					
		~	n		a .	
Name [<u>Add nev</u>	Action [Source	Destin	ation	Service	1
		Source	Destin	ation	Service	Ciuci
		Source	Destin	ation	Service	
		Source	Destin	ation	Service	
		Source	Destin	ation	Service	
[Add new	<u>*</u>]				Service	
[Add new					Service	



System	Firewall	Servers	Tools	Status	Help
Port Mapping	/ Virtual Servers				
Select "Add New	'' to create a new por	t mapping, or select a	a mapping to edit fi	rom the below list:	0
Configured mapp	pings:				Help
		stination	Service	Pass to	



н.

System Fi	irewall	Servers	Tools	Statu	S	Help
Port Mapping / Virtu	al Servers					
Edit new mapping :						
News	11					
Name:	Unnamed_1					
Source Nets:			Blank :	everyone =		
Users/Groups:			"Any"	= Any authent	ticated	
Destination IP:		Blank = V	VAN interface IP a	ddress		
Service:	Custom TCP	*				
	Custom source	e ports:	Blank	. = any port		
	destinatior) ports:				
	pass t	o port:	an	d up. Blank=n	o change.	
Pass To:						
Schedule:	- Always - 💌					
Intrusion Detec	Inspection onl					
Alerting:		S/IDP alerting via e	email for this rule			
Traffic shaping	- limits and qua	rantees for WAN tr	affic:			
	Limit	Guarantee				
Upstream:	kbit/s	kbit/s				
Downstream:	kbit/s	kbit/s				
	Normal Guara			- b (C - E b b	(V) / A	KI.
	interface are co	ies and guarantees onfigured correctly.	s will only work if th Simple limits will he	e trarric limits owever always	ror the WA s work.	N
				S	8	0
				Apply	Cancel	Help
Configured mappings:						
Name Source	n Dee	tination	Service	Pass to		



System	Firewall	Servers	Tools	Statu	JS	Help
User Managemen	it					
🗌 Enable Lleer	Authentication	via HTTP / HTTI	DC			
HTTP Se		as well as HTTPS	-0			
Idle Tin	neout: 2 hours	\sim				
🗌 Enable RAD	IUS Support					
Primary S		port 1812	1			
Secondary S		port 1812]			
	Mode: PAP 🔽		1			
Shared S		_				
Retype S	ecret:					
RADIUS	retry: 2 se	conds				
					\$	0
				Apply	Cancel	Help
					cuncer	neip
Select a user to edit	from the below list	, or select "Add new"				
Administrative users						
Admin: <u>adn</u> Read-only:	nin					[Add [Add
Users in local databa	ase					
User name	Groups					
[Add new]						



System	Firewall	Servers	Tools	Status	Help
User Managemer	nt				
Edit user admin :					
User	name: admin				
Group memb	ership: administra	ators			
🗌 Chang	e password				
Pas	sword:				
Retype pas	sword:				
Delete	user				
Membership in the '' Membership in the ''	administrators'' gro auditors'' group me	up means that the us ans that the user ha:	er can administer t s read-only access	to this unit.	0
Select a user to edit	from the below list	, or select "Add new"	ı.	Apply Cano	el Help:
Administrative users					
Admin: add					[Add]
Read-only:					[Add]
Users in local datab					
User name [Add new]	Groups				



	Firewall	Servers	Tools	Status	Help
User Manageme	nt				
Add new user:					
Use	r name:				
Group mem	bership:				
Pa	ssword:				
Retype pa	ssword:				
					_
				🛛 💟 🔮	3 🖸
				Apply Car	icel Help
Select a user to edi	it from the below list	, or select "Add new"			
Administrative user: Admin: ac					[Ad
Read-only:	<u></u>				[Ad
Users in local datal	Dase				
User name	Groups				
[Add new]					



Ľ

Anne	System	Firewall	Servers	Tools	Status	Help
	Manage Schedu		r .			
Policy	Pick a schedule to	edit from the below	list:			0
Port Mapping	Available schedule	s				Help
Users	Name [<u>Add new]</u>	Start Stop	Recurring			
Schedules						
Services						
s						
ering						



rirewaii	Servers	Tools	Status	Help
dules				
ile:				
э:				
n: 03 🔽 Aug 🔽	2004 🔽 Hour: 01	*		
o: 04 💌 Aug 💌	2004 🔽 Hour: 01	🔽 (inclusive)		
	12.00		10.00	
			- 🚺 💽) (
			💙 🔮 Apply Can) 🕻
r		ule: e: n: 03 V Aug V 2004 V Hour: 01 o: 04 V Aug V 2004 V Hour: 01 scheduling:	ule: e:	ule: e:





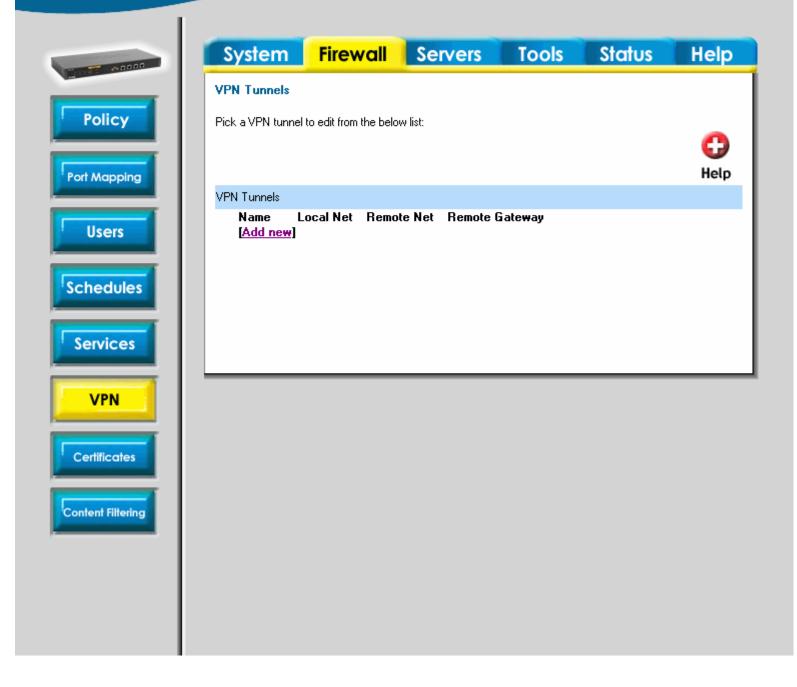
Services Settings	
Disk a service to add from the holes. But	
Pick a service to edit from the below list:	•
	• • • • • • • • • • • • • • • • • • • •
	Help
Defined services	
Name Parameters	
	dit]
	dit]
_ · ·	dit]
·	dit]
	dit
ipsec-natt UDP: All -> 4500	dit]
	dit]
ipcomp IP Protocol: 108	<u>[dit]</u>
l2tp-encap IP Protocol: 115	<u>dit</u>
	<u>dit</u>
	<u>dit</u>
	dit]
· · · · ·	dit]
_	dit]
	dit]
	dit]
	<u>dit</u>
	<u>dit]</u>
- · · · · · · · · · · · · · · · · · · ·	<u>idit]</u> idit]
-	dit]
- · ·	dit]
	dit]
- · ·	dit]
	dit]
	dit]
	dit]
	<u>dit</u>
	<u>dit</u>
	<u>dit]</u>
	dit]
	dit]
	dit]
	dit]
	<u>dit</u>
	<u>idit]</u> idit]
_	<u>: dit</u>]
-	dit]
	dit]
	dit]
	dit]
-	dit]
Idap TCP/UDP: All -> 389	<u>dit</u>
Idaps TCP: All -> 636	<u>dit</u>

ike	UDP: All -> 500	[Edit]
rexec	TCP: All -> 512	[Edit]
rlogin	TCP: All -> 513	[Edit]
remd	TCP: All -> 514	[Edit]
syslog	UDP: All -> 514	[Edit]
lpr	TCP: All -> 515	[Edit]
ms-sql-s	TCP: All -> 1433	[Edit]
ms-sql-m	TCP/UDP: All -> 1434	[Edit]
wins	TCP/UDP: All -> 1512	[Edit]
l2tp-ctl	UDP: All -> 1701	[Edit]
pptp-ctl	TCP: All -> 1723	[Edit]
rdp	TCP: All -> 3389	[Edit]
radius	UDP: All -> 1812	[Edit]
radius-acct	UDP: All -> 1813	[Edit]
nfs-udp	UDP: All -> 2049	[Edit]
nfs-top	TCP: All -> 2049	[Edit]
nfs-all	TCP/UDP: All -> 2049	[Edit]
ping-outbound	ICMP: Echo (Ping) Return ICMP Errors	[Edit]
ping-inbound	ICMP: Echo (Ping)	[Edit]
traceroute-udp	UDP: All -> 33434-33499 Return ICMP Errors	[Edit]
ftp-inbound	TCP: All -> 21 ALG: "ftp-inbound", max 100	[Edit]
ftp-outbound	TCP: All -> 21 ALG: "ftp-outbound", max 100	[Edit]
ftp-passthrough	TCP: All -> 21 ALG: "ftp-passthrough", max 100	[Edit]
http-all	TCP: All -> 80, 443	[Edit]
http-in-all	TCP: All -> 80, 443 SYN Relay	[Edit]
smb-all	TCP/UDP: All -> 135-139, 445	[Edit]
ipsec-suite	Group: ipsec-esp, ipsec-ah, ike, ipsec-natt	[Edit]
l2tp-raw	Group: I2tp-ctl, I2tp-encap	[Edit]
l2tp-ipsec	Group: I2tp-ctl, ipsec-suite	[Edit]
pptp-suite	Group: gre-encap, pptp-ctl	[Edit]
Add new		



System	Firewall	Servers	Tools	Status	Help
Services Settin	igs				
1	Name:				
💿 TCP / UDI	P Service:				
Pro	^{otocol:} 🔲 TCP				
	🔲 UDP				
Source	Ports:				
Destination	Ports:				
SYN F	Relay: 🗌 Protect	the destination from S	r'N flood attacks		
O ICMP Ech	o (Ping)				
O IP Protoco	ol:				
	ocols:				
	Example: "1-	5, 9, 15, 50-51''			
O Group:					
•	vices:				
	Comma-sepa	rated list of services o	r service groups.		
Protocol-indepen	dent settings:				
ICMP E		MP errors from the de:	stination to the sou	lice	
	ALG: -None-	~	P		
	Application L	ayer Gateways (ALGs) implement extra a	application logic tha	at is needed
	tor some prot dynamic data	ocols to work properly channels in addition	, like for instance to the command c	FTP, which needs hannel.	to open up
	Max ALG Se				
				🤍 🕓	, 🖸
				Apply Can	cel Help







E.

0000	System	Firewall	Servers	Tools	Status	Help
	VPN Tunnels					
Policy	Add VPN tunnel :					
Port Mapping	Lo	Name: cal Net: 192.168.	1.0/24			
Users						-
03613	Authentication:					
Schedules	⊙ PSK · F	Pre-Shared Key				
		PSK:				
Services	Retyr	be PSK:				
	O Certific	ate-based				
VPN	Local	Identity: Admin - 0	CN=000F3D59A840		~	
	Cert	ificates:				
		Use ctrl/s	hift click to select m	ultiple certificates.		
Content Filtering		To use ID	lists below, you mus	st select a CA certif		
	Ider	tity List: (no list)			\checkmark	
	Tunnel type:	ng Users - single-t	nost VPN clients			_
	IKE	XAuth: 🗌 Requ	iire user authenticati	on via IKE XAuth t	o open tunnel.	
	⊙ LAN-to	-LAN tunnel				
	Rem	ote Net:				
	Remote G					
		The gatev range of I	vay can be a numeri ^D addresses for roan	cal IP address, DN hing / NATed gates	S name, or vays.	
	Pro	xy ARP: 📃 Publi	sh remote network o	n all interfaces via	Proxy ARP.	
	IKE XAut	h client: 🔲 Pass requires it.	username and pass	word to peer via IK	E XAuth, if the remo	ote gateway
	XAuth Us	ername:				
	XAuth Pa	issword:				



VPN Tunnels

Name Local Net Remote Net Remote Gateway
[Add new]



Manage Certificates In order to do certificate-based authentication certificate to which you have the private key. You also need: • Copies of self-signed certificates of key. • One or more Certificate Authority cert These aspects can all be configured through Local identities (certificates to which you have Name Subject	nown peers, and/or tificates, and lists of identities that the below lists:	
Certificate to which you have the private key. You also need: Copies of self-signed certificates of k One or more Certificate Authority cert These aspects can all be configured through	nown peers, and/or tificates, and lists of identities that the below lists:	t they have signed.
 Copies of self-signed certificates of k. One or more Certificate Authority cert These aspects can all be configured through 	tificates, and lists of identities that n the below lists:	(
One or more Certificate Authority cert These aspects can all be configured through Local identities (certificates to which you have	tificates, and lists of identities that n the below lists:	(
Local identities (certificates to which you have		H
	e the private key)	H
	re the private key)	
Name Subject Ex		
	xpires Issuer D31-04-14 CN=000F3D59A84	40 [<u>E dit]</u>
Certificates of remote peers		
Name Subject Expires [Add_new]	Issuer	
Certificate Authorities		
Name Subject Expires [<u>Add new]</u>	Issuer	
Identities (lists of names signed by CAs)		
List name Members [Add new]		



System	Firewall	Servers	Tools	Statu	S	Help
HTTP Content I	Filtering					
Changes to these : By default, this incl	settings affect servi ludes the ''http-outb	ces that use the "HTT ound" service.	P/HTML Content I	Filtering'' AL(G.	
Global Destina	tion URL Whitel	ist:				
URLs match	ning the global white	list are excluded from	all the below checl	<s.< td=""><td></td><td></td></s.<>		
Contents: 10						
[Edit global l	JRL whitelist]					
Destination UF						
		ning the blacklist is blo	icked.			
Contents: 11						
Edit URL bl	<u>acklist</u>					
Active content	handling:					
📃 Strip Ac	ctiveX objects (inclu	ding Flash)				
📃 StripJa	iva applets					
📃 Strip Ja	wascript/VBScript					
📃 Block C	Cookies					
					52	0
					<u> </u>	•
				Apply	Cancel	Help

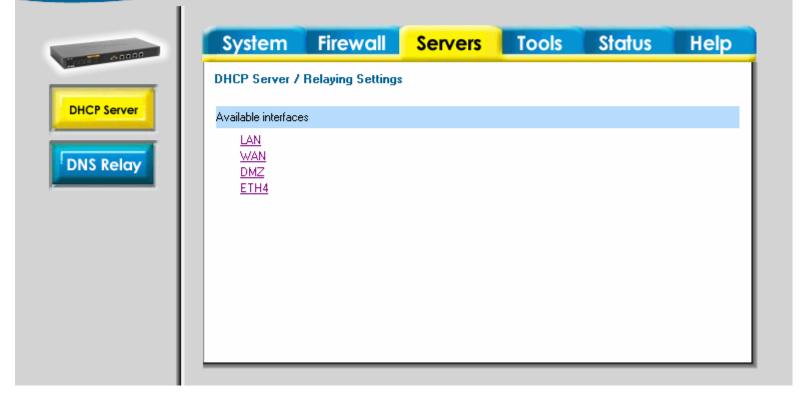


HTTP Content Filtering Edit Destination URL Global Whitelist: To allow access to a whole domain, use e.g. "".safesite.com/"". Note the ending slash, which protects a someone setting up e.g. "www.safesite.com.dyndnsprovider.net" as an alias for an otherwise disallowed Blank lines are ignored. Lines beginning with "#" are also ignored. # Access to sites that are important for software updates and # require cookies / scripts: d-link.com/" ".dlink.com/" ".dlink.com/" ".dlink.com.tw/" ".dlink.com.tw/" ".dlink.com.tw/" ".dlink.com.tw/" ".dlink.com.tw/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/" ".dlink.com/"								
Edit Destination URL Global Whitelist: To allow access to a whole domain, use e.g. "*.safesite.com/*". Note the ending slash, which protects a someone setting up e.g. "www.safesite.com.dyndhsprovider.net" as an alias for an otherwise disallowed Blank lines are ignored. Lines beginning with "#" are also ignored. # Access to sites that are important for software updates and # require cookies / scripts: dink.com/* *.dink.com/* *.dink.com/* *.dink.com/w *.dink.com/tw/*	Help	is l	Statu	Tools	Servers	Firewall	System	
To allow access to a whole domain, use e.g. "* safesite.com/*". Note the ending slash, which protects a someone setting up e.g. "www.safesite.com.dyndnsprovider.net" as an alias for an otherwise disallowed. Blank lines are ignored. Lines beginning with "#" are also ignored. # Access to sites that are important for software updates and # require cookies / scripts: dlink.com/* *.dlink.com/* *.dlink.com/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.microsoft.com/*						iltering	HTTP Content F	
someone setting up e.g. "www.safesite.com.dyndhsprovider.net" as an alias for an otherwise disallowed Blank lines are ignored. Lines beginning with "#" are also ignored. # Access to sites that are important for software updates and # require cookies / scripts: d-link.com/* *.d-link.com/* *.d-link.com/* dink.com/* *.d-link.com/* *.d-link.com.tw/* *.d-link.com.tw/* *.d-link.com.tw/* *.d-link.com.tw/* *.d-link.com.tw/* *.d-link.com/*						L Global Whitelist:	Edit Destination UF	
# Access to sites that are important for software updates and # require cookies / scripts: d-link.com/* *.d-link.com/* *.dlink.com/* d-link.com/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/*	s against ed site.	ich protects se disallowe	ng slash, wh)r an otherwi:	net'' as an alias I	.com.dyndnsprovider.	e.g. "www.safesite	someone setting up	L
<pre># require cookies / scripts: d-link.com/* *.d-link.com/* *.dlink.com/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.microsoft.com/*</pre>							_	
.d-link.com/ d-link.com/* *.d-link.com.tw/* *.d-link.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com/* *.microsoft.com/* *.microsoft.com/*			<u>^</u>	1	software updates an	hat are important for ' scripts:	# Access to sites t # require cookies .	
.dlink.com.tw/ *.d-link.com.tw/* dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.dlink.com.tw/* *.microsoft.com/* *.microsoft.com/* *.microsoft.com/*								
.d-link.com.tw/ *.dlink.com.tw/* *.dlink.com.tw/* microsoft.com/* *.microsoft.com/* *.microsoft.com/*								
.dlink.com.tw/ microsoft.com/* *.microsoft.com/*								
.microsoft.com/								
Apply Cancel							.microsoft.com/	
Apply Cancel								
Apply Cancel								
Apply Cancel	0	<u> </u>						
	Help	Cancel	Apply					



Syst	em Firewall	Servers	Tools	Status	Help
НТТР С	ontent Filtering				
Edit Desti	ination URL Global Blacklist:				
	blacklist can be used to der ords in them.	y access to complete :	sites, to file types	by extension, or to	URLs with
Use e.g. '	"*example.org/*" to disallow	access to an entire site	ə.		
Blank line	es and lines beginning with "‡	t" are ignored.			
#	le for blocking all access to a ple.com/*	a whole site:			
# *.exar # # Or, a sl	mple.com/* horter variant that runs the ris end with the same text:	sk of blocking sites wh	ose		
	nple.com/×				
# #Denya #	access to potentially dangero	us file types:			
# Malicio *.exe *.scr *.cpl	ous executables can be dowr	nloaded by exploits			
*.pif	probably not a good idea	given the .com TLD			
				× 🔊	0
				Apply Can	ol Help







I

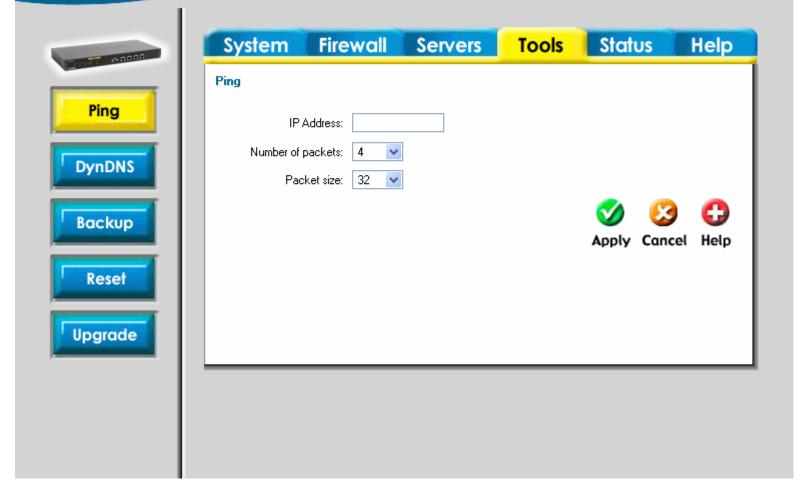
System	Firewall	Servers	Tools	Status	Hel
DHCP Server /	Relaying Setting	\$			
DHCP server / rela	ying settings for LAI	N interface:			
💿 No DHCP (processing				
The unit wil	ignore DHCP reque	ests heard on this inte	face.		
🔘 Use built-ir	DHCP Server:				
IP Sp	an:				
DNS Serve	ers:				
		(optional)			
	🗹 Use unit's	own DNS relayer add	resses		
WINS Serve	ers:	(optional)			
		(optional)			
	WINS servers	are used for name res	olution in windov	vs networks.	
Domain na	me:	(optional)			
Lease ti	me: 1 hour 🔽				
	The gateway v	vill be set to the IP ad	dress of the rece	iving interface.	
🔘 Relay DHC	P requests to ot	her DHCP server:			
Server	IP:				
				🛛 🕐 🥴) C
				Apply Can	cel Hel
Available interface	S				
LAN WAN					
DMZ					
<u>ETH4</u>					



E

0000	System	Firewall	Servers	Tools	State	US I	Help
	DNS Relay						
DHCP Server			vice on up to two fixe computers on the LA		ses.		
DNS Relay	Enable DN						
		Use addres:	s of LAN interface				
	IP Address	2:	(optional)				
	The requests will b	e relayed to the DNS	servers that this unit	itself uses.			
						83	0
					Apply	Cancel	Help
					_	_	







System	Firewall	Servers	Tools	Status	Help
Dynamic DNS	Registration via H	TTP			
The unit can aut	omatically register its er is useful for e.g. VPN1	kternal IP address with cunnels between gatew	a Dyn DNS ser	vice so that it can b	e located via
DNO hame. This	is ascial of e.g. vi in	unneis between gatew	ays with dynamic	nic n'addresses.	
Oisabled					
O <u>cjb.net</u>					
Username	:	(hostname become	s username.cjt	o.net)	
Password	:				
O <u>dyns.cx</u>					
Hostname	.dyns.cx				
Username	:				
Password	:				
O dyndns.o	ſġ				
Hostname	.dyndns.org				
Username	:				
Password	:				
🔘 Custom -	up to 3 HTTP requests	, posted in sequence			
To use HT	TP POST rather than	GET, use "httppost://"	' rather than ''h	ttp://".	
URL 1	:				
URL 2	:				
URL 3	:				
	: 1440 minutes				
Example:	http://user:pass@svc	example.com/path?ar	g1=val1&arg2=	=val2	
				🧭 🔮) 🕄
				Apply Can	cel Help



see Sys	tem Firewa	Servers	Tools	Status	Help
Backu	ip / Restore				
Backup	o unit's configuration				
By cor	clicking ''Download configu nfiguration. This can later be	ation", you will receive a uploaded to the unit to r 	package file cor estore the configu	ntaining the unit's en uration.	itire
	Download configuration				
Restore	e unit's configuration				
To	restore an old configuration,	you can upload a previo	usly downloaded	l backup file.	
	Upload configuration		Brow	vse	
					0
					Help



System	Firewall	Servers	Tools	Status	Help
Restart / Reset					
Restart					
-	start - reset interfac art - restart from pow	es and re-read config ver-on state	guration		
all firmware upg On the next sta wizard. It will no	e the unit to factory (grades removed. rt-up, its LAN IP add	defaults. This means I dress will be 192.168. ns on any interface ot	1.1, and the wet	o GUI will begin with	
					🛟 Help



	System	Firewall	Servers	Tools	Status	Help
Ī	Jpgrade					
L L	Jpgrade unit's firm	ware				
	To upgrade th it on your hard		vnload the firmware u	pgrade from the [)-Link support web	site and place
		ware is available, use be restarted to actival	this form to upload the the new firmware	he new firmware (o the unit. The unit	will
				Brow	se	
	Upload fi	irmware image				
l I	Jpgrade unit's sigr	nature-database				
		e unit's IDS signature ite and place it on yo	e-database, download ur hard drive.	the new signatu	re database file fron	n the D-Link
	When the sigr has been verif	ature file is available, ied, the unit will autor	, use this form to uplo matically be restarted	ad it to the unit. A to activate the cl	After the new signationanges.	ure-database
				Brow	_	
	Upload	signature database				
						0
						Help



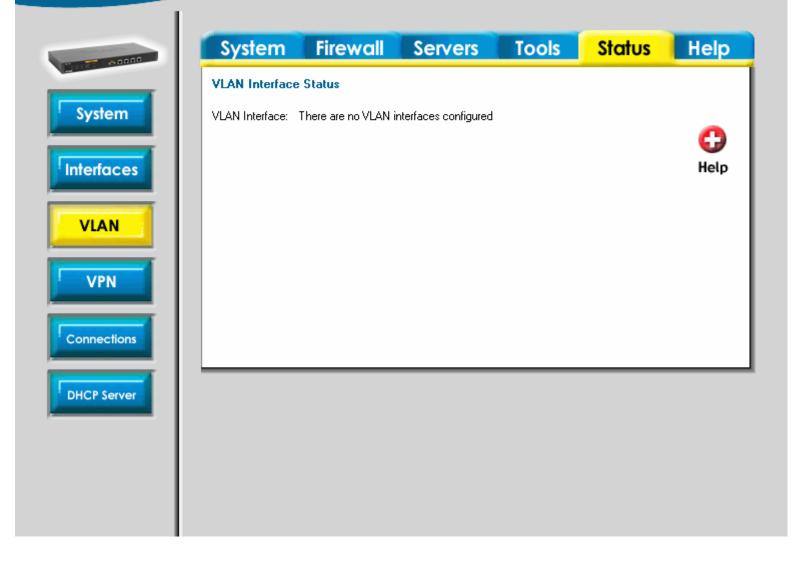
н.

System	Firewall	Servers	Tools	Status	Help
System Status	:				
Up	time: 0 days, 00:49:5(3			
	ation: Version 1, last c by "admin" from	hanged at 2004-08-04	\$ 00:36:05		
СРОТ	.oad: 0%				
	ions: 2 out of 200000	(0.0%)			
	sion: 1.20.00	· · ·			
Lastre	start: 2004-08-04 00:3	36:06: Configuration g	enerated by admir	(192.168.1.231)	
	ures: Last changed a				
CPU load ove	r the past 24 hours	s			
100% * * * *					
50% • • • •					
50%					
0% 24 hrs ag	0		now		
24116 09	0		1000		
State table us	age over the past	24 hours			
20					
10					
24 hrs ago			now		
					Help

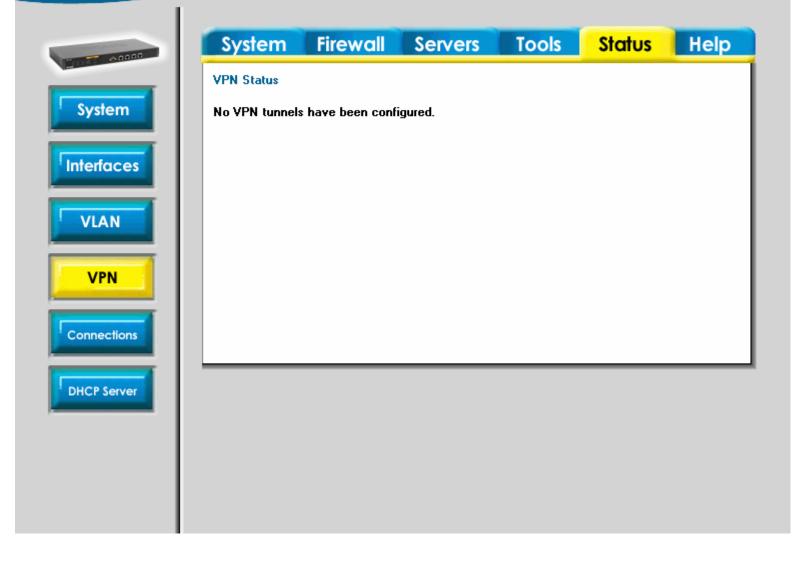


		The second			Charles of	
00000	System	Firewall	Servers	Tools	Status	Help
-	Interface Status	:				
L	Interface: LAN	WAN-PHYS WAN	<u>DMZ ETH4</u>			
	Interface:	LAN				
	IP Address:					
		100 Mbps Full Duple	×			
		000f:3d59:a842				
	Send rate:					
	Receive rate:	1 kbps				
L	Send rate over	the past 24 hours	:			
	20 kbps					
L.	10 kbps			_		
	0 kbps					
	24 hrs ag	0		now		
	Receive rate ov	ver the past 24 ho	ours			
	20 kbps					
	10 kbps					
	0 kbps			_		
	24 hrs ag	0		now		
						0
						U
						Help





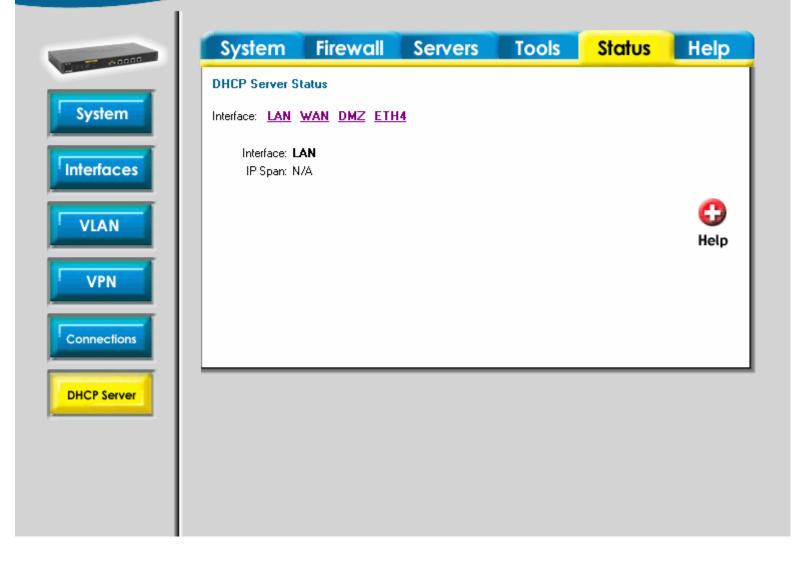






State Table Contents Filter state table display: Source Destination IP Address: Interface: Interface: Any IP Protocol Any Port Any DMZ ETH4 State table contents (max 100 entries) Timeout	System	Firewall	Servers	Tools State	us Help
State table contents (max 100 entries) State Proto Source Destination Timeout	Filter state table dis IP Address: Interface: IP Protocol	splay: Source	Any V Any V Core LAN WAN DMZ		ॐ
FIN_RCVD TCP LAN:192.168.1.231:1825 core:192.168.1.1:443 2		Proto Sc		Destination core:192.168.1.1:443	Timeout







I

Help System Interfaces VLAN Bouting HA Logging HA Logging Firewall Poit Mapping Users Schedules Services VPN Centificates Content Filtering Servers DNS Relay Ping DynDNS Backup Reset Upgrade Status VLAN VAN VAN Preset Upgrade VEN Cennections DHOP Servers	System	Firewall	Servers	Tools	Status	Help
Interfaces YLAN Routing HA Loaging Time Firewall Pott Mapping Users Schedules Services VPN Certificates Content Filtering Servers DNS Relay Ving Ven Status System Interfaces VAN HA VPN Connections	Help					
Policy Port Mapping Users Schedules Services VPN Certificates Content Filtering Servers DHCP Server DNS Relay Tools Ping DynDNS Backup Reset Upgrade Status System Interfaces VLAN HA VPN Connections	Interfaces VLAN Routing HA					
Servers DHCP Server DNS Relay Tools Ping DynDNS Backup Reset Upgrade Status System Interfaces VLAN HA VPN Connections	Policy Port Mapping Users Schedules Services <u>VPN</u> Certificates					
DynDNS Backup Reset Upgrade Status System Interfaces VLAN HA VPN Connections	Servers <u>DHCP Server</u> <u>DNS Relay</u>					
System Interfaces VLAN HA VPN Connections	DynDNS Backup Reset					
	System Interfaces VLAN HA VPN Connections					