The Version of Ubuntu in this KM is Ubuntu-11.04-desktop-i386 The DFL FW is v2.40.00.10

[Test Topology] PC1(192.168.1.100)-----(L1:192.168.1.1/24)DFL-2560(W1:PPPoE)-----Internet PC2(192.168.1.66)-----/

PC1 is the Radius server; PC2 is the End User The MAC address of PC2 is 00-21-70-b5-ee-92

The settings of DFL-2560

Setup DFL-Firewall RADIUS Server, the shared secret is "dlink"

D-Link Building Networks for People				Logged in as administrator admin - 192.168.11.168
🛞 Home 🛛 🔣 Configuration 🗸 🛛 🎢 T	ools 🗸 📔 🚳 Statu	s 🗸 🗌 🍇 Maintenar	ice 🗸	😚 Logout 👔 He
DFL-2560 DFL-2560 System Dobjects Dobjects Dobjects Dobjects Dobjects Debjects	General	STV ADIUS server used to veri	y user name	s and passwords.
Bouting DP / IPS DP / IPS Local User Databases Local User Databases Accounting Servers Suser Authentication Rules Authentication Settings Traffic Management D= ZoneDefense	Name: IP Address: Port: Retry Timeout: Shared Secret: Confirm Secret:	radius_srv 192.168.1.100 1812 2	seconds	Notel Existing secret will always be shown with 8 characters to hide the actual length.

Setup the WebUI before rule and change the http port to 8080

Setup and configure methods and	Setup and configure methods and permissions for remote management of this system.						
🎦 Add 🗸 🚀 Advanced settings							
Name 👻	Type 👻	Mode 👻	Interface 🔻	Network 🔫			
🜖 RemoteMgmtHTTP_1	HTTP/HTTPS management	Admin: HTTPS	🛐 any	🗟 all-nets			
🜖 ssh2	Secure Shell Management	Admin: Password, Public Key	🔝 wani	🤤 all-nets			

General			
Setup and cor	figure methods and per	missions for remote management of this system.	
SSH Before Rules:	N	Enable SSH traffic to the firewall regardless of configured IP Rules.	
NebUI Before Rules:	V	Enable HTTP(S) traffic to the firewall regardless of configured IP Rules.	
validation Timeout:	30	Time in seconds to wait for an admin to login before reverting config.	
WebUI HTTP Port:	8080		
WebUI HTTPS Port:	4433		
HTTPS Certificate:	AdminCert		

Setup DFL Firewall User Authentication Rule

D-Link Building Networks for People				Logged in as administrator admin - 192.168.11.168	
S Home 💥 Configuration 🗸 🎢	Tools - Status -	Mainte	nance 🗸 n Rule	🖇 Logout 🔶 ?	He
System System Solects Sules Interfaces	Ceneral Log	Settings	pecifies from v	where users are allowed to authenticate to the system, and how.	
E B IDP / IPS	Name: Authentication agent:	http_auth_ru	le		-
User Authentication	Authentication Source:	RADIUS	~		
External User Databases	Interface:	lan1	~		5
User Authentication Settings	Originator IP: Terminator IP:	all-nets (None)	~	For XAuth and PPP, this is the tunnel originator IP.	
E ZoneDefense	Comments				



Select "MAC authentication" as the Login Type

D-Link [®]	
Building Networks for People	
🗞 Home 🛛 🔣 Configuration 🗸 🛛 👖 To	ols 🗸 🛛 💁 Status 🗸 🔧 Maintenance 🗸
VLAN VLAN VLAN PSec GRE PPPDE PTP/L2TP Servers PTP/L2TP Clents SSL VPN Interface SSL VPN Interface SSL VPN Interface Switch Management Interface Groups ARP/Neighbor Discovery	Nttp-auth-rule The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how. General Log Settings Authentication Options Accounting Agent Options Allow no authentication, Use PAP authentication protocol. Use CHAP authentication protocol. Use MS-CHAP authentication protocol. Use MS-CHAP v2 authentication protocol. We MS-CHAP v2 authentication protocol. We MS-CHAP v2 authentication protocol. We MS-CHAP v2 authentication protocol.
Routing Rules GMP GMP Route Load Balancing Routing Settings GDP / IPS GUE Authentication	Login Type: MAC authentication HTTP Banners: Default Realm String:
Coal User Databases	Allow Clients behind router to connect Allow Clients behind router to connect MAC Auth Secret: Password used to authenticate MAC user, if empty the MAC address will be sent as password. Confirm Secret: Note! Existing secret will always be shown with 8 characters to hide the actual length. Define Secret: HTTPS Certificates

Add an IPv4 address object for authenticated users

D-Link Building Networks for People	
🔄 🌕 Home 🔰 🎇 Configuration 🗸 🕴 🕅	Tools 🗸 🛛 🕤 Status 🗸 🛛 🗞 Maintenance 🗸
DFL-2560 System Objects D-Link_License_SRV D-Link_License_SRV InterfaceAddresses Servers Jan1 ypn	IP4 Address Use an IP4 Address item to define a name for a specific IP4 host, network or range. General User Authentication Image: Ian1_webuser_authed Address: 192.168.1.0/24 Image: Image: User Authentication Image: Image: Image:
ALG with AV/WCF Services Pools NAT Pools Schedules WA uthentication Objects	Comments:

The authed user is "00-21-70-b5-ee-92", or the authed group is "webauthedgroup".

D-Link Building Networks for People	9 	
🍕 Home 🛛 🔣 Configuration 🗸 🗌	T Tool	is 🗸 🛭 💁 Status 🗸 🔧 Maintenance 🗸
Remote Management	*	Use an IP4 Address item to define a name for a specific IP4 host, network or range.
The DHCP DHCP DHCP Misc. Clients The Ardware Monitoring		General User Authentication
Whitelist Advanced Settings Objects		Groups and user names that belong to this network object. Objects that filter on oredentials can only be used as source nets and destination nets in the Rules section. Comma-separated list of user names and groups: 00-21-70-b5-ee-92.webauthedgroup
Address Book	н	No defined oredentials O checking this box specifies that this network object requires user authentication, but that it has no oredentials (user names or groups) defined. This means that the network object
ALT Pools		group membership.
HTTP Banner Files		
8 IP Rules		

Setup the required IP Rules

General	Log Settings	NAT	SAT M	ultiplex SAT	SLB SAT	SLB Monitor
🎒 Gener	al					
Name:	no_auth_sat					
Action:	SAT	~				
Service:	all_services	~				
Schedule:	(None)	~				
Addre	ss Filter					
Specify sou	rce interface and source n	ietwork, toge	ether with desti	nation interface	and destination	network. All parame
	Interface	N	letwork	1000		
Source:	lan1		an1_net	<u> </u>		
	HINEL PPPOE		an-nets			
IP Ru	le a specifies what action to per	form on netw	ork traffic that r	natches the sper	afied filter oriteria.	
IP Ru An IP ruk General	le e specifies what action to per Log Settlings NAT	form on netw T SAT	ork traffic that r	natches the spec	afied filter oriteria. SAT SLB M	lonitors
Bestination An IP Ru General General	IE e specifies what action to per Y Log Settings Y NAT	form on netw	ork traffic that r Multiplex	natches the spec	affied filter ontena. SAT SLB M	lonitors
An IP Ru An IP ruk General General Translate the So	Ie a specifies what action to per Log Settings NAT	form on netw	ork traffic that r	natches the sper	offied filter oriteria.	lonitors
IP Ru An IP ruk General General Translate the So O De	IC e specifies what action to per Log Settings NAT	form on netw	ork traffic that r Multiplex	natches the spec	affied filter oriteria. SAT / SLB N	lonitors
P Ru An IP ruk General General General So De to: New IP A	IC a specifies what action to per Log Settings NAT urce IP stination IP	form on netw	ork traffic that r	SAT SLB	offied filter oriteria. SAT ∕ SLB M	lonitors
IP Ru An IP ruk General General General O General O General O De to: New IP A New Por	Log Settings NAT Log Settings NAT urce IP stination IP Address: lan1_ip t:	form on netw T SAT	ork traffic that r Multiplex	natches the spec SAT Y SLB	affied filter oriteria. SAT SLB N	Ionitors
P Ru An IP ruk General General General General O General New IP A New IP A New Por	le a specifies what action to per Log Settings NAT urce IP stination IP Address: lan1_ip t:	form on netw T SAT	This value gaps to a single IP	natches the spec SAT SLB	sified filter oriteria.	Ionitors
IP Ru An IP ruk General General O General O General O De to: New IP A New Por All-	Log Settings NAT Log Settings NAT uroe IP stination IP Address: lan1_ip tt	form on netw T SAT	This value gaps to a single IP	natches the spec	SAT SLB N	Ionitors
P Ru An IP ruk General General O General O General O General O General New IP A New IP A New Por	le a specifies what action to per Log Settings NAT urce IP stination IP Address: [an1_ip t:	form on netw T SAT	Ork traffic that r Multiplex Multiplex This value gaps to a single IP	natches the spec	ified filter oriteria.	Ionitors
IP Ru An IP ruk General General General O General O General O Ce New IP / New IP / New Por All-	Ie specifies what action to per Log Settings NAT uroe IP stination IP Address: lan1_ip tt to-One Mapping: rewrite all de	form on netw T SAT	Ork traffic that r Multiplex Multiplex This value gaps to a single IP	natches the spec	SAT SLB N	Ionitors

General	Log Settings	NAT	SAT Mul	plex SAT SLB SAT	SLB Monitors
🛐 Gener	al				
Name:	no_auth_allow				
Action:	Allow	~			
Service:	all_services	~			
Schedule:	(None)	~			
Maddre	ss Filter				
Specify sou	rce interface and sour	se network	, together with destina Network	on interface and destination	network. All parameters
Source:	lan1	~	lan1_net	~	
	1	1	1742		

Genera	Log Settings	NAT	SAT M	ultiplex SAT	SLB SAT	SLB Monitors
Gener	al					
Name:	authed_allow					
Action:	NAT	~				
Service:	all_services	*				
Schedule:	(None)	~				
_	-					
Addre	SS FIITER	os natuork	together with dest	ination interface	and destination r	etwork All paramet
opeony sou	Interface	or network	Network	marcon miteridue	and desination in	ernen. en paratitet
Source:	lan1	~	lan1 webuse	er auth		
	1.254270	10000				

👌 Add	👻 🚮 Edit this object						
# 🔻 N	lame -	Action	Source interface	Source network	Destination interface	Destination network	Service
1	g dns_allow	NAT	🔀 lan1	😌 lan1net	Hinet_PPPoE	😌 all-nets	🗑 dns-all
2	authed_allow	NAT	🔝 lan 1	lan1_webuser_authed	Hinet_PPPoE	🖁 all-nets	all_service
3	no_authed_sat	SAT	🔝 lan1	😌 lan1net	Hinet_PPPoE	🖁 all-nets	all_service
4	no_authed_allow	Allow	🔝 lan1	💡 lan1net	Hinet_PPPoE	🔋 all-nets	all_service

The settings of the Radius Server

Install the freeradius

#apt-get install freeradius

Setup the information of radius client(DFL-2560)

#vi	/etc	/freeradius	/clients	conf
#VI	/ כונ	/ II EEI aulus	/ LIIEIILS.	COIII

client 192.168.1.1 {

secret	= dlink

shortname = private-network-test

Setup the group information

#vi /usr/share/freeradius/dictionary
\$INCLUDE dictionary.dlink

Setup the user account and password

/etc/freeradius/users
00-21-70-b5-ee-92 Cleartext-Password := " 00-21-70-b5-ee-92"
D-Link-User-Group = "webauthedgroup"
Note : the user name and password is PC2's MAC address.

#/etc/init.d/freeradius stop
#/etc/init.d/freeradius start
#/etc/init.d/freeradius restart
or
#freeradius -X -i [ip address] -p 1812

End of this document