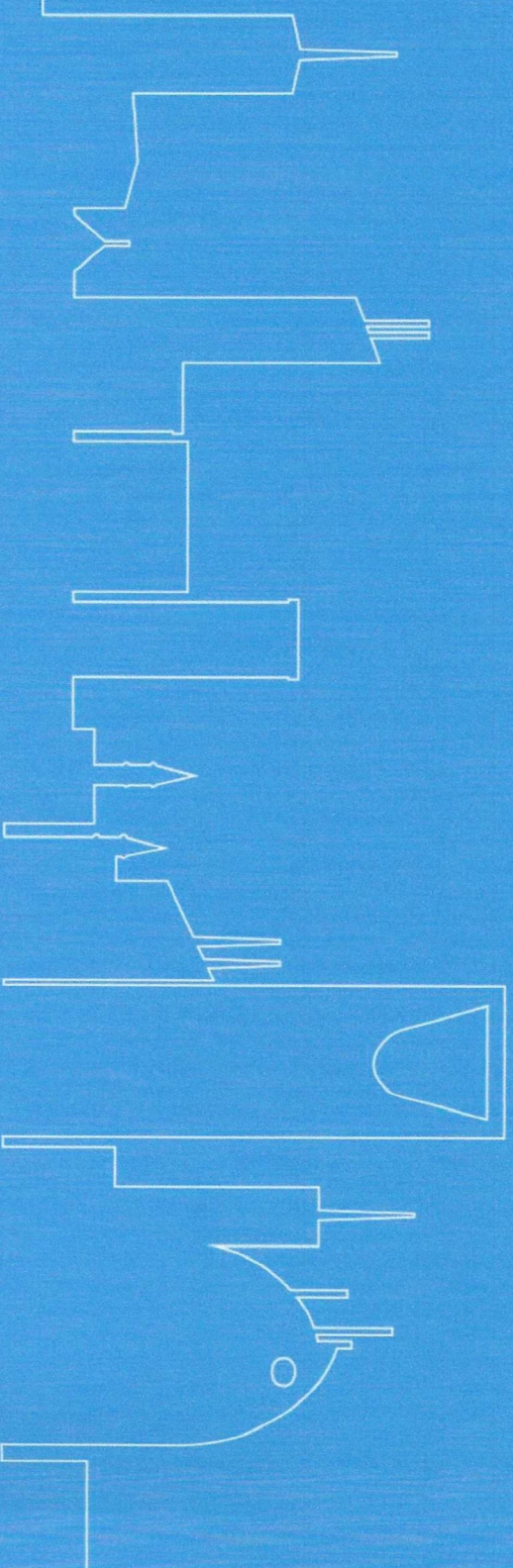
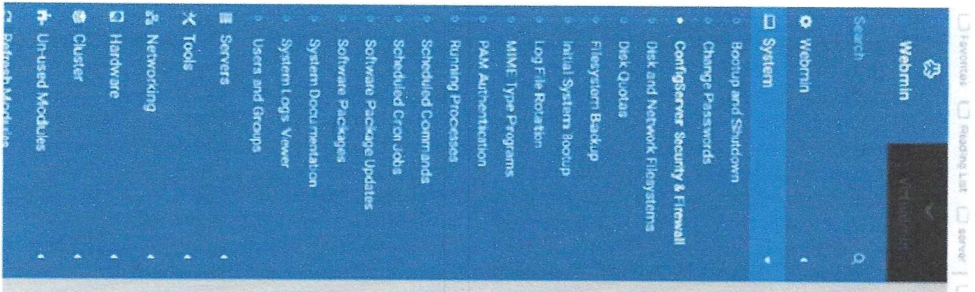


Evidence Document



password	name	email	privilege
6572aea1b8f891952a80854edd1d582e	[REDACTED]	ni@taqnyat.sa	rechargeMenu:
efa82a8e9edb3c027f6b73ee4c309ed4	[REDACTED]	@taqnyat.sa	rechargeMenu:
572661e9761e1f2c4d9fddd768c6b3de	[REDACTED]	@taqnyat.sa	rechargeMenu:
6cfdad10f38174e577bf2c062c00c59	[REDACTED]	@taqnyat.sa	rechargeMenu:
f9eda8b72e8a05cb10e5cea534b3c088	[REDACTED]	@taqnyat.sa	rechargeMenu:
fa231767ae433c50190c3b5fe376fa9a	[REDACTED]	@taqnyat.sa	rechargeMenu:
c70d783bb91e2cblea0b8c36b744c57b	[REDACTED]	@taqnyat.sa	rechargeMenu:
d69140f4d068487b64a88508153ab6e4	[REDACTED]	@taqnyat.sa	rechargeMenu:
9674b2d075bf0f6121d9c21686b6388c	[REDACTED]	@taqnyat.sa	rechargeMenu:
ed70299abf13f3234345dc172fe8f3de	[REDACTED]	@taqnyat.sa	accounting:w.a



Note: This option should **ONLY** be enabled if you know you are under a SYN flood attack as it will slow down all new connections from any IP address to the server if triggered

SYNFLOOD = **Off** ☒

SYNFLOOD RATE = 100/s

SYNFLOOD BURST = 150

Connection Limit Protection. This option configures iptables to offer more protection from DOS attacks against specific ports. It can also be used as a way to simply limit resource usage by IP address to specific server services. This option limits the number of concurrent new connections per IP address that can be made to specific ports.

This feature does not work on servers that do not have the iptables module `xt_connlimit` loaded. Typically, this will be with MONOLITHIC kernels. VPS server admins should check with their VPS host provider that the iptables module is included.

For further information and syntax refer to the Connection Limit Protection section of the `csf/readme.txt`

Note: Run `run /etc/csf/csf test -l` to check whether the option will function on this server

CONNLIMIT =

Port Flood Protection. This option configures iptables to offer protection from DOS attacks against specific ports. This option limits the number of new connections per time interval that can be made to specific ports.

This feature does not work on servers that do not have the iptables module `ipt_recent` loaded. Typically, this will be with MONOLITHIC kernels. VPS server admins should check with their VPS host provider that the iptables module is included.

For further information and syntax refer to the Port Flood Protection section of the `csf/readme.txt`

Note: Run `run /etc/csf/csf test -l` to check whether this option will function on this server

PORTFLOOD = 80tcp/20,50081tcp/20,5

شركة تطوير الحلول

Taqnyat

JEDDAH 40303945715 - RIYADH 1010296254

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow

General Settings

Enable SYN-flood protection ☒

Drop invalid packets ☒

Input	accept	▼
Output	accept	▼
Forward	reject	▼

Routing/NAT Offloading

Experimental feature Not fully compatible with QoS/SQM

Software flow offloading ☐

☒ Software based offloading for routing/NAT

Zones

Zone → Forwardings

	Input	Output	Forward	Masquerading	
lan	accept	accept	accept	☒	Edit Delete
VPD	reject	accept	reject	☒	Edit Delete
VPD	accept	accept	accept	☒	Edit Delete
guest	reject	accept	reject	☐	Edit Delete

Add

Login

Username:

Password:

OTP

Login

Get

شركة تاقنيات

Taqnyat

JEDDAH 4030394715 - RIYADH 1010296254

