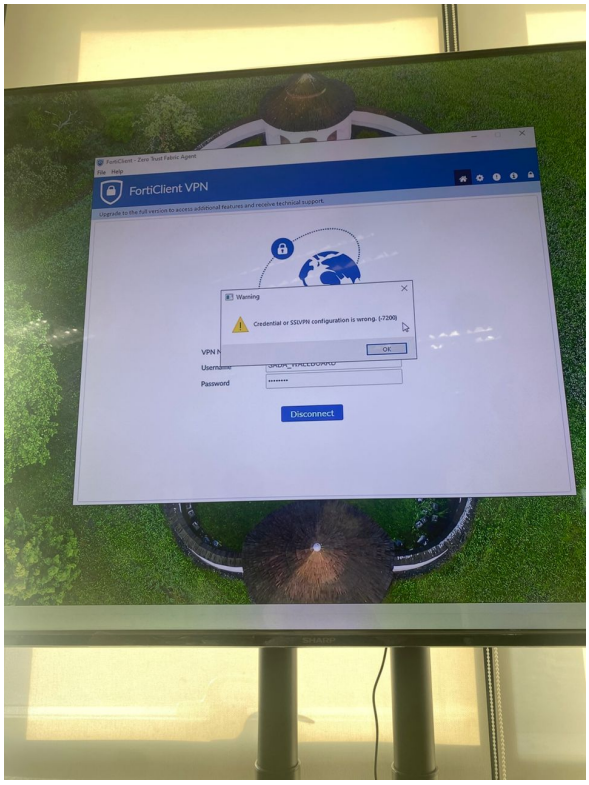
SOUL KATANA

Perkhidmatan Penyelenggaraan Rangkaian Komputer Dan Server Selama Tiga (3) Tahun Untuk Syarikat Air Darul Aman Sdn Bhd (SADA) - SADA/OM/QS/002/11/2/2024

Report Period of 01/01/2025 - 30/06/2025

Date	Description
02/02/2025	Update SSL cert on all firewalls and primera (API Server for SADA-Mobile)
03/02/2025	Wallboard TM Center cannot access from SADA network. Checked and found TM side needs to resuscitate IPSec connection to SADA.



IPsec

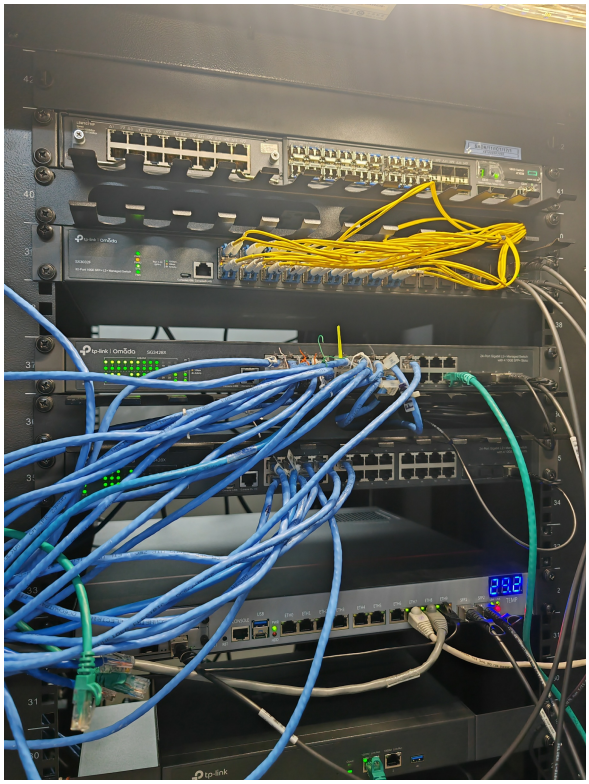
Overview | Tunnels | Mobile

Source	Destination	Description	Status
175.138.111.181	202.162.27.110	TM Support Center	
DMZLEGACY subnet	10.200.13.0/24	TM Support Center	
175.138.111.181	175.136.228.217	Soul Katana	
DMZLEGACY subnet	172.16.9.0/24	DMZLEGACY-LAN	
DMZ subnet	172.16.9.0/24	DMZ-LAN	
DMZLEGACY subnet	172.16.20.0/24	DMZLEGACY-DMZ	
DMZ subnet	172.16.20.0/24	DMZ-DMZ	

05/02/2025	Update SADA-Mobile to version 1.1.4 - Client request to refresh home screen / bill list every time app initiates.
14/02/2025	Upgrade the following switches with additional Omada network controller: 1. Core Switch 2. DMZ Switch x 2

SOUL KATANA

Date	Description



14/02/2025	Readjustment of LANMASTER DHCP range 10.1.0.51-10.1.0.250
19/02/2025	Request to add QR code on printed/PDF bill for corporate customers who've registered e-invoice with LHDN. Code successfully deployed and verified by Amri.

PERINGATAN

1. Pembayaran selain daripada tunai hendaklah dikeluarkan atas nama Syarikat Air Darul Aman Sdn. Bhd. dan dipalang Kira-Kira Penerima sahaja. Bukti Pembayaran hanyalah melalui mesin resit Syarikat Air Darul Aman Sdn. Bhd./ejen lain yang sah.

JENIS BACAAN: N
SILA BAYAR SEBELUM: 13/02/2025

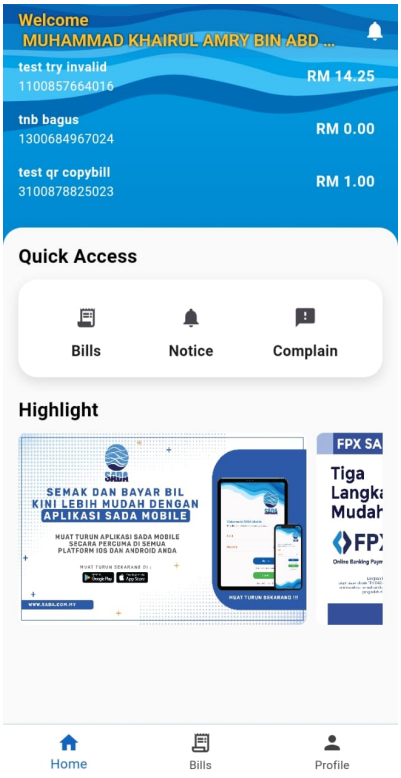
e-Invoice

TUNGGAKAN BIL AIR	:	RM	994,429.80
TUNGGAKAN GST	:	RM	0.00
LAIN-LAIN TUNGGAKAN	:	RM	0.00
JUMLAH TUNGGAKAN	:	**RM**	**994,429.80**
CAJ BULAN SEMASA	:	RM	970,560.50
GST SEMASA	:	RM	0.00
JUMLAH CAJ SEMASA	:	**RM**	**970,560.50**
PELARASAN DEPOSIT	:	RM	0.00
PELARASAN ANGGARAN	:	RM	0.00
PELARASAN GST	:	RM	0.00
JUMLAH PELARASAN	:	**RM**	**0.00**
PENGGENAPAN	:	RM	0.00
JUMLAH PERLU DIBAYAR	:	**RM**	**1,964,990.30**

3251
3100878825023
Nombor Telefon Anda

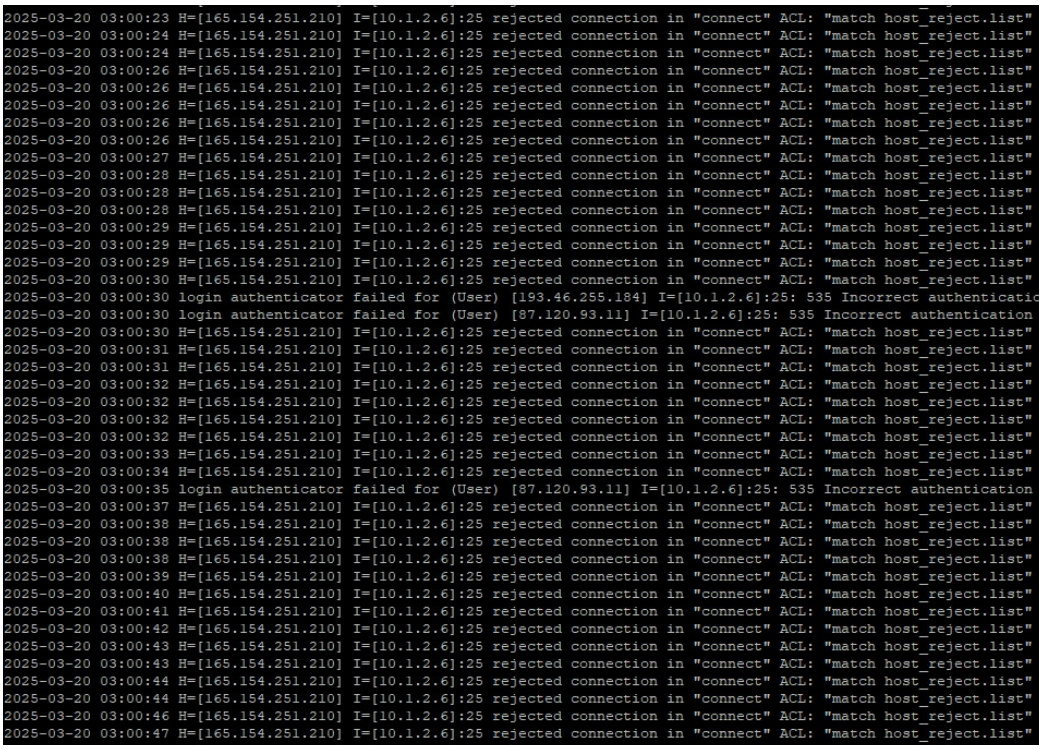
20/02/2025	SADA-Mobile not showing correct current bill if the figure exceeds more than 6 figures. Corrected parsing in code.

SOUL KATANA

Date	Description
	
26/02/2025	Attended to Asyraf to input code that extract the same bill PDF generation API (with QR) from primera to be used on sada fpx web server.
11/03/2025	Upgrade of devices firmware - 1 x Core switch SX3032F v1.0 firmware to 1.0.4 - 2 x DMZ Switch SG3428X v1.30 to 1.30.4
13/03/2025	A user account anisnabila@sada.com.my suspected being hacked. Suspended the account access by changing password. Reported to Amri and Fauzi for further action.
20/03/2025	Identified a host 165.154.251.210 from Singapore came knocking on the email server nonestop. Assigned a subnet block of /24.

SOUL KATANA

Date	Description



```
2025-03-20 03:00:23 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:24 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:24 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:26 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:26 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:26 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:26 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:26 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:27 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:28 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:28 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:28 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:29 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:29 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:29 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:30 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:30 login authenticator failed for (User) [193.46.255.184] I=[10.1.2.6]:25: 535 Incorrect authenticatio
2025-03-20 03:00:30 login authenticator failed for (User) [87.120.93.11] I=[10.1.2.6]:25: 535 Incorrect authentication
2025-03-20 03:00:30 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:31 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:31 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:32 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:32 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:32 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:32 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:33 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:34 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:35 login authenticator failed for (User) [87.120.93.11] I=[10.1.2.6]:25: 535 Incorrect authentication
2025-03-20 03:00:37 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:38 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:38 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:38 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:39 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:40 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:41 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:42 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:43 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:43 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:44 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:44 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:46 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
2025-03-20 03:00:47 H=[165.154.251.210] I=[10.1.2.6]:25 rejected connection in "connect" ACL: "match host_reject.list"
```

20/03/2025

SADA email server having problem reaching yahoo.com directly into the inbox. It's either lost because of bad reputation or sent into spam folder. Attend to backend code of SADA Mobile app to divert email sending routine to another host (aloqstaq.com) if regular expression detects user email domain is yahoo.com:

```
$domain = preg_replace( '!^.+?([^@]+)$!', '$1', $email );

if ($domain != "yahoo.com") {
$mailconfig = $mailconfig;
} else {
$mailconfig = $mailconfig2;
}
```

20/03/2025

The SMTP attack from 165.154.251.210 seems not to be stopping at all. Proceed to block at firewall level.

20/03/2025

Users who have lost the verification email cannot verify hence the verification routine is done only once. To work around this the verification routine is done simultaneously if user use the forget password tool. Once receive email, the user will input password and submit. The process after is to update email_verify_at column simultaneous. Code as follows in login.php:

SOUL KATANA

Date	Description
	// force verify email if user receive email to reset password $dbconnect->query("UPDATE $tableusers SET email_verified_at=NOW() WHERE id='$user_id' AND email_verified_at IS NULL");

25/03/2025	Improved regular expression to detect users with yahoo-wide domains eg: yahoo.com.my, yahoo.com.sg, yahoo.co.uk, etc:
	
	$pattern = '/^[a-zA-Z0-9._%+-]+@([a-zA-Z0-9.-]+\.)?yahoo\.[a-zA-Z]{2,3}(\.[a-zA-Z]{2})?$/';
	
	if (preg_match($pattern, $email)) {
	$mailconfig = $mailconfig;
	} else {
	$mailconfig = $mailconfig2;
	}