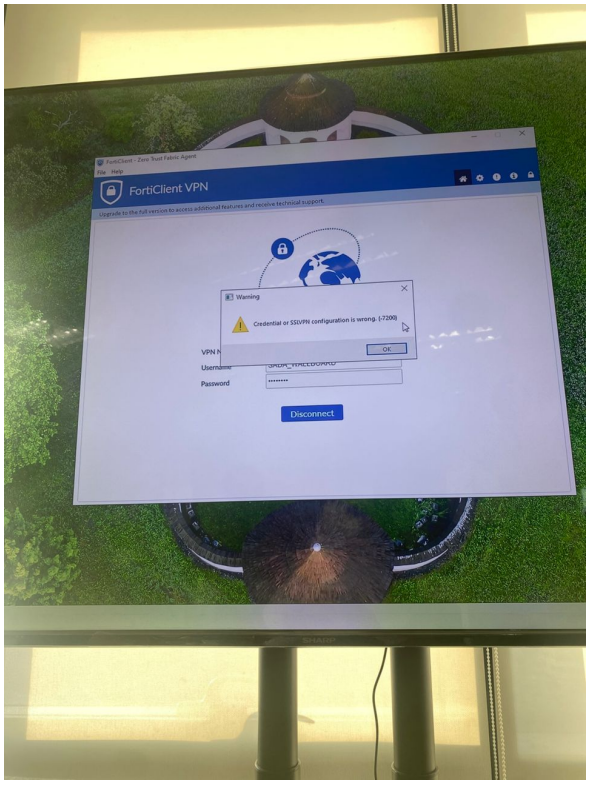
SOUL KATANA

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

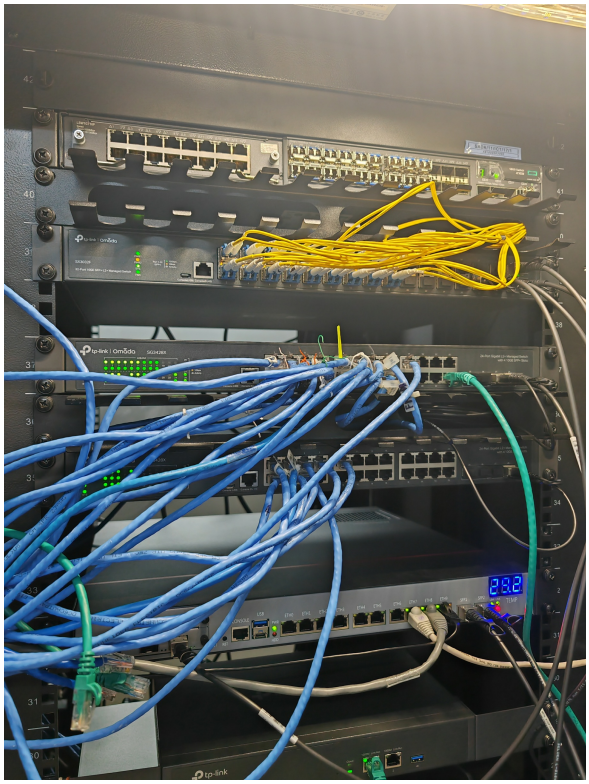
Overview | Tunnels | Mobile

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

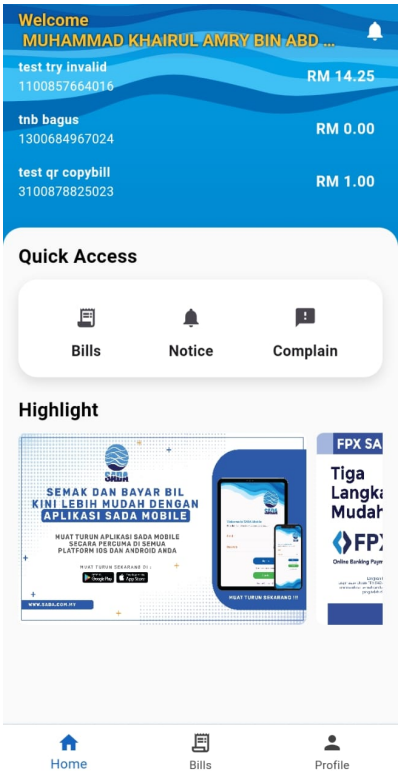
e-Invoice

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

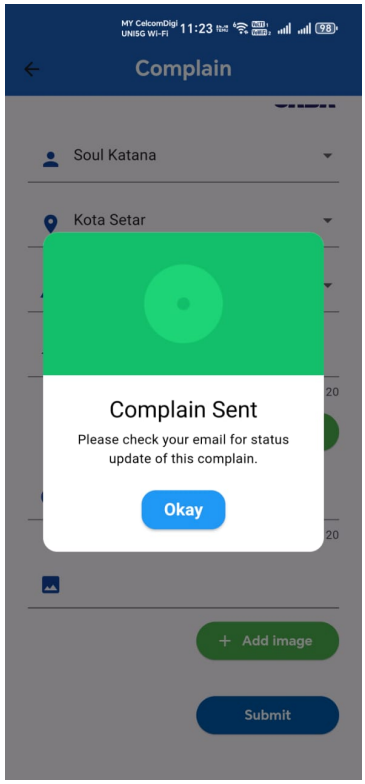
Date	Description
	// force verify email if user receive email to reset password $dbconnect->query("UPDATE $tableusers SET email_verified_at=NOW() WHERE id='$user_id' AND email_verified_at IS NULL");

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;
	}

01/04/2025	Received inquiry from Asyraf about a post on facebook concerning water disruption. The post stated reporting through SADA mobile app was faulty. Checked and confirmed everything functional as is.

SOUL KATANA

Date	Description



10/04/2025	Received request to update IPSec configuration from TM via Fauzi - to change to following 2nd phase subnets: 10.28.8.50/32 10.28.8.51/32 10.28.9.0/24 Once chance/added reverted to Fauzi to ask TM for affective confirmation.

SOUL KATANA

Date	Description

		ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
	Disable	1	V2	U02 202.162.27.110	Mutual PSK -	AES (128 bits)	SHA256	14 (2048 bit)	TM Support Center	

		ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
	Disable	1	tunnel	DMZLEGACY subnet	10.200.13.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	TM Support Center	
	Disable	7	tunnel	DMZLEGACY subnet	10.28.8.50/32	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	TM Support Center	
	Disable	8	tunnel	DMZLEGACY subnet	10.28.9.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	TM Support Center	
	Disable	9	tunnel	DMZLEGACY subnet	10.28.8.51/32	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	TM Support Center	
	+ Add P2									

02/05/2025	VM server built for the purpose of IMAP migration to Office 365 crashed. Rebuild.
13/05/2025	Received request to purge the cache folder of account 1100367818012 from Amri because user did not get bill with QR LHDN attached.
14/05/2025	On the migration purpose-built server, discovered that Office 365 server does not accept login command. The method is no longer suitable for migration. Moving on to the built-in function in Exchange Admin Center. [root@senbonzakura ~]# openssl s_client -connect outlook.office365.com:993 -crlf -quiet depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert Global Root CA verify return:1 depth=1 C = US, O = DigiCert Inc, CN = DigiCert Cloud Services CA-1 verify return:1 depth=0 C = US, ST = Washington, L = Redmond, O = Microsoft Corporation, CN = outlook.com verify return:1 * OK The Microsoft Exchange IMAP4 service is ready. [UwBHADIAUABSADAAMgBDAEEAMAAxADAAMwAuAGEAcABjAHAAcgBkADAAMgAuAHAAcgBvAGQALgBvAHUAdABsAG8AbwBrAC4AYwBvAG0A] ? login najib@sada.com.my @KedahS4D42025 ? NO LOGIN failed. ? logout * BYE Microsoft Exchange Server IMAP4 server signing off. ? OK LOGOUT completed.

SOUL KATANA

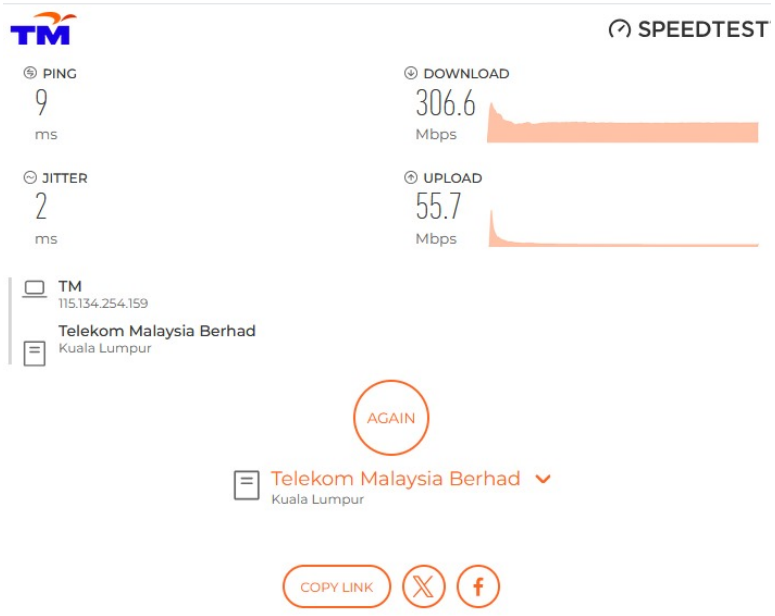
Date	Description
	read:errno=0
14/05/2025	Personnel Amri requested to purge all bill's PDF folder containing 6K+ accounts.
14/05/2025	Tested one account using Exchange Center to migrate and it was successful.
15/05/2025	Appended new SPF record: autodiscover 3600 IN CNAME autodiscover.outlook.com. @ 3600 IN TXT "v=spf1 include:spf.protection.outlook.com -all"
16/05/2025	Reset all user passwords to @KedahS4D42025 for the purpose of migration.
16/05/2025	Migration completed with the following: Migration batch "Migrate-Attempt-02" has some errors Couldn't migrate: Mailboxes - 26 Needs investigation: Mailboxes - 106 Data consistency score: Investigate Apparently 26 accounts do not exists in the legacy email server while the 106 mailboxes containing certain messages that are more than 35MB.
16/05/2025	When migration engaged with multiple pipes representing multiple account logins simultaneously it was discovered the full uplink bandwidth was used. This is for future planning purposes.
24/05/2025	Personnel Amri complained about slow access via the U02 fiber line (Unifi 800Mbps). Went into investigation mode and found that TM is having a minor maintenance that affected the connection slowness. It is also worth noting that the slowness itself made VPN dial into connection an intermittent issue. The following is the test on the fiber service invoked from the firewall: 33 packets transmitted, 25 packets received, 24.2% packet loss round-trip min/avg/max/stddev = 10.120/10.929/12.144/0.749 ms

SOUL KATANA

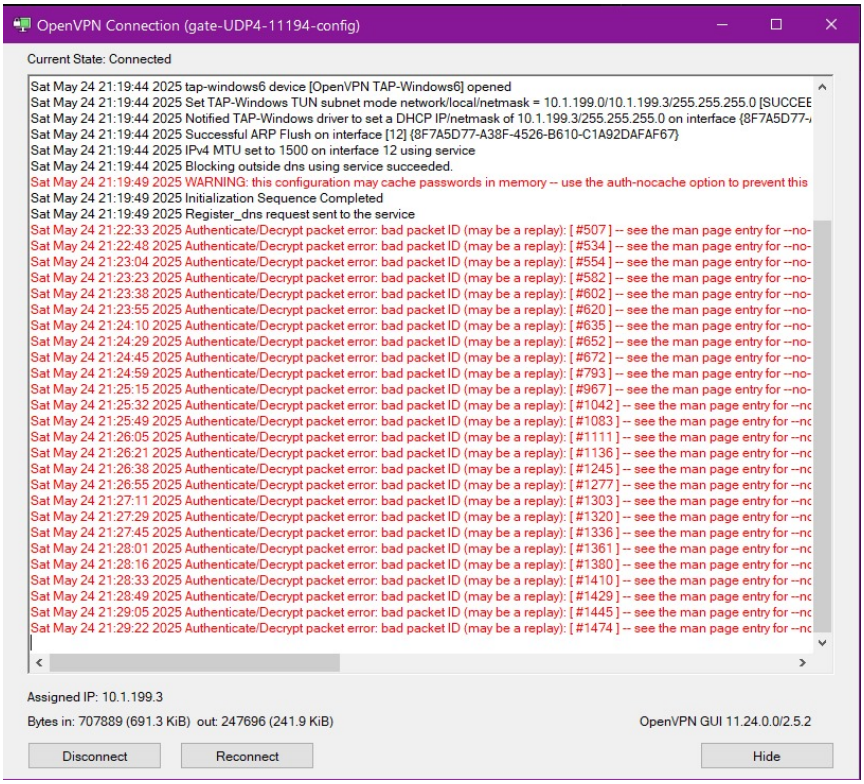
Date	Description

```
C:\Windows\system32>ping 10.34.1.143 -t

Pinging 10.34.1.143 with 32 bytes of data:
Request timed out.
Reply from 10.34.1.143: bytes=32 time=28ms TTL=63
Reply from 10.34.1.143: bytes=32 time=30ms TTL=63
Reply from 10.34.1.143: bytes=32 time=29ms TTL=63
Request timed out.
Reply from 10.34.1.143: bytes=32 time=25ms TTL=63
Reply from 10.34.1.143: bytes=32 time=26ms TTL=63
Request timed out.
Request timed out.
Request timed out.
Reply from 10.34.1.143: bytes=32 time=24ms TTL=63
Reply from 10.34.1.143: bytes=32 time=31ms TTL=63
Reply from 10.34.1.143: bytes=32 time=26ms TTL=63
Reply from 10.34.1.143: bytes=32 time=25ms TTL=63
Reply from 10.34.1.143: bytes=32 time=24ms TTL=63
Request timed out.
Request timed out.
Reply from 10.34.1.143: bytes=32 time=26ms TTL=63
Reply from 10.34.1.143: bytes=32 time=28ms TTL=63
Reply from 10.34.1.143: bytes=32 time=26ms TTL=63
Request timed out.
Reply from 10.34.1.143: bytes=32 time=30ms TTL=63
Request timed out.
Reply from 10.34.1.143: bytes=32 time=27ms TTL=63
Request timed out.
Reply from 10.34.1.143: bytes=32 time=30ms TTL=63
Reply from 10.34.1.143: bytes=32 time=25ms TTL=63
Reply from 10.34.1.143: bytes=32 time=30ms TTL=63
Reply from 10.34.1.143: bytes=32 time=26ms TTL=63
Request timed out.
```

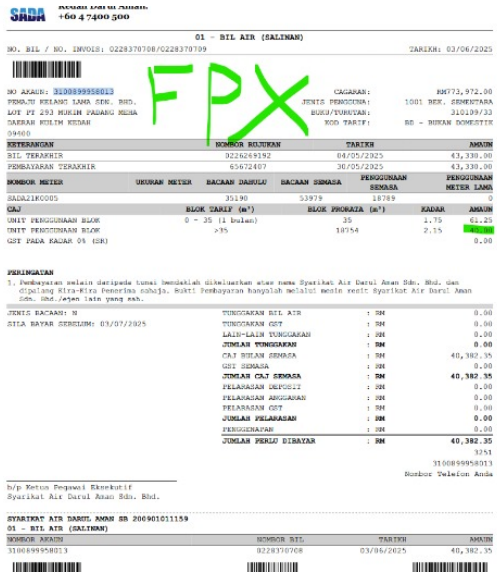


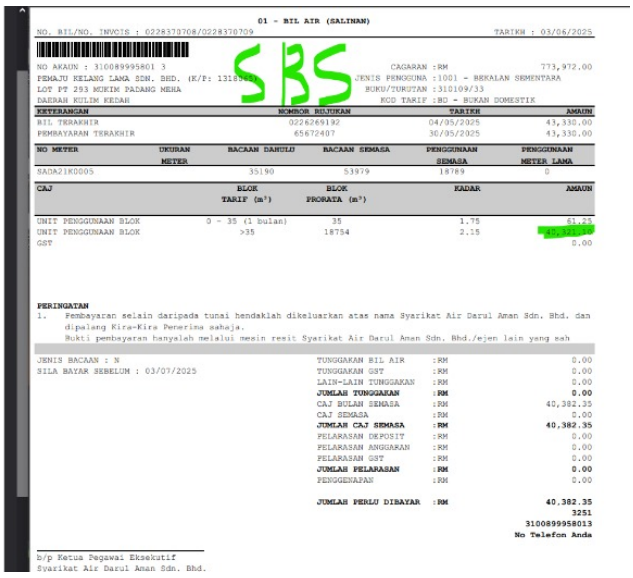
SOUL KATANA

Date	Description
	
25/05/2025	Personnel Amri requested to add another IP (10.1.2.23) into the 'allowed-access' list for IFAS users. IFAS users will add the following host locally to access the system from their end: http://sadaappvm/RMA
26/05/2025	It is discovered that the 365 server do not allow unauthenticated connection for on-the-fly SMTP connection from the servers hosting eaduan: Failed to authenticate on SMTP server with username "eaduan@sada.com.my" using 2 possible authenticators. Authenticator LOGIN returned Expected response code 235 but got code "535", with message "535 5.7.139 Authentication unsuccessful, user is locked by your organization's security defaults policy. Contact your administrator. [KU0P306CA0031.MYSP306.PROD.OUTLOOK.COM 2025-05-29T02:32:28.618Z 08DD9E059AC6E01C] ". Authenticator XOAUTH2 returned Expected response code 235 but got code "535", with message "535 5.7.3 Authentication unsuccessful [KU0P306CA0031.MYSP306.PROD.OUTLOOK.COM 2025-05-29T02:32:38.961Z 08DD9E059AC6E01C] ". Prepared an external SMTP server *.aloqstaq.com to temporary host the service.
04/06/2025	Added the following DNS lines in BIND configuration (10.1.2.3) to alternate online public services if DOM uplink goes down: ;; Essential public-related services ;; There are 2 lines for each subdomains ;; Only 1 line for this domain supposed to be in use - depending on which uplink is available ;; Comment one line and uncomment another depending on which uplink available

SOUL KATANA

Date	Description
	primera IN A 58.27.58.168 ; if DOM is up ;primera IN A 175.138.111.181 ; if DOM is down ;; Only 1 line for this domain supposed to be in use - depending on which uplink is available smapi IN A 58.27.58.164 ; if DOM is up ;smapi IN A 175.138.111.182 ; if DOM is down
16/06/2025	Request from personnel Amri to sync account azminabazli@sada.com.my to Office 365
17/06/2025	Fix tariff table of the 2nd tear block in the copybill.





23/06/2025	Personnel Amri requested to purge the PDF storage of account no 3200851438014