Group Media Contact IT Network Assessment Report

March 2020

Table of contents

1. INTRODUCTION

As per the TIC-IT's proposal to Group Media Contact, on the 5th March 2021, articulating our value proposition with respect to IT Network Infrastructure services for Group Media Contact (GMC), TIC-IT Telecoms subsequently conducted an IT Network Assessment of the GMC environment.

2. SCOPE OF THE ASSESSMENT

This report details TIC-IT Telecoms' findings and recommendations of the GMC's network Infrastructure environment. The Remote assessment was completed between the 06th – 12th March 2021. The Senior Network Security Consultant from TIC-IT conducted the IT network assessment. The scope of assessment can be summarised as follows:

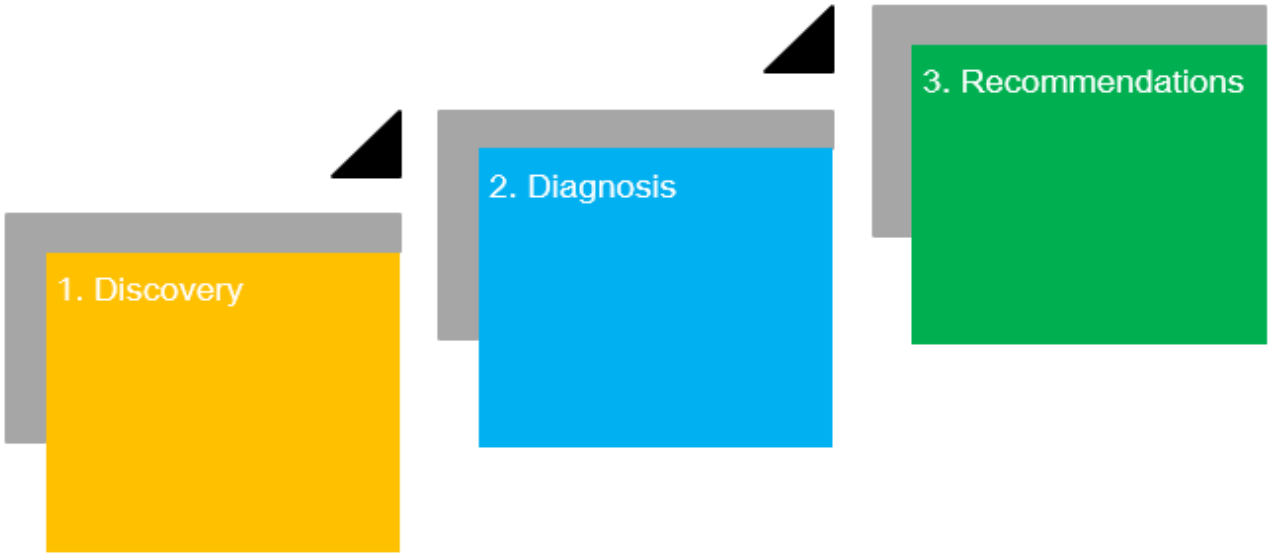
a) Management Plane

b) Control Plane

c) Data Plane

3. APPROACH ARTEFACTS

TIC-IT Telecoms' approach to conducting assessments, is underpinned by three (3) key assessment artefacts, to ensure that the outputs of our work is authentic and actionable under the Management , Control and Data plane of the network devices.



The key activities performed by TIC-IT Telecoms at each stage of the assessment are outlined hereunder;

1) Discovery:
   - Design documents collection
   - Network configuration extraction

2) Diagnosis:
   - Benchmark end to end network environment against industry best practice.

3) Recommendations:
   - Document significant issues and actionable recommendations across the network technology stack and value chain.
   - Develop a network assessment report detailing the findings and areas of improvement
   - Presentation of the network assessment report to GMC.

4. NETWORK ARCHITECTURE DESIGN

GMC has effected collapsed/distribution network architecture design at a Local Area Network level, underpinned by a HP switches, Cisco switches and routers, and Cisco firewall device.

5. FIREWALL

Management Plane

a) Password-recovery
Finding It was observed that the ASA firewall have service password recovery enabled
Risk & Impact Password recovery prevent an attacker that have physical access to firewall to reset firewall password.
Recommendation Disable password-recovery.
Duration to remediate One day.

b) Password Policy
Finding It was observed that the ASA firewall have no password policy enabled.
Risk & Impact Password policy helps to prevent unauthorized accesses by enforcing the policy for more complexity and making them difficult to be guessed.
Recommendation Enable password policy.
Duration to remediate 1 day.

c) Domain name
Finding It was observed that the ASA firewall is configured with no domain.
Risk & Impact The domain name is import during the deployment of RSA keys and certificate
Recommendation Configure domain name.
Duration to remediate 1 day.

d) No HA
Finding It was observed that the ASA firewall is no configured with HA.
Risk & Impact Enable failover to achieve High availability
Recommendation Procure another firewall and configure HA
Duration to remediate 6 months

e) Local AAA rules
Finding It was observed that the ASA firewall is no configured with AAA rules.
Risk & Impact AAA rules limits number of the times a local user can enter a wrong password before being locked out. This protect against brute force and dictionary attacks.
Recommendation Enable local authentications attempts.
Duration to remediate 1 day.

f) AAA authentication enable console
Finding It was observed that the ASA firewall is no configured with aaa authentication enable console.
Risk & Impact This authenticate users who is trying to access the Enable mode through the enable command.
Recommendation Configure aaa authentication enable console
Duration to remediate 1 day

g) AAA command authorization
Finding It was observed that the ASA firewall is no configured with aaa command authorization.
Risk & Impact Required authorization for commands enforce separation of duties.
Recommendation Configure aaa command authorization local
Duration to remediate 1 day

h) AAA authorization exec
Finding It was observed that the SA firewall is no configured with aaa authorization exec.
Risk & Impact Required authorization for exec enforce separation of duties.
Recommendation Configure aaa authorization exec authentication-server
Duration to remediate 1 day

i) AAA command accounting
Finding It was observed that the ASA firewall is no configured with command accounting.
Risk & Impact The ensure accountability.
Recommendation Configure aaa command accounting local
Duration to remediate 1 day

j) AAA accounting for SSH, Exec and Serial
Finding It was observed that the ASA firewall is no configured with aaa accounting for ssh,Exec, and serial.
Risk & Impact The ensure accountability.
Recommendation Configure aaa accounting ssh/serial/Exec console local
Duration to remediate 1 day

k) Banner
Finding It was observed that the ASA firewall is no configured with banner
Risk & Impact Banner are used to deter hackers by letting them know that their access is illegitimate and the possible consequence of going further.
Recommendation Configure banner for both Exec , MOTD, Login and ASDM.
Duration to remediate 1 day

l) SCP
Finding It was observed that the ASA firewall is no configured with SCP for files transfer.
Risk & Impact SCP ensures that files are transfer is secure.
Recommendation Configure scp.
Duration to remediate 1 day

m) Enable TLS 1.0

Finding

It was observed that the ASA firewall is no configured with TLS 1.X

Risk & Impact

SSL it has many security vulnerabilities and its been replace by TLS.

Recommendation

Configure TLS 1.X and disable SSL

Duration to remediate

1 day

n) Session timeout

Finding

It was observed that the ASA firewall is no configured with console and http session timeout.

Risk & Impact

Limiting session timeout prevents unauthorized users from using abandoned session.

Recommendation

Configure console and http session timeout.

Duration to remediate

1 day

o) NTP servers

Finding

It was observed that the ASA firewall is no configured with ntp server.

Risk & Impact

NTP server ensures accurate logging time.

Recommendation

Configure ntp server

Duration to remediate

1 day

p) Local timezone
Finding It was observed that the ASA firewall is no configured with correct local timezone.
Risk & Impact Local timezone ensures that relevant time stands when logging information
Recommendation Configure timezone.
Duration to remediate 1 day

q) Logging
Finding It was observed that the ASA firewall is no configured with Syslog servers , logging timestamp, and logging buffer.
Risk & Impact Syslog servers ensures that logs are save centrally and review for accounting and monitoring. Logging timestamp ensure accurate logging timestamp.
Recommendation Configure syslog and logging timestamp
Duration to remediate 1 day

r) SNMP
Finding It was observed that the ASA firewall is configured with default SNMP community/traps , snmp-server.
Risk & Impact SNMP ensures that are monitored via NMS.
Recommendation Configure snmp v3 , traps and snmp server and disable default snmp community strings.
Duration to remediate 1 day

Control Plane

s) DHCP services
Finding It was observed that the ASA firewall is configured with dhcp services.
Risk & Impact This services is not required because firewall no users is using it.
Recommendation Disable dhcp services.
Duration to remediate 1 day

t) DNS Guard
Finding It was observed that the ASA firewall is configured with dhcp services.
Risk & Impact This services is not required because firewall no users is using it.
Recommendation Disable dhcp services.
Duration to remediate 1 day

u) ICMP is restricted
Finding It was observed that the ASA firewall is not configured to deny icmp from outside
Risk & Impact This services is not required because firewall no users is using it.
Recommendation Create icmp policy deny icmp request from outside.
Duration to remediate 1 day

Data Plane

a) DoS protection
Finding It was observed that the ASA firewall is not configured with DoS protection.
Risk & Impact Limiting the number of connections protects from DoS attacks
Recommendation Configure the maximum connections , embryonic , connections per clients and embryonic per client that can be accepted from outside interface.
Duration to remediate 2 days

b) IP Spoofing
Finding It was observed that the ASA firewall is not configured with ip spoofing protection.
Risk & Impact This protected the ip spoofing
Recommendation Configure unicast Reserve-Path Forwarding on untrusted interface.
Duration to remediate 2 days

c) Botnet Protection
Finding It was observed that the ASA firewall is not configured with botnet protection.
Risk & Impact Filter Botnet traffic on the untrusted interface
Recommendation Configure dynamic-filter on untrusted interface. This requires dns working.
Duration to remediate 2 days

Supportability and Maintainability

a) EOL and ESO
Finding It was observed that Firewall ASA 5520 end of life and support.
Risk & Impact Having legacy equipment in a network layer can impact business operations and "", in the event of network core failure. Legacy network platform also impact on ability of the organisation to optimise the network and introduce new technologies at the local network layer.
Recommendation It is recommended that the Firewall be replaced with new generation equipment. The new firewall will enhance performance of the network as well as enable introduction of security technologies, such as IPS,VPN,etc.
Duration to remediate The new firewall can be procured and implemented within 6 months.

Network Security

Replace firewalls with a next-generation firewall.

Remediation Services

Deploy a datacenter firewall to protect the datacenter servers

6 SWITCHES and ROUTERS

Management Pane

a) Shared account
Finding It was observed that administrators are using shared account
Risk & Impact Shared account creates issues of accountability.
Recommendation Create user accounts for each administrator.
Duration to remediate 3 day.

b) Password-recovery
Finding It was observed that switches and routers have service password recovery enabled.
Risk & Impact Password recovery prevent an attacker that have physical access to network to reset switches and routers password.
Recommendation Disable password-recovery.
Duration to remediate 1 day.

c) Password Policy
Finding It was observed that not all switches and routers all have password policy enabled.
Risk & Impact Password policy helps to prevent unauthorized accesses by enforcing the policy for more complexity and making them difficult to be guessed.
Recommendation Enable password policy , 'password' for 'enable secret', and 'service password-encryption', 'username secret' for all local users
Duration to remediate 1 day.

d) Domain name
Finding It was observed that not all switches and routers are not configured with domain.
Risk & Impact The domain name is import during the deployment of RSA keys and certificate
Recommendation Configure domain name.
Duration to remediate 4 day.

e) aaa new-model
Finding It was observed that not all switches and routers are configured with 'aaa new-model'
Risk & Impact Rules in the Local authentication, authorization and accounting (AAA) configuration class enforce device access control, provide a mechanism for tracking configuration changes, and enforcing security policy.
Recommendation Enable 'aaa new-model'.
Duration to remediate 1 day.

f) Remote AAA servers
Finding It was observed that not all switches and routers are configured with remote AAA servers.
Risk & Impact Remote AAA servers create central management of the AAA services
Recommendation Configure AAA servers and AAA policy on all routers and switches
Duration to remediate 3 months

g) 'aaa authentication login and enable'
Finding It was observed that not all switches and routers are configured with 'aaa authentication login/enable'.
Risk & Impact This authenticate users who is trying to access the Enable mode through the enable command.
Recommendation Configure 'aaa authentication login/enable'
Duration to remediate 3 day

h) login authentication for 'line con 0' and line vty
Finding It was observed that not all switches and routers are not configured with 'login authentication for 'line con 0' and live vty
Risk & Impact This authenticate users who is trying to access the switches and routers through the serial console port and line vty.
Recommendation Configure 'login authentication for 'line con 0' and line vty
Duration to remediate 2 day

i) AAA command authorization
Finding It was observed that not all switches and routers are configured with command authorization.
Risk & Impact Required authorization for commands enforce separation of duties.
Recommendation Configure aaa command authorization
Duration to remediate 2 day

j) AAA authorization exec
Finding It was observed that not all switches and routers are configured with authorization exec.
Risk & Impact Required authorization for exec enforce separation of duties.
Recommendation Configure aaa authorization exec authentication-server
Duration to remediate 1 day

k) AAA command and exec accounting
Finding It was observed not all switches and routers are configured with command and exec accounting.
Risk & Impact The ensure accountability.
Recommendation Configure command accounting local
Duration to remediate 2 day

l) Banner
Finding It was observed that not all switches and routers are configured with banner
Risk & Impact Banner are used to deter hackers by letting them know that their access is illegitimate and the possible consequence of going further.
Recommendation Configure banner
Duration to remediate 2 day

m) Secure management protocols
Finding It was observed that that not all switches and routers uses the secure management protocols.
Risk & Impact Ensures that management connection secure.
Recommendation Disable http,telnet and enable SSH version 2 and HTTPS.
Duration to remediate 2 day

n) Authorized Management IP address

Finding

It was observed that switches and routers are not configured with authorized management ip address.

Risk & Impact

ACLs control what addresses may attempt to log in to the routers and switches. By default any may connect to routers

Recommendation

Configure authorized management ip address

Duration to remediate

2 day

o) Session timeout

Finding

It was observed that some switches and routers are not configured with session timeout.

Risk & Impact

Limiting session timeout prevents unauthorized users from using abandoned session.

Recommendation

Configure console,exec , line vty and https session timeout.

Duration to remediate

2 day

p) Set 'transport input none' for 'line aux 0'
Finding It was observed that some switches and routers are not configured with 'transport input none' for 'line aux 0'.
Risk & Impact Unused ports should be disabled, if not required, since they provide a potential access path for attackers.
Recommendation Configure transport input none on line aux
Duration to remediate 2 day

q) NTP servers
Finding It was observed that all switches and routers are not configured with ntp server.
Risk & Impact NTP server ensures accurate logging time.
Recommendation Configure ntp server
Duration to remediate 2 day

r) Local timezone
Finding It was observed that nor all routers and switches are configured with correct local timezone.
Risk & Impact Local timezone ensures that relevant time stands when logging information
Recommendation Configure timezone.
Duration to remediate 2 day

s) Logging
Finding It was observed that not all switches and routers are configured with Syslog servers , logging timestamp, logging enabled and logging buffer.
Risk & Impact Syslog servers ensures that logs are save centrally and review for accounting and monitoring. Logging timestamp ensure accurate logging timestamp.
Recommendation Configure syslog, enabled logging, logging buffer , logging console , logging trap information , logging timestamp, logging source interface and login success/failure logging
Duration to remediate 2 day

t) SNMP
Finding It was observed some switches and routers are configured with default SNMP community/traps , snmp-server.
Risk & Impact SNMP ensures that are monitored via NMS.
Recommendation Configure snmp v3 , traps and snmp server and disable default snmp community strings.
Duration to remediate 2 day

u) SNMP ACL
Finding It was observed all switches and routers are not configured with SNMP ACL.
Risk & Impact SNMP ACL restrict only NMS access.
Recommendation Configure SNMP ACL.
Duration to remediate 7 day

Control Plane

a) Set maximimum value for 'ip ssh authentication-retries'

Finding

It was observed that some switches and routers are not configured with ssh authentication retries.

Risk & Impact

This limits the number of times an unauthorized user can attempt a password without having to establish a new SSH login attempt.

Recommendation

Configure ssh authentication retries

Duration to remediate

2 day

b) CDP

Finding

It was observed that some switches and routers are configured with cdp run.

Risk & Impact

CDP should be completely disabled unless necessary.

Recommendation

Disable cdp.

Duration to remediate

2 day

c) bootp server

Finding

It was observed that some switches and routers are configured with bootserver.

Risk & Impact

BootP allows a router to issue IP addresses.

Recommendation

Disable bootserver.

Duration to remediate

3 day

d) Disable unwanted services

Finding It was observed that some switches and routers are configured with default services
Risk & Impact This create large attack vector.
Recommendation Disable unwanted services
Duration to remediate day

Data Plane

a) Routing Rules
Finding It was observed not all routers are configured with correct routing rules.
Risk & Impact Disable the handling of IP datagrams with source routing header options.
Recommendation Set 'no ip source-route'
Duration to remediate 2 days

b) Proxy ARP
Finding It was observed that not all routers have arp proxy enabled .
Risk & Impact Proxy ARP is a service where a device connected to one network (in this case the Cisco router) answers ARP Requests which are addressed to a host on another network, replying with its own MAC Address and forwarding the traffic on to the intended host.
Recommendation Disable proxy arp.
Duration to remediate 2 days

c) Routing protocol Authentication

Finding It was observed that layer 3 devices are not configured with routing protocol authentication .
Risk & Impact Organizations should plan and implement enterprise security policies that require rigorous authentication methods for routing protocols.
Recommendation Configure routing protocol authentication
Duration to remediate 2 days

Supportability and Maintainability

a) EOL and ESO
Finding It was observed that Some switches and switches are end of life and support.
Risk & Impact Having legacy equipment in a network layer can impact business operations and "", in the event of network core failure. Legacy network platform also impact on ability of the organisation to optimise the network and introduce new technologies at the local network layer.
Recommendation It is recommended that the GMC replaced old equipment.
Duration to remediate The new firewall can be procured and implemented within 6 months.

Network Security

a) Virtual LAN setup and Configuration
Finding It was observed that GMC is using vlan 1 for management, users , IoT and servers.
Risk & Impact One increase collision domain and it is best practice to have different vlan for users, IoT and Servers
Recommendation It is recommended that the virtual network setup and configuration is reviewed and implemented adequately in line with best practice. The ideal configuration structure is to one to one ratio, one VLAN one subnet.
Duration to remediate 2 months

b) Servers are no protected by datacentre firewalls
Finding It was observed that GMC servers are not protected by firewall.
Risk & Impact Firewalls protects servers by only allowing required services and ensures that IoT cant access servers.
Recommendation Procure data center firewall to protect servers
Duration to remediate 4 months

c) Network Architecture Diagram
Finding The current network architecture diagram does not represent the current network setup
Risk & Impact The updated network architecture diagram assists in troubleshooting and network management
Recommendation Update the current network architecture diagram to reflect the current network setup
Duration to remediate 1 week

d) Network Device Policy and Standard
Finding We found that devices are inconsistently configured.
Risk & Impact Inconsistent security measures in devices.
Recommendation Create the policy, standard , guidelines, baselines and procedures for all devices
Duration to remediate 2 months

6. CONCLUSION

We recommend that GMC remediate the findings as recommended by this report.

7. CONTACT DETAILS

TIC-IT Telecoms		
Names:	Bashi MaKhafola	John Kgorutle
Tel:	+27 87 121 0040	
Cell:	+ 27 73 023 2414	+27 (0) 67 146 2978
Email:	bmakhafola@tic-it.co.za	jkgorutle@tic-it.co.za
Address:	197 Smit Street, Fairlands, Johannesburg	