

Connectivity Services Quotation

Reference Number: 014-01-2022

**Malawi Internet Service
Providers Association - MISPA**

Date: 14th January, 2022



**simpler.
seamless.
solutions.**

Chairperson, MISPA,
Malawi Internet Service Providers Association - MISPA,
C/O Malawi SDNP,
Polytechnic Road,
P.O. Box 31762,
Chichiri,
Blantyre 3

14th January 2022

Attention: Dr Paulos B. Nyirenda,

Please find below our quotation for 100Mbps, 200Mbps and 250Mbps dedicated Internet Services to be terminated at your offices in Blantyre and a statement on CDN Management at the MIX.

1. Pricing

No.	Description	Quantity	Unit Charge (MK)	Total Monthly Cost (MK)
1	Option A: 100Mbps Dedicated Internet Services	100	32,400.00	4,152,060.00
2	Option B: 200Mbps Dedicated Internet Services	200	28,350.00	7,266,105.00
3	Option C: 250Mbps Dedicated Internet Services	250	24,300.00	7,785,112.50
4	CDN Management	1	243,000.00	283,095.00
5	Installation and Configurations	Once Off		330,277.50

NOTE:

- Prices above are inclusive Government 10% Excise and 16.5% Value Added Tax.

2. Statement on how inq can manage the CDNs at the MIX

inq Digital will provide a centralized Universal Client Premise Equipment (UCPE) Managed Services router which will be helping in troubleshooting, monitoring, controls has abilities such as and not limited to provide;

Managed Services – Also has Firewall capabilities for security, monitor and internet usage, blocking sites, to avoid abuse and more. We can be able to onboard and off board any services and functionalities which can be required at the MIX seamlessly.

The UCPE has Unified threat management (UTM) refers to when multiple security features or services are combined into a single device within your network. Using UTM, your network's users are protected with several different features, including antivirus, content filtering, email and web filtering, anti-spam, and more.

UTM enables an organization to consolidate their IT security services into one device, potentially simplifying the protection of the network. As a result, your business can monitor all threats and security-related activity through a single pane of glass. In this way, you attain complete, simplified visibility into all elements of your security or wireless architecture.

Desired Features of a Unified Threat Manager - There are certain features that an ideal UTM solution must possess.

- a) **Antivirus** - A UTM comes with antivirus software that can monitor your network, then detect and stop viruses from damaging your system or its connected devices.
- b) **Anti-malware** - Unified threat management protects your network against malware by detecting it and then responding. A UTM can be preconfigured to detect known malware, filtering it out of your data streams and blocking it from penetrating your system.
- c) **Firewall (if needed)** - A firewall has the ability to scan incoming and outgoing traffic for viruses, malware, phishing attacks, spam, attempts to intrude on the network, and other cybersecurity threats. Because UTM firewalls examine both the data coming in and out of your network, they can also prevent devices within your network from being used to spread malware to other networks that connect to it.
- d) **Intrusion Prevention** - A UTM system can provide an organization with intrusion prevention capability, which detects then prevents attacks. This functionality is often referred to as an intrusion detection system (IDS) or intrusion prevention system (IPS). To identify threats, an IPS analyzes packets of data, looking for patterns known to exist in threats. When one of these patterns is recognized, the IPS stops the attack.
- e) **Virtual Private Networking (VPN)** - The virtual private network (VPN) features that come with a UTM appliance function similarly to regular VPN infrastructure. A VPN creates a private network that tunnels through a public network, giving users the ability to send and receive data through the public network without others seeing their data. All transmissions are encrypted, so even if someone were to intercept the data, it would be useless to them.
- f) **Web Filtering** - A UTM's web filtering feature can prevent users from seeing specific websites or Uniform Resource Locators (URLs). This is done by stopping users' browsers from loading the pages from those sites onto their device.
- g) **Data Loss Prevention** - The data loss prevention you get with a UTM appliance enables you to detect data breaches and exfiltration attempts and then prevent them.

Benefits of Using a Unified Threat Management Solution

Flexibility and Adaptability - With a UTM network, you can use a set of flexible solutions to handle the complicated assortment of networking setups available in modern business infrastructure. You can cherry-pick what you need from a selection of security management tools, choosing what is best for your specific network. You can also opt to obtain one licensing model that comes with all the technologies you want, saving you time shopping for individual solutions.

Centralized Integration and Management - In a normal setup without UTM, you may have to juggle several security components at once, including a firewall, application control, a VPN, and others. This can take time and resources away from your team. However, with a UTM, you can consolidate everything and control it all with a single management console. This makes it easier to monitor the system, as well as address particular components within the UTM that may need to be updated or checked.

The centralized nature of a UTM also allows you to monitor several threats simultaneously as they impact multiple components of your network. In a network without this centralized structure, when a multi-module attack is occurring, it can be very difficult to prevent it.

Cost-effectiveness - Because of its centralized setup, a UTM reduces the number of devices your organization needs to protect your network. This may result in significant cost savings. In addition, because fewer staff are required to monitor the system, you can save on manpower costs as well.

Increased Awareness of Network Security Threats - The combination of a UTM's centralization and faster operation results in an increased awareness of network security threats, enabling you to implement advanced threat protection (ATP).

Faster Security Solution for Businesses - With a UTM, you can streamline the way data is processed and use fewer resources at the same time.

NETWORK MANAGEMENT AND MONITORING

inq. Digital Limited has a Network Operations Centre (NOC) located in Blantyre and Lilongwe that monitors the **inq. Digital Limited's** infrastructure. In addition, the NOC has network management experts that are available during working hours and on stand-by during non-working hours, holidays and weekends.

FAULT MANAGEMENT

Troubleshooting and assisting clients connected to the router/MIX with any issues they may be facing. We have a highly experienced and resourced NOC, with engineers on hand to assist with any configurations on various hardware platforms.

The Customer is encouraged to log tickets with our 24x7x365 call centre when they are experiencing Network problems (Call Centre hotline: 01-820 200, Email: helpdesk-mw@inq.inc). Likewise, the call centre will always log tickets on behalf of the Client so as to ensure the problem is resolved in time through the traceable ticket number.

We believe the quotation is well within your expectations. If you require additional clarification/information please do not hesitate to contact the undersigned.

Kind Regards,

Feason Masowa
Solution Sales Representative
Tel: + 265 (0) 999 963 754
Mail: feason@inq.inc
Web: www.inq.inc