MountainBox iDiG 2.0

Technical White Paper

iDiG 2.0

At last an Internet Solution tailored for SMMEs as well as Corporates with small and medium sites!

Turning "Best Effort" Networks into Great Networks!

The MountainBox iDiG2.0 (Intelligent Dynamic Internet Gateway) takes the best of global practice and applies it locally to address the specific needs of South African small - medium sites, requiring consistent levels of security, network availability and management, such as enjoyed by Head Office and Regional Sites - at a price break they (the smaller sites) can afford.

We consider a smaller site as ranging from a single user to around a hundred users.

The MountainBox comprises leading globally sourced hardware and software, packaged into a cost effective and convenient single appliance. This replaces the need for complex and costly multiple hardware devices, software and services.

Our single appliance delivers a powerful firewall, IDS and IPS, VPNs, multiple connectivity options with built-in automatic fail-over, bandwidth steering, Wireless LAN (optional), Captive Portal and an optional IP PABX. All current network service providers and media can be connected via a MountainBox e.g. ADSL2+, Metropolitan Ethernet, WiMax, VSAT, Microwave, 3G/4G etc.

The developers of the MountainBox are fully cognicent of the challenges facing businesses with remote sites in terms of connectivity options, network availability, security, management and control and have optimised the product to overcome these obstacles at a fair price without compromise to the expected functions.

CONTENTS

1. About

Today there are many brand name products offering you firewalls, intrusion detection, failover, bonding, VPN functionality, content filtering etc., but typically these services are run on multiple boxes.

At MountainBox we have decided to combine all these services, and more, into one box, making it an ideal, low cost solution for SMMEs as well as corporates with small to medium sites. This means that you save on hardware costs, software costs, licensing costs and support costs.

Do not however for one moment think that we have compromised anything by doing this. We use the latest state of the art hardware platforms with dual-core processors and 64-bit operating systems. Our entry level box is rated at ~200Mbps - more than enough to saturate multiple ADSL2+ and 3G/HSPA lines simultaneously.

It was developed locally for local conditions. We know telecommunications and we know the South African telecommunication networks.

2. Features

MountainBox iDiG 2.0 is noted for its features, reliability and security functionality often only found in much more expensive commercial gateways and/or firewalls.

It can be configured and upgraded through a web-based interface, and requires no knowledge of the underlying system to manage.

MountainBox iDiG 2.0 is commonly deployed as a firewall, router, wireless access point, DHCP server, DNS server, VPN endpoint/concentrator, traffic steering device and/or failover device.

It is a total solution put together using industry standard global packages and hardware. These packages include:

1. Firewall, Gateway, Router
2. IDS/IPS
3. Content Filtering
4. Management

3. Services

3.1. Powerful Firewall

- Stateful
- Deep Packet Inspection
- Next Generation
- Policy Enforced

3.1.1. Firewall Features

- Packet filtering by source and destination IP, IP protocol, source and destination port for TCP and UDP traffic
- Able to limit simultaneous connections on a per-rule basis
- MountainBox utilises an advanced passive OS/Network fingerprinting utility to allow you to filter by the Operating System initiating the connection. Want to allow FreeBSD and Linux machines to the Internet, but block Windows machines? MountainBox can do so (amongst many other possibilities) by passively detecting the Operating System in use.
- Option to log or not log traffic matching each rule.
- Highly flexible policy routing possible by selecting gateway on a per-rule basis (for load balancing, failover, multiple WAN, etc.)
- Aliases allow grouping and naming of IPs, networks and ports. This helps keep your firewall rule set clean and easy to understand, especially in environments with multiple public IPs and numerous servers.
- Transparent layer 2 fire walling capable - can bridge interfaces and filter traffic between them, even allowing for an IP-less firewall (though you probably want an IP for management purposes).
- Packet normalization - 'Scrubbing' is the normalisation of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembles fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations."
    - Enabled in MountainBox by default
    - Can disable if necessary.
- Disable filter - you can turn off the firewall filter entirely if you wish to turn MountainBox into a pure router.

3.1.2. State Table

The firewall's state table maintains information on your open network connections. MountainBox is a Stateful firewall and by default all rules are Stateful.

Most firewalls lack the ability to finely control your state table. MountainBox has numerous features allowing granular control of your state table, thanks to the abilities of the operating system.

- Adjustable state table size - there are multiple production MountainBox installations using several hundred thousand states. The default state table size is 10,000, but it can be increased on the fly to your desired size. Each state takes approximately 1 KB of RAM, so keep in mind memory usage when sizing your state table. Do not set it arbitrarily high.
- On a per-rule basis:
    - Limit simultaneous client connections
    - Limit states per host
    - Limit new connections per second
    - Define state timeout
    - Define state type
- State types - MountainBox offers multiple options for state handling.
    - Keep state - Works with all protocols. Default for all rules.
    - Modulate state - Works only with TCP. MountainBox will generate strong Initial Sequence Numbers (ISNs) on behalf of the host.
    - Synproxy state - Proxies incoming TCP connections to help protect servers from spoofed TCP SYN floods. This option includes the functionality of keep state and modulate state combined.
    - None - Do not keep any state entries for this traffic. This is very rarely desirable, but is available because it can be useful under some limited circumstances.
- State table optimisation options offer four options for state table optimisation.
    - Normal - the default algorithm
    - High latency - Useful for high latency links, such as satellite connections. Expires idle connections later than normal.
    - Aggressive - Expires idle connections more quickly. More efficient use of hardware resources, but can drop legitimate connections.
    - Conservative - Tries to avoid dropping legitimate connections at the expense of increased memory usage and CPU utilization.

3.1.3. Network Address Translation (NAT)

- Port forwards including ranges and the use of multiple public IPs
- 1:1 NAT for individual IPs or entire subnets.
- Outbound NAT
    - Default settings NAT all outbound traffic to the WAN IP. In multiple WAN scenarios, the default settings NAT outbound traffic to the IP of the WAN interface being used.
    - Advanced Outbound NAT allows this default behaviour to be disabled, and enables the creation of very flexible NAT (or no NAT) rules.
- NAT Reflection - in some configurations, NAT reflection is possible so services can be accessed by public IP from internal networks.

3.1.4. Redundancy

Common Access Redundancy Protocol (CARP) allows for hardware failover. Two or more firewalls can be configured as a failover group. If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active. MountainBox also includes configuration synchronization capabilities, so you make your configuration changes on the primary and they automatically synchronize to the secondary firewall.

Synchronisation ensures the firewall's state table is replicated to all failover configured firewalls. This means your existing connections will be maintained in the case of failure, which is important to prevent network disruptions.

3.1.5. Simultaneous built-in Automatic Fail-over/Load Balancing

3.1.5.1. Fail-Over

The MountainBox has built-in automatic fail-over and multiple levels of fail-over are available. In the event that the primary link fails, the MountainBox will automatically fail-over to the secondary link and will revert on restoration of the primary link. Fail-over does not need to be only on a complete failure, but can be set to fail-over on certain levels of degradation, such as packet loss or latency on the connectivity and will revert on appropriate service levels being restored.

3.1.5.2. Outbound Load Balancing

Outbound load balancing is used with multiple WAN connections to provide load balancing and failover capabilities. Traffic is directed to the desired gateway or load balancing pool on a per-firewall rule basis.

3.1.5.3. Inbound Load Balancing

Inbound load balancing is used to distribute load between multiple servers. This is commonly used with web servers, mail servers, and others. Servers that fail to respond to ping requests or TCP port connections are removed from the pool.

Please Note: Fail-over and Load Balancing can be configured simultaneously for different traffic types, e.g. secure web traffic can be forced through a fail-over gateway while other protocols can load share the links.

3.1.6. VPN

MountainBox offers four options for VPN connectivity:

- IPsec
- OpenVPN (SSL)
- L2TP
- PPTP

3.1.6.1. IPsec

IPsec allows connectivity with any device supporting standard IPsec. This is most commonly used for site to site connectivity to other MountainBox installations, other open source firewalls and most commercial firewall solutions (Cisco, Juniper, etc.). It can also be used for mobile client connectivity.

NAT-T is supported, as well as other advanced capabilities of IPsec-tools, including DPD and XAuth.

3.1.6.2. OpenVPN

OpenVPN is a flexible, powerful SSL VPN solution supporting a wide range of client operating systems.

3.1.6.3. PPTP Server

PPTP is a popular VPN option because nearly every OS has a built in PPTP client, including every Windows release since Windows 95 OSR2.

The MountainBox PPTP Server can use a local user database, or a RADIUS server for authentication. RADIUS accounting is also supported. Firewall rules on the PPTP interface control traffic initiated by PPTP clients.

3.1.6.4. PPPoE Server

MountainBox offers a PPPoE server. A local user database can be used for authentication, and RADIUS authentication with optional accounting is also supported.

In addition, we originate and terminate VPNs.

We also support Branch-to-Branch and mobile VPNs.

3.1.7. Reporting and Monitoring

3.1.7.1. RRD Graphs

The RRD graphs in MountainBox maintain historical information on the following.

- CPU utilisation
- Total throughput
- Firewall states
- Individual throughput for all interfaces
- Packets per second rates for all interfaces
- WAN interface gateway(s) ping response times
- Traffic shaper queues on systems with traffic shaping enabled

3.1.7.2. Real Time Information

Historical information is important, but sometimes it's more important to see real time information.

SVG graphs are available that show real time throughput for each interface.

For traffic shaper users, the Status -> Queues screen provides a real time display of queue usage using AJAX updated gauges.

The front page includes AJAX gauges for display of real time CPU, memory, swap and disk usage, and state table size.

3.2. Dynamic DNS

A Dynamic DNS client is included to allow you to register your public IP with a number of dynamic DNS service providers.

- DynDNS
- DHS
- DyNS
- easyDNS
- No-IP
- ODS.org
- ZoneEdit

A client is also available for RFC 2136 dynamic DNS updates, for use with DNS servers like BIND which support this means of updating.

Multi-WAN is supported, as is unlimited accounts.

3.3. Captive Portal

Captive portal allows you to force authentication, or redirection to a click through page for network access. This is commonly used on hot spot networks, but is also widely used in corporate networks for an additional layer of security on wireless or Internet access. The following is a list of features in the MountainBox Captive Portal.

- Maximum concurrent connections - Limit the number of connections to the portal itself per client IP. This feature prevents a denial of service from client PCs sending network traffic repeatedly without authenticating or clicking through the splash page.
- Idle timeout - Disconnect clients who are idle for more than the defined number of minutes.
- Hard timeout - Force a disconnect of all clients after the defined number of minutes.
- Logon pop up window - Option to pop up a window with a log off button.
- URL Redirection - after authenticating or clicking through the captive portal, users can be forcefully redirected to the defined URL.
- MAC filtering - by default, MountainBox filters using MAC addresses. If you have a subnet behind a router on a captive portal enabled interface, every machine behind the router will be authorized after one user is authorized. MAC filtering can be disabled for these scenarios.
- Authentication options - There are three authentication options available.
    - No authentication - This means the user just clicks through your portal page without entering credentials.
    - Local user manager - A local user database can be configured and used for authentication.
    - RADIUS authentication - This is the preferred authentication method for corporate environments and ISPs. It can be used to authenticate from Microsoft Active Directory and numerous other RADIUS servers.
- RADIUS capabilities
    - Forced re-authentication
    - Able to send Accounting updates

    - RADIUS MAC authentication allows captive portal to authenticate to a RADIUS server using the client's MAC address as the user name and password.
    - Allows configuration of redundant RADIUS servers.
- HTTP or HTTPS - The portal page can be configured to use either HTTP or HTTPS.
- Pass-through MAC and IP addresses - MAC and IP addresses can be white listed to bypass the portal. Any machines with NAT port forwards will need to be bypassed so the reply traffic does not hit the portal. You may wish to exclude some machines for other reasons.
- File Manager - This allows you to upload images for use in your portal pages.
- Supports all and unlimited interfaces.

3.4. DHCP Server and Relay

MountainBox includes both DHCP Server and Relay functionality

4. Security

Internet Security – Intrusion Detection, Prevention and Protection including

- Malware Protection & Mitigation
- Botnets Detection & Mitigation
- Phising and Fraud Protection

4.1. IDS/IPS Overview

- Next-generation IPS (NGIPS) with contextual awareness
- Rule-driven language combining the benefits of signature, protocol and anomaly-based inspection methods.
- The single most widely deployed intrusion detection and prevention technology in the world
- Fastest and most accurate detection tested by NSS Labs*
- Leader in the Gartner Magic Quadrant for Network IPS Appliances*
- Best IDS/IPS from *SC Magazine**
- ICSA Labs Certified*

  * 3D8260 Hardware

4.2. Next-Generation Intrusion Prevention System (NGIPS)

Automate Security with Contextual Awareness

Today's networks are highly dynamic. New technologies add complexity, and the number and type of applications and systems on your network continues to grow. Information security risks multiply in number and scale as attackers become more sophisticated—and stealthy.

MountainBox iDiG 2.0 raises the bar for IPS technology by integrating real-time contextual awareness into its inspection. The system gathers information about network and host configurations, applications and operating systems, user identity, and network behaviour and traffic baselines. By having the utmost visibility into what's running on your network, NGIPS offers event impact assessment, automated IPS tuning, and user identification to significantly lower the total cost of ownership.

Below is a sampling of the threat detection provided by iDiG 2.0:

DoS Attacks	Invalid Headers	IPv6 Attacks
Buffer Overflows	Blended Threats	Statistical Anomalies
P2P Attacks	Rate-based Attacks	Protocol Anomalies
Worms	Zero-day Threats	Application Anomalies
Trojans	Port Scans	Malformed Traffic
Backdoor Attacks	VoIP Attacks	TCP Segmentation
Spyware		IP Fragmentation

5. Content Filtering

Internet Content Control – Blocking of sites, such as violence, etc. by Category and Blacklist

MountainBox iDiG 2.0 could be hard coded to use OpenDNS.

5.1. Best-in-class Web security

Secure Web and Internet traffic by protecting against malware, phishing and botnet infections. We offer a unique DNS-based solution that protects your network across all protocols: immobilising botnets, preventing drive-by downloads, and eliminating leaks of confidential information.

5.2. Comprehensive Web content filtering

The OpenDNS content filtering solutions allow you to easily enforce your organization's acceptable use policy by selective blocking traffic to undesirable sites.

5.3 Global cloud service

Reduce your operational burden by offloading DNS and Web security to the original cloud security service. OpenDNS satisfies 30 billion requests every day for tens of millions of customers from data centres located strategically around the globe, setting the bar for reliable infrastructure.

5.4. World DNS leader

We are the only security and filtering service that increases performance without hogging bandwidth or introducing latency. This is because the services are built on top of highly optimised DNS platforms (the phonebook of the Internet), which makes setup easy too.

5.5. Web-based reporting and administration

No matter where you are in the world, you can administer the settings for any office or user from any Internet connection. Access all your reports and analyse, aggregate and compare usage across multiple locations using our state-of-the-art web-based statistics system.

6. Bandwidth Management

6.1. QoS

MountainBox iDiG 2.0 has extensive management tools built in, including wizard driven queue Layer 7 and limiter configurations. MountainBox is able to interact with MPLS networks using diffserve code point and these configurations can be time scheduled to optimise bandwidth on a time of day basis.

6.2. Caching

MountainBox iDiG 2.0 features a caching proxy for the web supporting HTTP, HTTPS, FTP and more. It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages. iDiG 2.0 has extensive access controls and makes a great server accelerator.

6.3. Usage Reports

MountainBox iDiG 2.0 also provides a built in reporting application.

This provides an easy method of monitoring internet usage on your network. Its log analyser runs by parsing through the proxy access logs, the system produces web based reports that detail the URLs accessed by each user on the network.

The reports have some useful features that allow you to see bandwidth usage, URL access by date and time and top site reports.

Since it runs directly on iDiG 2.0 it is both centralised and stealth. Users on the network have no way of knowing their traffic is being logged and analysed using this method.

7. Management Features

7.1. Local

Every MountainBox features an on-board webserver that is accessed through popular browsers via any of its interfaces such as LAN, WAN or Wi-Fi. The access is password protected and certificate based from the inbuilt CA.

The user interface has a user friendly consolidated dashboard view, which graphically summarises activities and status of important aspects, such as:

- State of interface links,
- Traffic and graphing of traffic in real time,
- Status of gateways including packet loss and latency and
- General system status such as
    - CPU,
    - Memory and memory usage (system load) as well as
    - VPN tunnel status.

Different user profiles allow full scale administration or limit the user to the dashboard view only. Historical traffic usage summaries are stored locally by RRD graphing tools as user friendly graphs and summaries.

If the optional proxy server (free) is included, then Internet usage, down to URL, time and data usage is available through a special report.

Locally the appliance is able to mail alerts and also supports GROWL alerts.

7.2. Remote

MountainBox can be accessed via a certificate HTTPS session remotely through the Internet or other networks via modern browsers.

7.3. Interoperability with other Management Systems

Every MountainBox includes industry standard SNMP agents. The appliance can uplift statistics to external management systems via an SNMP agent or via Netflow or Zabbix selectable agents. The system also includes a management agent for Nagios. This enables triggers such as on/off status and traffic counters to be uplifted to external systems for post processing and alerting.

8. VoIP

MountainBox can be supplied with a full Asterisk or FreeSwitch VoIP PABX implementation with full IVR System for increased productivity

It provides more agility in the form of:

- Access - Via any internet connection, crucial for a mobile workforce, accommodating workers stationed abroad, in transit, or simply telecommuting from home. With VoIP, users can check voicemail and email, access project data, and place calls--all over a single network, using a single communication device.
- Integration - Integrates with other communication technology, i.e. CRM and Outlook.
- Flexibility

It scales immediately to a business' needs.

Functionality - Many advanced functions that are either a luxury or unavailable on PBX systems come standard with VoIP. These features include advanced call forwarding and electronic messaging, custom auto-attendant, three-way conferencing, videoconferencing, and Advanced Call Distribution (ACD) functions such as skills-based call routing.

Lower Total Cost of Ownership

Cut telecommunications costs by about 30% when switching to VoIP i.e.:

- Lower start-up costs
- No initial investment in PBX and other expensive equipment.
- Lower maintenance costs
- Dramatically reduces maintenance costs.
- Lower monthly phone bills

8.1. Call Features

ADSI On-Screen Menu System
Alarm Receiver
Append Message
Authentication
Automated Attendant
Blacklists
Blind Transfer
Call Detail Records
Call Forward on Busy
Call Forward on No Answer
Call Forward Variable
Call Monitoring
Call Parking
Call Queuing
Call Recording
Call Retrieval
Call Routing (DID & ANI)
Call Snooping
Call Transfer
Call Waiting
Caller ID
Caller ID Blocking
Caller ID on Call Waiting
Calling Cards
Conference Bridging
Database Store / Retrieve
Database Integration
Dial by Name
Direct Inward System Access
Distinctive Ring
Distributed Universal Number Discovery (DUNDi™)
Do Not Disturb
E911
ENUM
Fax Transmit and Receive
Flexible Extension Logic
Interactive Directory Listing
Interactive Voice Response (IVR)
Local and Remote Call Agents
Macros
Music On Hold
Music On Transfer:
- Flexible Mp3-based System
- Random or Linear Play
- Volume Control
Predictive Dialer
Privacy
Open Settlement Protocol (OSP)
Overhead Paging
Protocol Conversion
Remote Call Pickup
Remote Office Support
Roaming Extensions
Route by Caller ID
SMS Messaging
Spell / Say
Streaming Media Access
Supervised Transfer
Talk Detection
Text-to-Speech (via Festival)
Three-way Calling
Time and Date
Transcoding
Trunking
VoIP Gateways
Voicemail:
- Visual Indicator for Message Waiting
- Stutter Dialtone for Message Waiting
- Voicemail to email
- Voicemail Groups
- Web Voicemail Interface
Zapateller

9. Benefits

Optimising the efficient use of bandwidth
Increased Broadband speed
An enforceable Internet usage policy increasing staff productivity (Cyber loafing)
Protection from Cyber attacks
Maximum business continuity for all sites irrespective of location
Secure workforce mobility
Significant cost reductions in both WAN and LAN network deployment & management
Protection from security threats
Freedom to utilise services of choice dependant on budget and site location
Tailor-made for small to medium sites (SMME or Corporate)
Powerfully priced

10. Advantages

Cost effective rental of full suite of services tailored specifically for small sites
Business continuity peace of mind for small business through built-in automatic fail-over
Optimises the South African broadband connectivity for small and medium sites.
In-house development and packaging for strategically positioning it for local conditions and specific customers
Less affected by negative Global influences, such as unfavourable ROE
Customisable for more customer specific solutions
Faster than normal response to client requirements
Cost effective solution for SMMEs and/or corporates with small and medium sites
High performance device due to standard industry hardware
Open source operating systems

11. Connectivity

The MountainBox iDiG 2.0 connects to the following:

- ADSL2+ - (up to 2 Ports)
- 3G (HSPA+) – (up to 6 Ports)
- Ethernet (10/100/1000 Mbps) – (up to 5 Ports)
- Wi-Fi (802.11 a/b/g/n) – (1 Port – Multiple SSIDs)
- Wi-Max (802.16) – (i.e. iBurst)*
- VSAT*
- Diginet*

* Via Ethernet

12. Contact

Physical Address

Ground Floor, AMR 1
9 Concorde Road East
Bedfordview
2007
Johannesburg
South Africa

Postal Address

P O Box 751118
Gardenview
2047
South Africa

Telephone

Local: 011 450 1048
International: +27 11 450 1048
Local: 087 985 0062 VoIP
International: +27 87 985 0062 VoIP

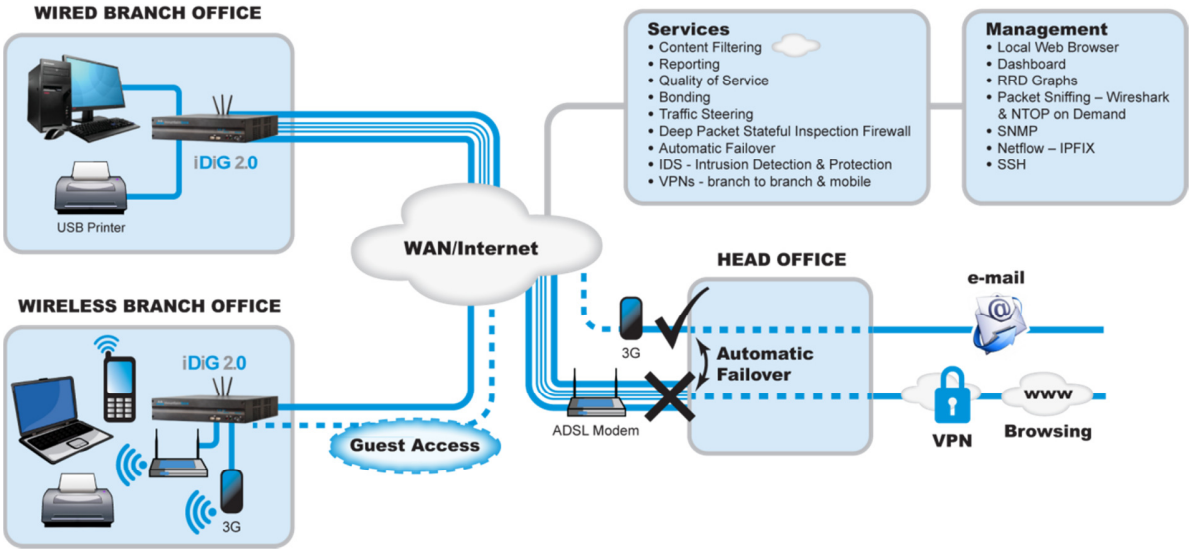
Fax

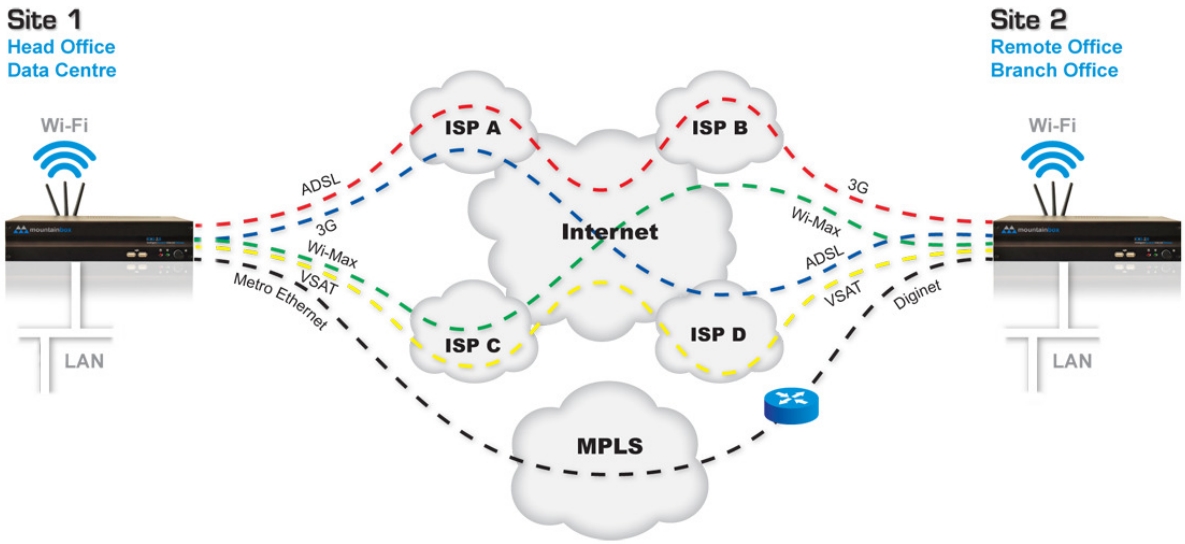
Local: 011 450 3117
International: +27 11 450 3117

eMail

info@mountainbox.co.za
info@5thmountain.co.za

13. Appendix A – Network Diagrams





mountainbox

iDiG 2.0
Intelligent Dynamic Internet Gateway