Datasheet

NetDefense® Dual Core (NDDC)

Design Your Network Against Service Provider Outage, Malware, and DDoS

Introduction

Network traffic to and from mission-critical businesses pass through today's service provider networks via many hops before reaching its destination. From data centers or last-mile HQs, to telco's central exchanges, to core backbone, to internet gateway or another destination, the failure of any part of the service provider network can result in an outage. Even exchange diversity does not take into account that other parts of the core network could fail.

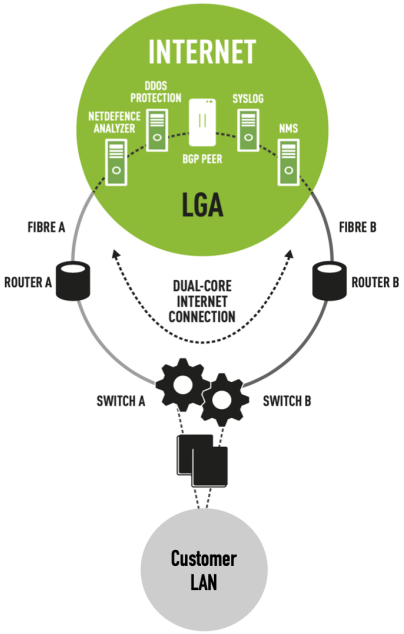
NetDefense® Dual Core

NetDefense® Dual-Core identifies, protects, and mitigates against external and internal threats and vulnerabilities, such as service availability, threats from the internet or within the local network. It is designed to ensure smooth and uninterrupted business services and operations at all times, as well as to protect your valuable business assets.

By leveraging LGA's networking & security expertise and infrastructure, you empower your IT department to focus on core business activities without worrying about network outages and security. It lowers risk, improves service availability, security and reduces unnecessary costs to business owners.

Network design and IP address definitions are simplified without relying on complex link controllers and IPs assigned by underlying service providers (FBOs).

- **Malware**
- **Ransomware**
- **Phishing**
- **DDOS**
- **Web Attacks**
- **Intrusion Attacks**
- **Service Provider Failure**



Benefits

- Zero interruption - ensures operational availability with near-zero downtime for mission critical class-level service connectivity
- Survives service provider outages above and beyond exchange diversity via dual core technology - full network redundancy using duallinks from two different telco infrastructure (NGN & Non-NGN) to avoid a single point of failure
- IP address independence - no reliance on service provider provided IPs as the solution is telco-neutral
- Unified Threat Management (UTM) inspects all inbound and outbound traffic and allows only safe traffic to pass while blocking unsafe content
- Stops DDoS threats
- WAF provides robust security for your server by identifying, verifying and protecting against threats
- Endpoint protection against advanced threats
- Line and Security monitoring managed services is available 24/7 and comes with a guaranteed response time to an incident

NetDefense® Dual Core (NDDC)

Standard Features

High Availability

NetDefense® stops at nothing to ensure operational service ability at all times. Your Internet connection has dual links (dual service providers) to attain near-zero downtime for mission critical class-level service connectivity.

Unified Threat Management

UTM inspects all inbound and outbound traffic on any given network and allows only safe traffic to pass while blocking unsafe content. With Virtual Private Network (VPN) built-in, all employees can access their company's network outside the office while enjoying the same security level. Complete with Intrusion Prevention Systems (IPS), NetDefense® vigilantly stops threats from hackers, sophisticated malware, botnets, and other advanced, persistent threats.

Simplified Control Management

Performance management has become a crucial part of the IT team's role - especially for global organisations. NetDefense® makes it easier for IT managers to make informed decisions in complex business environments that leverage heavily on technology. By making network activities plain, simple and visible to our clients, it empowers them with complete control and manageability.

Event and Log Management

LGA's Event & Management Service is capable of dealing with large volumes of device events and log messages. It collects and stores the data, and can be called upon to search, analyse, and report as well. It gives a comprehensive perspective on what is happening in your network and system.

Securing both the network perimeter and the interior is daunting. Even in a medium-sized organisation, the sheer number and types of devices on the network can easily overwhelm any administrator's ability to manage. Our solution is capable of configuring, monitoring, remedying, and auditing these devices. Aside from protection from threats, NetDefense® can help you reduce operational costs and streamline your Compliance Lifecycle.

Threat Response

Time is of the essence in containing and arresting threats. NetDefense® Threat Response is an optimised process that quickly identifies, verifies and stops malicious data that attempt to breach our customers' network, such that it has minimal impact on internal IT operations when it occurs.

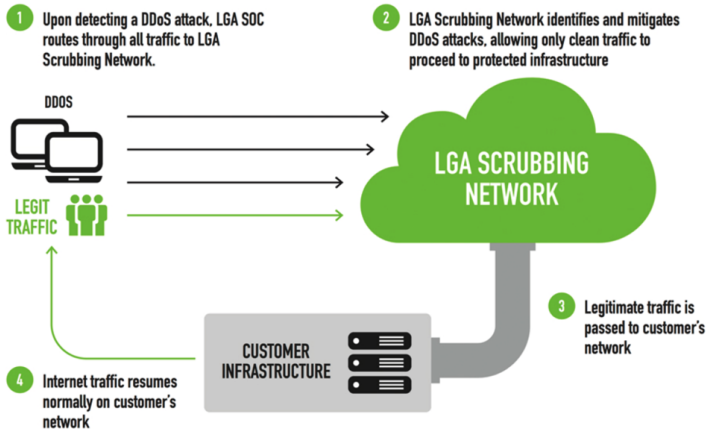
SOCaas & Comprehensive Support

NetDefense® monitoring & support is available 24/7 and comes with a guaranteed response time to an incident. Our customers are served by highly skilled network and system engineers who have undergone rigorous security training. Hardware is warranted at all times, and in the event of failure, it will be promptly replaced.

NetDefense® Dual Core (NDDC)

Managed DDoS Protection

Effective network protection against volumetric attacks goes beyond regular security devices such as firewalls and intrusion detection systems. Such attacks disrupt your business continuity or gain access to valuable customer data. DDoS Protection is a comprehensive, round the clock service that responds to DDoS threats. It also comes with Data Scrubbing Service to screen and remove malicious data. DDoS service mitigates the threat outside of your network and passes only legitimate traffic to your network so that the real users remain satisfied and undenied of real service.



Optional Features

Web Application Firewall

The business of today relies heavily on the Internet. Access speed must be swift, site availability must be absolute, and security must be tight. Web-driven applications of today are tuned to run at peak and deliver optimal performance. Poor service availability results in business losses or brand impairment. Hackers target web applications to disrupt business. Web Application Firewall (WAF) is a solution to meet this challenge. From dealing with data breaches to defacement, WAF service clients can provide robust security for your server by identifying, verifying and protecting against these threats.

Endpoint Detection & Response

With Endpoint Detection & Response, you mitigate against advanced threats - without the need for IT expertise. It is an affordable, easy-to-use security solution that combines industry leading threat protection with web and messaging security, data protection, and rigorous mobile security and device management to secure your internal IT infrastructure.

NetDefense® Dual Core (NDDC)

Solution Options Deploying NDDC:

Customers can deploy NDDC according to their needs and even grow the scope of the solution:

	NDDC Scope
1	Dual Core + Line Monitoring
2	Dual Core + 1 Next-Gen Firewall + Line Monitoring
3	Dual Core + 2 Next-Gen Firewall + Line Monitoring
4	Dual Core + 1 Next-Gen Firewall + Line Monitoring + SOCaaS
5	Dual Core + 2 Next-Gen Firewall + Line Monitoring + SOCaaS
6	Dual Core + 2 Next-Gen Firewall + Line Monitoring + SOCaaS + Dual Site
7	Add on options: DDoS, WAF

Contact Us

LGA Telecom Pte Ltd
33 Ubi Avenue 3
#08-53 Vertex (Tower A)
Singapore 408868

Tel (65) 6892 2308
Email: sales@lgatelecom.net
Website: www.lgatelecom.net