

# Internet DDoS Protection

**nextgen**  
pure-data



Nextgen's Internet DDoS Protection service detects and defends against Distributed Denial of Service attacks which can materially disrupt your web-based business systems.

## Service Overview

Nextgen's Internet DDoS Protection service comprises both attack detection and attack mitigation services.

The detection service identifies a DDoS attack in the Nextgen Internet network and provides alarms to the Nextgen Service Management Centre (SMC).

When a suspected DDoS attack is detected, Nextgen's SMC calls the customer to verify the authenticity of the attack. This allows the customer to confirm if the suspected attack is genuine traffic or not, thus avoiding any unnecessary disruptions.

With customer agreement, Nextgen then takes action against the attack by blocking the 'attack' traffic that would otherwise congest and potentially disable the customer site or service.

## Nextgen Solution Architecture

Nextgen uses network anomaly detection based attack mitigation technology. The service operates by collecting Netflow, SNMP and BGP information from Internet border routers.

The data is correlated by the detection appliances and an alert is generated when an anomaly is detected. These anomalies are based on individual thresholds that have been established for each customer during the service baselining period.

Nextgen's SMC enables the attack mitigation on the cleaning platform where 'attack' traffic is blocked and discarded and 'clean' traffic is allowed to flow through to the customer's connection.

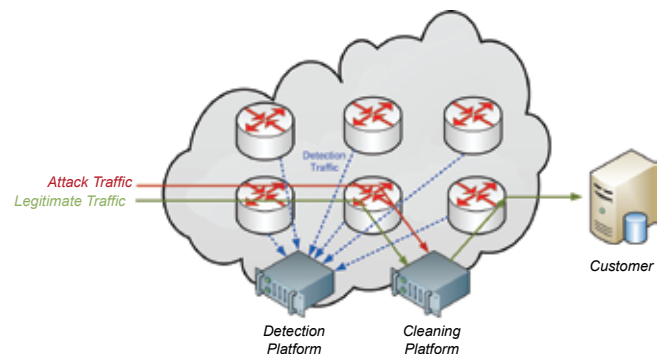


Diagram 1: Nextgen DDoS Protection Platform Architecture

## Key Features

- **Detects and cleans** DDoS attacks
- **Blocks attack traffic** from congesting the customer network
- **Customer control** allowing you to confirm that suspected traffic is hostile before blocking
- **24x7 service** including monitoring and access to help desk
- **Service level guarantee** with rebate backed protection

## Key Benefits

- **Business continuity** support in the event of a DDoS attack
- **Business Reputation** underpinned with reliable on-line service availability

# Nextgen DDoS Protection Service Components and Process

## Configuration

Nextgen configures the DDoS protection service to look for traffic targeted at the customer's specific IP addresses.

## Baseline

Once configured, the service automatically begins to collect data to characterize the customer's normal traffic. This baseline discovery process takes approximately four (4) weeks.

## Monitoring

Nextgen's DDoS Protection service uses NetFlow data to continually monitor traffic destined for the customer's IP addresses. The NetFlow samples are used to look for patterns of behaviour outside of what is expected as normal from the baseline exercise.

## Alerts

When the platform detects traffic that falls outside of the preset thresholds, it sends an alert to Nextgen's Service

Management Centre (SMC). The SMC will call the customer with notification of the attack.

## Mitigation

If agreed by the customer, the SMC enables attack mitigation by advertising the targeted IP address on the Nextgen Threat Management System (TMS). All traffic destined to this IP address will then be routed through the TMS.

"Clean" traffic is allowed to continue to the customer's connection via a different IP address that is nominated by the customer.

"Attack" traffic is discarded. Mitigation is typically enabled for 24 hours, at which time the SMC revisits the platform to check if the attack is still underway.

Should the attack cease, the routing is restored to normal. If the attack is still ongoing, the process continues for another 24 hours and is repeated until the attack is over.

## Service Level Guarantee

Nextgen is committed to delivering the following service level to Internet DDoS Protection customers, backed by the following Service Level Guarantee and rebate offer.

Feature	Service Level Target	Rebate Guarantee [1, 2]
Installation lead time	5 business days from receipt of order or as otherwise agreed [4]	N/A
Attack notification call	Nextgen will call the customer within 30 minutes of DDoS attack identification	10% rebate off the monthly service fee
Time to mitigate	Nextgen will commence attack mitigation within 30 minutes from the customer's authorisation to mitigate	10% rebate off the monthly service fee
Attack mitigation	Customer site is available [3] during the DDoS attack	Rebate if the DDoS attack causes service unavailability [3] Unavailable for more than 6 hours: 40% rebate Unavailable for more than 12 hours: 60% rebate Unavailable for more than 18 hours: 80% rebate Unavailable for more than 24 hours: 100% rebate
Service availability of DDoS protection infrastructure	99.95% target availability for DDoS Protection infrastructure within Nextgen's network excluding scheduled maintenance periods	N/A

Applicable conditions:

- [1] Nextgen provides no guarantees on product performance parameters, other than those mentioned specifically in this document. The payment of a rebate is conditional on the Customer requesting a rebate within 1 month of the relevant incident, and the amount of rebate and whether a rebate is payable is a matter solely for Nextgen, acting in good faith.
- [2] Rebates are specified as a percentage of the DDoS protection monthly service fee. The rebate offer commences after the initial baseline learning period. Rebates are subject to the customer fulfilling the obligations as listed in this data sheet. Rebates in aggregate are capped at 100% of the monthly DDoS protection fee for all attacks in any month, and are the sole remedy available to the customer.
- [3] In the context of this Service Level Guarantee, Nextgen defines service unavailability as an outage or degradation to the extent that the Internet service may not reasonably be used for its intended purpose, falls outside of its service parameters and is assessed by Nextgen as being caused by the DDoS attack.
- [4] Applicable to DDoS Protection service installations on existing Nextgen internet services and speeds of up to 300Mb/s.

## DDoS Attacks

Distributed Denial of Service (DDoS) attacks can materially disrupt a corporation's Internet and web business environment by preventing a target Internet site or service from functioning effectively. Typical DDoS attack targets include the web sites of businesses or organisations that place a high value on the correct functioning of their on-line infrastructure.

Attackers typically use a wide network of computers to covertly generate an attack. Unbeknown by their owner, these computers are then remotely controlled by the attacker to deliver the high traffic flow required for a DDoS attack.

## Service Attributes

Feature	Details
Supported internet link bandwidths	From 10Mb/s to 1Gb/s in standard Internet product bandwidth increments.
Base Lining period (learning period)	The initial 4 weeks after service activation during which time the specific customer service is analysed in detail and characterised to provide the baseline for attack detection. During this period: - flooding attacks can be detected and mitigated - detection of other attack types is not supported - in the case of an attack not detected by Nextgen, customers may call the Nextgen SMC to advise of the attack which may be mitigated using a range of measures available to the Nextgen SMC Nextgen reserves the right to make adjustments to sensitivity of alarm thresholds at any time.
Minimum Contract Term	1 year (includes Base Lining period)
Service performance during mitigation	Some latency and potentially traffic congestion performance degradation is expected during mitigation processes.
Recognised attacks types	Spoofed: Sending packets with a forged source address Malformed: Sending packets with abnormal bits or flags set Floods: Sending high rates of legitimately formed packets Null: Sending packets with no content or illegitimate protocol Protocol: Sending packets with illegitimate protocols Fragmented: Sending packets fragments that will never be completed Brute Force: Sending packets that exceed defined flow rate thresholds
Recognised attack protocols and packet formats	ICMP, IP Fragment, IP NULL, IP Private TCP NULL, TCP Reset, TCP SYN.
Service Limitations	Attacks between Nextgen Customers, or between Customers and Peers will not be detected. If a customer chooses to have the same AS number on multiple services, the type of DDoS protection implemented must be applied across all services applicable to that AS number.
Use with Nextgen Shadow Internet Service	Shadow Internet services will adopt the features of the Primary service.
Customer parameter maintenance	Customers are obligated to maintain the following information with Nextgen. Changes to these parameters are lodged with a phone call to the Nextgen SMC: - IP address prefix changes for static IP address customers - BGP AS number changes for BGP customers - Customer gateway IP address - Detection sensitivity setting
Customer obligations	To be eligible for the mitigation service, the customer must be able to nominate a public IP address within their network to which Nextgen should deliver the mitigated traffic. This information is required to be captured on the customer order form. It is also desirable that the customer nominates a test IP address for service activation.
Services not included	- Permanent archival and storage of log files relating to the DDoS attack - Forensic investigation relating to the source of the DDoS attack - Legal case preparation relating to the source of the DDoS attack - Security consulting service
Nextgen network integrity rights	If the size of the attack is such that the Nextgen network is threatened and other customers could be effected, Nextgen will take all the required measures in order to maintain the integrity of the Nextgen network. No SLA rebates are payable to customers in such circumstances.

## DDoS Attack Impact

DDoS attacks can severely impact the effective operation of customer web-based business systems that include:

- Corporate websites and customer portals
- Critical web-based business applications
- E-commerce transaction engines
- E-mail and DNS servers
- Network routers, switches and firewalls
- Remote access infrastructure
- Private network infrastructure which is shared with the Internet

## Reporting Portal

Nextgen's Performance Reporting Portal provides the following information for DDoS protected customer services:

- Recent alerts on customer network
- Ongoing alerts on customer network
- Detailed view of each alert up to TCP / IP Layer 4 including:
  - Attack traffic direction
  - Source and destination address
  - Protocols
  - Port numbers

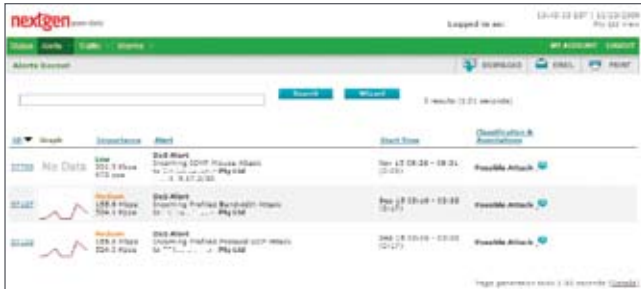
(See separate Nextgen Performance Reporting Portal data sheet for more information).

## Post Mitigation Reporting

Upon request, Nextgen will provide a post incident report including DDoS attack duration, peak traffic and mitigation actions taken.

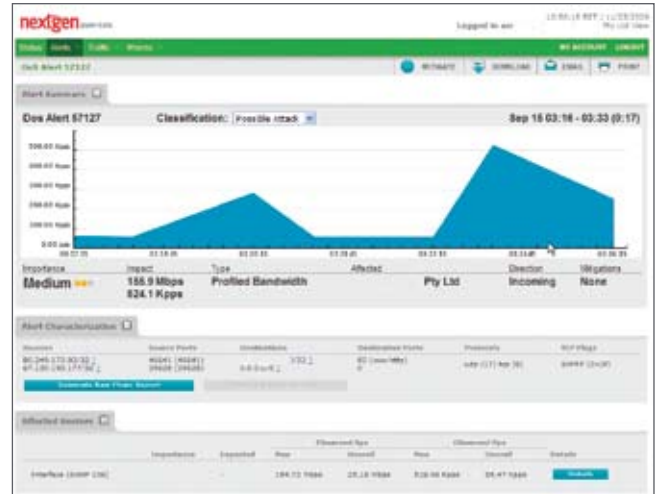
Reports will be sent by e-mail in PDF format to the nominated customer technical contact.

### Snapshot of all Recent DDoS Alerts



Alert ID	Alert Name	Start Time	Classification
57127	DDoS Alert: Smurfing UDP Flood Attack	Nov 17 08:30 - 09:24 (2:03)	Possible Attack
57127	DDoS Alert: Smurfing UDP Flood Attack	Nov 18 03:18 - 03:33 (2:15)	Possible Attack
57127	DDoS Alert: Smurfing UDP Flood Attack	Nov 18 03:18 - 03:33 (2:15)	Possible Attack

### Details of Individual Alert



## ABOUT NEXTGEN NETWORKS

Nextgen Networks is a national Telecommunications carrier that specialises in high performance data services. Our customers are other Corporations, Government, Service Providers and other Carriers. Nextgen products include high capacity data transmission services ranging from corporate links up to complete wavelengths, nationwide multi-point Ethernet networks (VPLS Service), Internet and carrier grade co-location offerings. Nextgen owns and operates infrastructure that includes the third largest fibre network in Australia, a latest generation national switched Ethernet data network and co-location centres throughout Australia. Nextgen is a wholly owned subsidiary of the Leighton Group.

Check out the benefits of our award winning data solutions

Phone: 1300 653 351

[www.nextgennetworks.com.au](http://www.nextgennetworks.com.au)