Schedule document

DDoS Protection as a Service

Node4 Limited
01/06/2024

Schedule Document

DDoS Protection as a Service

This schedule contains additional terms and conditions, service description and service levels applicable to the DDoS Protection as a Service and should be viewed with associated Order Form, Node4's General Terms and Conditions and the Acceptable Use Policy.

1. Overview

DDoS Protection as a Service provides the Client with a combined approach to mitigate against DDoS attacks.

2. Definitions

"Client Responsible Incident" means in the event that a Service Affecting or Non-Service Affecting Incident is identified as being attributable to Client Provided Equipment, Premises, Client power supplies, or the action of the Client, employees or agents of the Client, the Incident shall be deemed the responsibility of the Client. Any downtime shall not be included in service availability measurements and does not qualify for compensation.

"DDoS" means Distributed Denial of Service - a type of electronic attack involving multiple computers which send repeated requests to a server (web site) generating false traffic and rendering it inaccessible to valid users.

"Mitigation" means an attempt by the DDoS mitigation service to block an attack by filtering out malicious attack traffic and passing on genuine client traffic.

"Incident" *means* an unplanned interruption to a service or a reduction in service quality**.**

"Installation Fees" means charges payable by the Client for the installation of Services as provided in the Order Form.

"Monthly Review Period" means the calendar monthly periods commencing on the 1st of each month during the Term, over which Service performance measurements are calculated, provided that the first Monthly Review Period will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client.

"Node4 Network" means the network wholly owned and managed by Node4.

"Non-Service Affecting Incident" means a Incident or condition which is not a Service Affecting Incident.

"Penetration Test" Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

"Planned Outage" means proactive work required to maintain the service provided, Node4 may with reasonable notice require a temporary outage in service. Wherever possible Node4 will agree the outage with you in advance of the required work. Any planned downtime shall not be included in Incident or service reliability measurements.

"Service Affecting Incident" means any failure of Node4 service, which, in our reasonable opinion causes a loss of a Client's service. In all such cases the service shall be deemed unavailable and the length of downtime recorded by Node4 from when the Incident is registered by Node4 and a Service Ticket allocated.

"Service Availability" means the time for which a Node4 service is usable, expressed as a percentage of the total time in a given Monthly Review Period. The Node4 service shall be deemed available for the purposes of calculating Service Availability if it is not usable due to an event outside our reasonable control, a Client Responsible Incident, a Third Party Attributable Incident or is due to a Planned Outage.

"Service Desk" means the single point of entry for all Service Tickets and Service Requests which can be accessed over the phone, by email or via our portal.

"Service Request" means a request for a change for information

"Service Ticket" means the tickets which are raised in relation to Incident or Service Request

"Third Party Attributable Incident" means in the event that a Service Affecting or Non-Service Affecting Incident is identified as being attributable to a third party this measurement period shall not be

included in service availability measurements. Such Incidents do not qualify for rebates or compensation. Node4 will endeavour to resolve and rectify such Third-Party Attributable Incidents as soon as possible.

"Volumetric Attack" means a DDoS attack intended to paralyse the system or resource through saturation of the network (typically multiple Gbps).

3. Specific terms

The following terms and conditions shall apply when Node4 provides the DDoS Protection as a Service to the Client.

3.1 Client cooperation

Node4 expects any Client to co-operate to provide full notice and visibility of any cyber-attack threat or incident when required, and to treat advanced notification of such as urgent. This may include sharing of information such as ransom emails or telephone calls.

Any Client penetration tests must be notified in advance and agreed with Node4 before they are initiated. DDOS protection services can be disabled for the duration of the penetration test if required, requested by the Client and approved by Node4. Requests should be made with a minimum of 8 working days notice and will be categorised as a Level 5 service request.

3.2 Disclaimer

DDoS Protection will not detect and prevent all possible DDoS threats and attacks and will not make the Client invulnerable to all DDoS attacks.

3.3 Third parties

The Client commits to fully manage all their Customers and suppliers directly. Node4 will not interface directly with any third parties working with the Client unless by prior arrangement. If the Client requires Node4 to provide their customers with a customer care or NOC service this is available on request and subject to Professional Service Fees.

Node4 shall not be liable in respect of any contract, agreement or relationship that Client may have with any third party. If a dispute arises between Client and a third party involving Node4's DDoS Protection as a Service, Node4 shall provide the Client with reasonable information and assistance (to the extent that such is not adverse to Node4's interests to Client (at Client's expense)) in the resolution of such dispute.

4. Fees

Fees will commence when the implementation of such Product or Service is completed by Node4 and such Product or Service is available for use by the Client.

Fees may comprise any or all of the following.

4.1 Installation and set-up fees

Any applicable Design, Configuration, and Installation Fees for the implementation of the DDoS Protection as a Service shall be detailed on the Order Form.

4.2 Monthly fees

Monthly Fees are paid in advance. Monthly Fees for DDoS Protection as a Service are associated with the bandwidth internet access connection that it protects.

4.3 Professional service fees

Additional tasks undertaken at the request of the Client by Node4 personnel, will be charged at rates agreed between the parties in advance.

5. Client responsibilities

In order to deliver DDoS Protection as a Service we expect the Client to provide:

- IP Addressing information
- Liaison with Node4 Engineering, Provisioning and project management teams.
- Liaison with Node4 Client Support teams.

5.1 Approval for Pentation testing

The Client must obtain approval to run penetration testing, on the IP addresses protected by the DDoS Protection service. The Client must provide:

- 10 business days' notice of the start of any penetration testing.
- Request should be made by emailing security@node4.co.uk.

- Request should state the request start and end dates and time for the testing.
- Penetration testing must not start until permission has been granted by security@node4.co.uk.
- Penetration testing must not start before the date and time notified in the request.
- Penetration testing must end by the date and time notified in the request.

Node4 may refuse permission if the penetration start, end time or duration are likely to impair the performance of the Node4 network or connectivity of its other Clients.

6. Service provision

The Node4 DDoS Protection as a Service provides the Client with DDoS mitigation services for internet access connections provided by Node4 and delivered from Node4's core network.

6.1 Installation

Included within the product, Node4 will complete the following works to activate the service:

- Agree the parameters within the scope of the service offering with the Client.
- Implement the configuration changes required to direct Client traffic through the DDoS protection service.
- Establish monitoring of the connection on which DDoS protection is applied, with thresholds to determine unmitigated attacks.

For Node4 to complete these activities, the Client must:

- Specify the IP addresses, IP address ranges or ASN for which the Client desires the DDoS Protection Service to be activated, by completing a form which Node4 will provide.
- Provide contact details for the departments and/or people Node4 may contact during a DDoS attack.

Professional Services work beyond the scope above are subject to additional fees.

6.2 Protected services

Client internet access services to be protected by the Node4 DDoS Protection as a Service product will be identified on the Order Form. Each Client internet access service requires its own associated DDoS protection service.

For the Client to benefit from fully automated DDoS mitigation, they must use provider assigned public IP space as directed by Node4. This may require the Client to migrate from their existing IP space to Node4 specified IP space at the time the service is setup.

If the Client is unable to use the IP space directed by Node4, then manual intervention may be required to activate the DDoS mitigation service at the time of an attack, which will delay the time before protection is effective.

6.3 Internet security

Node4 DDoS Protection as a Services provides a specific protection capability that mitigates detected DDoS attacks. Node4 can provide Clients with additional internet and other security services, to offer further protection and layered security.

6.4 DDoS Protection

DDoS Protection as a Service provides a mitigation of application layer DDoS attacks including:

- HTTP-GET Attacks
- HTTP-PST Attacks
- SSL Attacks

Resource Exhaustion	Volumetric DDoS	Reflective DDoS
Malformed and Truncated Packets (e.g., UDP Bombs)	TCP Flood	NTP Monlist Response Amplification
IP Fragmentation/Segmentation AETs	UDP Flood	SSDP/UPnP Responses
Invalid TCP Segment IDs	UDP Fragmentation	SNMP Inbound Responses
Bad checksums and illegal flags in TCP/UDP frames	SYN Flood	Chargen Responses (Character Generator Protocol)

Invalid TCP/UDP port numbers; Use of reserved IP addresses	ICMP Floods	DNS Amplification
IP Fragmentation/Segmentation AETs		Connectionless LDAP (CLDAP) Amplification

Mitigation protection is available as soon as the service is enacted, baselining nor 'learning' is required.
DDoS Protection as a Service provides a mitigation of volumetric DDoS attacks including:

- TCP SYN Floods (SYN, SYN ACK, etc.)
- ICMP Flood Attacks (Ping Barrage,
- Smurf, etc.)
- UDP Flood Attacks (UDP Barrage,
- Fraggle, Etc.)
- Reflection Attacks

To enable this service the Client's provider assigned IP range is directed through an external system. Mitigation is then activated automatically for the duration of a detected attack.

6.5 Latency

Transit routing will be adjusted to enable the service which may have a minimal impact on latency. The DDoS mitigation action itself will not add more than 0.5 microseconds latency to delivered traffic.

6.6 Service Continuity

In the event of individual DDoS protection node outages, traffic may follow a higher-latency path than it otherwise would to pass through the next available mitigation node to maintain protection.

In the event of total DDoS service failure or inability to reach any DDoS protection nodes, traffic will continue to be forwarded through other internet transit routes without DDoS protection.

6.7 Monitoring

Node4's core infrastructure is monitored on a 24/7 basis. Our monitoring will detect large scale DDoS attacks which are not immediately or accurately mitigated by the DDoS protection service.

For an additional fee, Node4 can also monitor Client premises equipment (CPE). Several levels of monitoring are available based on Client requirements.

6.8 Unmitigated DDoS attack

In the event that a volumetric DDoS attack takes place on the Node4 network core, attacks not mitigated by this service or Node4's core network mitigation, will be prioritised as a Priority 1 issue, as they will likely impact all Clients.

Where a DDoS attack is unable to be mitigated by the service and disrupts the Node4 Network, Node4 may take action to discard traffic destined to the target IP addresses so that the attack does not disrupt the flow of traffic to other IP addresses.

6.8 Maintenance window

Where Node4 plans to perform essential works Node4 will endeavour to perform such works during low traffic periods and will endeavour to give the Client at least five (5) days prior notice. In the event of emergency works or a Service Affecting Incident, Node4 will aim to provide notice in advanced and as much advanced notice as possible.

This notice may be provided on N4Status (www.n4status.co.uk) rather than a direct notification. Clients can subscribe to status updates on the N4Status website to receive automated direct notifications.

6.10 Service exclusions

Node4 will validate the service configuration as part of the setup works. However, testing the service with a DDoS attack by either Node4 or the Client is not possible and not permitted.

The DDoS Protection Service neither offers nor provides:

- Load balancing of traffic or of the functionality of any Service
- Direct access to Node4 network security (except and to the extent allowed in the case of Self-Mitigation) or engineering staff
- Archival and storage of log files beyond thirty (30) days
- Security Incident response, forensics and investigations

- Legal case preparation, PR incident support
- Security consulting services
- Security reporting and analysis
- Permanent filtering or cleaning of traffic

Where any of the above services are provided by Node4, they are provided as additional services not subject to the terms and clauses in this document.

7. Incident management

7.1 Incident handling

Incidents are handled as outlined in Incident Management Schedule Document.

7.2 Fault duration

All Incidents recorded by the Node4 monitoring system will be reconciled against the corresponding Service Ticket raised by the Service Desk. The exact Incident duration will be calculated as the elapsed time between the Service Ticket being opened and the time when Service is restored.

7.3 Hours of support

Node4 DDoS Protection as a Service includes Gold level support, as detailed in the table below.

Support Hours	
Gold	Priority 1 and 2 - Support hours 24/7 Priority 3,4 and Service Request - Support hours between 7am and 7pm weekdays, excluding bank and national holidays

7.4 Incident priority

Each new Incident will be assigned a priority level by the Service Desk based on the following definitions. These levels allow us to prioritise resources and escalate where appropriate.

Priority	Description
1 – Critical	A major Incident resulting in total loss of service.
2 – High	A major Incident resulting in a severe service degradation or loss of service to a significant percentage of users.
3 – Medium	A minor Incident resulting in a limited or degraded service or a single end user unable to work.
4 – Low	General, single user with degraded service, non-service affecting support.
5 – Service Request	Request for a change to an existing service or system, a request for information or simple questionnaire to be completed.

7.5 Time to repair

Node4 aims to respond, update and resolve Incidents in relation to the Node4 DDoS Protection as a Service within the following times

Priority (Number are in hours)	P1	P2	P3	P4	Service Request
Response / Acknowledgement	0.5 Hours	1 Hour	2 Hours	4 Hours	12 Hours
Commencement	1 Hour	2 Hours	4 Hours	N/A	N/A
Frequency of Updates	1 Hour	2 Hours	12 hours if Resolve / Target to Fix exceeded		
Resolve / Target to Fix	4 Hours	8 Hours	12 Hours	36 Hours	60 Hours

Resolution times in the table above do not apply where there is a Client Responsible Incident, a Third Party Attributable Incidents or events outside Node4's reasonable control, any incidents including these aspects will be excluded from reporting provided.

All priority 1 & 2 Incidents should be raised via the Service Desk by a phone call. Should a priority 1 or 2 incident be raised via the portal or e-mail, the Client is required to follow this up with a corresponding phone call to enable work to commence immediately on the issue.

Acknowledgement refers to an automated service which generates a response and alerts engineers of

a service failure; or where there is dialogue between the client and the engineer.

Service Requests outside of the support contract, or Service Request implemented outside normal business hours these will be dealt with as chargeable projects.

8. Service availability

Node4 will provide the Client with Service Credits, as set out below, for the failure to meet the following target:

8.1 Service availability objective

The service availability objectives of this service are detailed below:

Service	Availability
DDoS Mitigation Platform Availability	99.95%

Service availability is calculated monthly on a per service basis using the following formula and expressed as a percentage:

Total Time - Unavailable Time x 100%
Total Time

8.2 Service credits

Credits will only be provided for failure to meet the availability levels set out above.

With respect to any service outages that entitles the Client to receive a credit, the amount of the credit will be calculated as follows based on the duration of unavailable time beyond the applicable threshold time:

Availability	Service Credits as % of Monthly Service Charge for DDoS Protection service
>= 99.95%	0%
< 99.95% - 98.50%	5%
< 98.50% - 96.50%	10%
< 96.50%	20%

Where a Monthly Review Period incorporates part of a month, any Service credit will apply to a pro-rated Monthly Fee. Service credits will be calculated monthly, aggregated and credited to the Client on a quarterly basis. If a Service is cancelled during a Monthly Review Period, no Service credit will be payable in respect of that service for that Monthly Review Period. The Client must claim any Service credit due to a failure to meet the Service levels, in writing, within twenty one (21) business days of the date at which the Client could reasonably be expected to become aware of such failure. The Client shall not be entitled to any Service credits in respect of a claim unless and until Node4 has received notice of the claim in writing in accordance with the above. Should Node4 require additional information from the Client, the Client shall assist, and shall not be entitled to any Service credits until Node4 has received all the information it has reasonably requested.

8.5 Exclusions to payment of service credits

Service credits will not be payable by Node4 to the Client in relation to the Service Availability for Incidents or disruptions to the Service caused by any of the following:

- The Incident, action or negligence of the Client, its employees, agents or contractors;
- The Client failing to comply with Node4's Standard Terms and
- Conditions;
- An Incident in, or any other problem associated with, equipment connected on the Client's side of the Node4 Network Termination Point, except where such Incident or problem is directly caused by the action or negligence of Node4, its employees, agents or contractors;
- Any event described in Clause 12 (Force Majeure) of Node4's Standard Terms and Conditions (Schedule 1);
- A failure by the Client to give Node4 access to any equipment after being
- requested to do so by Node4;
- Planned Outage during any Maintenance;
- Any DDoS attack type that the platform is not able to effectively mitigate.

Service credits are not applicable for more than one breach of any targets outlined in this document arising from the same occurrence.

The provision of Service credits shall be the sole and exclusive remedy for the failure to meet targets for the service. Node4 shall have no additional liability to the Client.