NTT

Global IP Network | Service brochure

DDoS Protection Services

Global IP Network

Solutions to Protect Your Network From DDoS Attacks: DPS Control, DPS Core, DPS Detect, DPS Max, and DPS Max Plus

A world of cyber insecurity

Record numbers of consumers are going online for commerce, news and video entertainment. Exciting technologies such as IoT and virtualization are changing businesses and industries. But a more connected world also means more avenues for criminals to exploit with increasingly sophisticated cyberattacks. Internet-centric businesses and enterprises simply cannot afford to let their guard down, with such breaches having the potential to shut down networks and cost millions. Making protection a central feature when launching new products and services therefore remains a must – and one of the most critical business concerns of the moment.

Distributed denial of service (DDoS) attacks

At the top of the list are DDoS attacks, which have become a regular threat to the online business community. These can strike at any time – potentially leading to devastating effects on your network, damaged assets and big revenue losses. And they are growing in size, frequency and complexity – some have compromised hundreds of thousands of devices. Stamping these out before they can create real damage is therefore essential.

Volumetric attacks

Volumetric attacks are designed to overwhelm a host or network and make it unreachable. These types of attacks typically come from compromised devices or the exploitation of certain network protocols, often resulting in some sort of collateral damage and making the network inaccessible to more than just the intended target. They include:

- TCP SYN flood attack
- UDP flood attack
- ICMP flood attack
- Reflection attack

Application layer attacks

Application layer attacks are well-crafted attacks targeting a specific service on the host. These can be difficult to detect, as they look like a legitimate connection, but are often filled with garbage requests. Because of the numerous tools available for these types of attack, such as the Low Orbit Ion Cannon (LOIC) tool, they have become even more popular among hackers, and include:

- HTTP GET attacks
- HTTP POST attacks
- SSL attacks

State exhaustion attacks

These attacks can be volumetric and/or application layer in nature, often represented by a slowloris attack tool of HTTP-GET or SSL attacks.

A proactive approach to network security

We fully understand the need to stay ahead of these increasingly complex threats. That’s why we take a proactive approach to stopping them, not a reactive approach once the damage is already done. Our security products are geared to support multithreat security environments, and we offer customized options, letting you choose the support that best fits your organization’s cyberdefense strategy.

We also listen to your specific security needs to help you make the best choice. You can rest assured that we have the ideal team to support you: our dedicated Network Security Team has an average tenure of 10-plus years, providing truly in-depth expertise. Combined with the backing of our Tier 1 Global IP Backbone, this makes our security offering second to none.

DDoS Protection Services (DPS)

Our DDoS Protection Services (DPS) offer a comprehensive, tiered approach to DDoS mitigation – depending on the type and level of protection you want. These options give you the chance to get the protection that best fits your defense strategy, whether you want a basic, intermediate or high level of support. And if you do require strong protection, our services have the capabilities to deal with large-scale attacks, redirecting and cleaning traffic through our mitigation platform. So get in touch with us and defy the criminals before they can deny your service.

DDoS Protection Services options

Basic

DPS Control

- ACL Support

DPS Core

- Attack mitigation
- ACL support

Intermediate

DPS Detect

- Attack detection
- Self-initiated mitigation
- ACL support

Advanced

DPS Max

- Auto-Mitigation
- Attack detection
- Self-initiated mitigation
- ACL support

DPS Max Plus

- Enhanced Attack Diversion
- Auto-Mitigation
- Attack detection
- Self-initiated mitigation
- ACL support

DPS Control

DPS Control is our entry-level service. Using this service, you can define permanent access control lists (ACLs) to block the network from certain types of traffic, as determined by you. So if you do not need full mitigation assistance, but still want a robust service that you can really rely on for basic protection, this could be the option for you. This service offers the following features:

Permanent ACL support

- Support for ACL up to 50 lines
- Standard and emergency ACL change support

DPS Core

Our next level of protection is DPS Core. As well as offering a range of extra features, an additional layer of assurance is provided by the support from our Network Security Team – the very same team that defends our network from attacks. Using state-of-the-art technology in response to a mitigation request, our team can rapidly analyze an attack and take any necessary countermeasures to snuff it out – such as identifying key attack vectors, filtering traffic and rerouting it to our mitigation platform for scrubbing. Get this option if you want a swift, effective response to malicious DDoS activities. In addition to the basic features in DPS Control, this service includes:

Access to Network Security Team

As a DPS Core subscriber, you'd have direct access to our highly capable Network Security Team, so you can stay up to date during mitigations.

Attack mitigation

Our Network Security Team takes a multilayered approach to attack mitigation and will use a variety of tools and techniques, including scrubbing of attack traffic using our mitigation platform.

Portal and reporting

Our exclusive DPS Portal provides access to mitigation reports and the relevant history

DPS Detect

Want an even higher, more thorough level of support? DPS Detect might be the answer. On top of all the great features offered by DPS Core, it adds services such as detection capabilities to notify you of potential attacks. From the DPS Portal, you can initiate a mitigation, review your detection history and past mitigation reports, and request configuration changes. So for a full DDoS protection service that covers all the bases, get DPS Detect.

The features below are included with DPS Detect and DPS Max:

Attack detection

Based on thresholds you have defined, you will be alerted of potential attacks through the DPS Portal, and (if you choose) by email or syslog.

Self-initiated mitigation

In the DPS Portal, you can initiate a mitigation based on an active detection alert, or by specifying the target IP address.

DPS Max

DPS Max combines our resources, expertise and mitigation strategies to protect clients affected by DDoS attacks. DPS Max includes attack detection and automatic mitigation, and is supported by our Network Security Team – the same team responsible for defending our network from attacks.

Auto-Mitigation

When notified of a possible DDoS attack, the platform will start a mitigation, redirect traffic to our mitigation platform, and stop the mitigation once the attack has ended. This is all done automatically, with no action or intervention required from you.

Introducing DPS Max Plus

This is our most comprehensive offering for DDoS Protection. DPS Max Plus includes all of the DPS Max features and adds Enhanced Attack Diversion.

Enhanced Attack Diversion

This is the announcement of the /24 covering the attacked IP address into the global routing table to divert traffic to NTT for mitigation. To divert traffic, NTT uses BGP's "more specific path" by announcing the /24 of the /32 under attack, and traffic is redirected to the closest of 13 mitigation platform locations for mitigation using anycast routing. Customers will be required to create a RPKI Route Origin Authorization with AS2914 as an authorized origin.

Service Level Agreements

100% DPS Platform Availability
(DPS Core, Detect, Max, Max Plus)

Mitigation Response Time

- 30 minutes for telephone, email, or Customer Portal to the NTT NOC (DPS Core, Detect, Max, Max Plus)
- 15 minutes when utilizing the "Request Mitigation" function of the DPS Portal (DPS Core, Detect, Max, Max Plus)
- 2 minutes when utilizing the "Start Mitigation" function of the DPS Portal (DPS Detect, Max, Max Plus)
- 2 minutes when utilizing Auto-Mitigation (DPS Max, Max Plus)

ACL Change Response Time
(DPS Control, Core, Detect, Max, Max Plus)

- 1 business day for standard change requests
- 30 minutes for emergency change requests

NTT

For more information and updates on the Global IP Network:

Global IP Network
AS2914

GinNTTnet

Visit our website
www.gin.ntt.net

Speak to our
experts