Internet Initiative Japan

Internet Initiative Japan Inc.

Phone 03-5205-6310 E-mail press@iij.ad.jp URL https://www.iij.ad.jp/
Address Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan

For Immediate Release

IIJ Launches "IIJ DDoS Protection Service/Edge," a Managed Service for Protection from DDoS and APT Attacks

—Offering protection from DDoS attacks as well as other integrated functions that include APT countermeasures—

TOKYO—December 10, 2019—Internet Initiative Japan Inc. (IIJ, TSE1: 3774), one of Japan's leading Internet access and comprehensive network solutions providers, today launched its IIJ DDoS Protection Service/Edge, a solution that comprehensively detects and defends against DDoS, APT(*), and other cyberattacks.

*Advanced persistent threat (APT): A type of cyberattack that targets specific companies, infiltrates their corporate networks, and steals/destroys data over the long term

This security service defends user assets against cyberattacks by detecting security threats hiding in communications between user networks and the Internet. It uses a dedicated device, the Threat Intelligence Gateway, that is placed on the boundary (the network edge) between user networks and the Internet.

US-based NetScout Systems provides the Threat Intelligence Gateway device, which is equipped with the latest threat intelligence (threat-tracking data) generated from the firm's analysis of the massive volumes of data traffic over the globe-spanning Internet. The gateway device monitors inbound and outbound traffic at the boundary between user networks and the Internet. While protecting public-facing systems on user networks from DDoS attacks and unauthorized access, the device also monitors transmissions to the Internet from dedicated work PCs, MFCs, and personal devices on corporate networks. To determine threat levels, it applies its threat intelligence to transmissions to phishing sites and C&C servers, and to communications from devices infected with malware or remote operation tools, making it a practical solution to advanced targeted attacks. Through its subscription-based managed security service, IIJ offers complete support to users who install the gateway device, from consulting services to set-up, operation, monitoring, and maintenance.

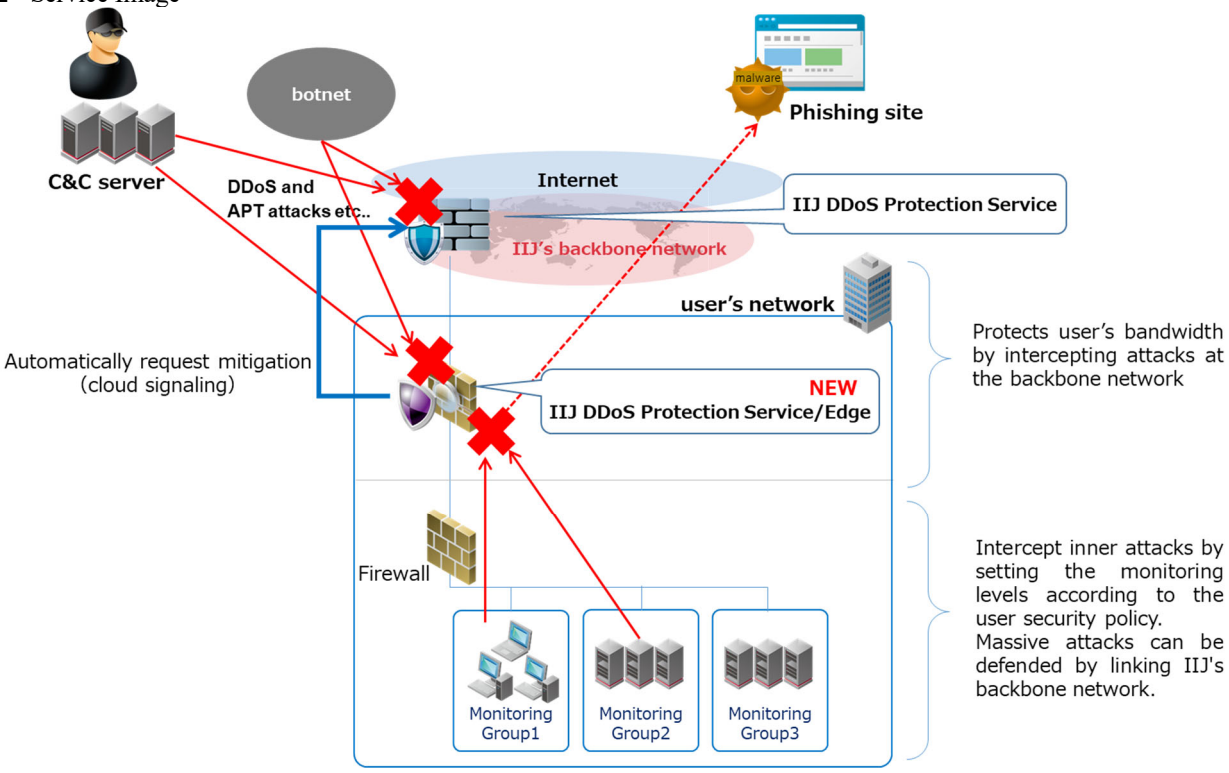
■ Background

IIJ offers its DDoS Protection Service to detect and defend against terabit-level cyberattacks through distributed installations on backbone networks. Through this protection service, IIJ identifies large-scale, Internet-based attacks every month. However, attacks have recently come to use methods that hinder detection and protection. For instance, slow HTTP attacks(*) use small numbers of packets to blend in with routine communications, leading to a rise in attacks that slip through backbone-side detection. Meanwhile, with APTs, attackers infiltrate user networks to steal or destroy data over the long term. These attacks use clever tricks, including reconnaissance, to ensure that network administrators do not notice the infiltration and instructions, disguised as routine communications that are sent to malware installed on user networks.

Users demand multilayered defense strategies that can respond to such increasingly sophisticated attacks. To create environments that can always defend against reconnaissance and infiltration attempts, these strategies must include security countermeasures installed at the boundaries of user networks, not just on backbone networks.

*Slow HTTP attacks: Security attacks that occupy server devices for the long term and interfere with operations by transmitting data extremely slowly

■ Service Image



■ Service Highlights

・ A defense against advanced cyberattacks that uses threat intelligence

The Threat Intelligence Gateway is equipped with threat intelligence accumulated through US-based NetScout Systems' Active Threat Level Analysis System (ATLAS). ATLAS generates threat data daily, using massive volumes of data on traffic gathered worldwide (equivalent to one-third of all Internet traffic). Using this threat intelligence, the gateway examines communications that occur between the Internet and user networks to determine threat levels.

IIJ plans to combine NetScout's threat intelligence with the intelligence data available at IIJ's Security Operation Center (SOC) to enable more advanced detection and protection capabilities for threats that impact Japanese corporations.

・ Multilayered defense strategies

Defense strategies that use gateway devices are not impenetrable against DDoS-type attacks that threaten user network connections by sending massive volumes of communications. Therefore, this service offers multilayered defenses by automatically rerouting (cloud signaling) to IIJ DDoS Protection Service, which detects and defends against cyberattacks on IIJ's backbone networks. This automatic connection occurs when the gateway device receives traffic above a threshold (bps/pps) its users set. Intercepting large-scale attacks at the backbone network level protects user bandwidth.

*This function is available only through the Hybrid service option.

・ Defense level settings for monitoring traffic

To conform with their security policies, users can create monitoring groups for systems, including email or web systems, and set appropriate defense and security strength levels for each group. Administrators can see the status of device defenses and traffic on a dedicated administration screen, and also output monthly summaries and response history reports to PDF to include in their monthly reports.

■ Service launch date December 10, 2019

■ Sample pricing (management fees)

Initial fee JPY437,000

Monthly fees Stand-alone: JPY292,000 Hybrid: JPY146,000

*The Hybrid option offers automatic connections (cloud signaling) with IIJ DDoS Protection Service.

*Users may deploy their own gateway devices or buy/rent them through IIJ.

*All prices shown do not include tax.

To expand its service options, through which its customers can safely use the Internet without having to worry about threats, IIJ continues to employ its wizSafe brand, a security business brand based on the idea of "making safety a matter of course."

Endorsement

NetScout welcomes the announcement that IIJ will offer Arbor Edge Defense (AED) as a part of their industry leading Managed Security Service. IIJ's layered approach to DDoS protection ensures that their customers will be protected, no matter what type of attack they face. With an increase in both application layer attacks, as well as outbound security threat, AED's award winning technology will assure that IIJ's customers stay connected and available.

Jeff Buhl
Vice President, Asia-Pacific Region
NetScout Systems, Inc.

About IIJ

Founded in 1992, IIJ is one of Japan's leading Internet-access and comprehensive network solutions providers. IIJ and its group companies provide total network solutions that mainly cater to high-end corporate customers. IIJ's services include high-quality Internet connectivity services, systems integration, cloud computing services, security services and mobile services. Moreover, IIJ has built one of the largest Internet backbone networks in Japan that is connected to the United States, the United Kingdom and Asia. IIJ was listed on the First Section of the Tokyo Stock Exchange in 2006. For more information about IIJ, visit the IIJ Web site at https://www.iij.ad.jp/en/.

The statements within this release contain forward-looking statements about our future plans that involve risk and uncertainty. These statements may differ materially from actual future events or results.

For inquiries, contact:
IIJ Corporate Communications
Tel: +81-3-5205-6310 E-mail: press@iij.ad.jp
https://www.iij.ad.jp/en/