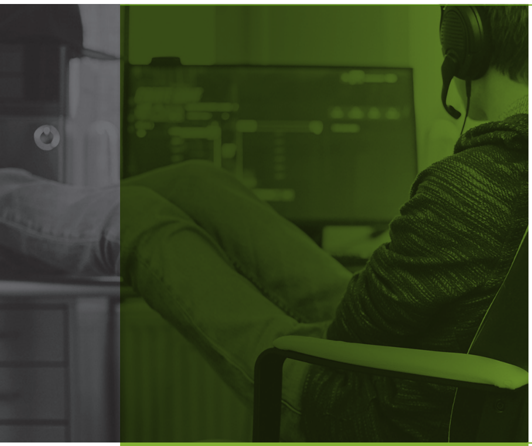

i3D.NET PERFORMANCE HOSTING

CLOUD SERVICE PROVIDER REDUCES IMPACT OF GLOBAL DENIAL-OF-SERVICE ATTACKS BY APPROXIMATELY 98 PERCENT

Summary

Company:
i3D.net

Industry:
Service Provider

Business Challenges:
- *Growing global demand for capacity of low-latency gaming cloud services*
- *Increasing distributed denial-of-service (DDoS) attacks on its services*

Technology Solution:
- *vSRX Virtual Firewall*
- *Juniper Sky Advanced Threat Prevention*

Business Results:
- *Effective attacks reduced by over 90 percent*
- *Lower service costs*
- *Easy to deploy and upgrade solution in remote locations*

i3D.net is a managed hosting provider based in Rotterdam, in the Netherlands. It provides services to more than 30,000 customers including dedicated servers, cloud services, colocation in its data centers, and gaming services. i3D.net has more than 10,000 servers in 26 data center locations worldwide, and it operates a core backbone across Europe and the United States which is connected to over 1600 peers on the world's largest Internet exchanges. Founded in 2004, i3D.net ranks among the fastest growing companies in the Netherlands.

"i3D.net found its high-performance DNA in the gaming industry," explains Stijn Koster, Chief Executive Officer at i3D.net. "Today, we provide capacity to enterprise game publishers on a global scale, where latency, performance, and security—especially limiting attacks at scale—are critical. A single game can use thousands of servers worldwide, with some highly demanding users. And now, more and more enterprise clients are turning to us as well, because they understand that if we can deliver these service levels to gamers, we can meet their cloud service needs too."

Business Challenge

"We had two main challenges," recalls Stefan Ideler, Chief Technology Officer at i3D.net. "The first was an ever growing demand for bandwidth and performance, particularly lower latency. The other big challenge was managing the security of our services."

i3D.net hosts projects in regions suffering from attacks on an hourly basis and if gaming services are affected, it will generate high profile coverage on social media platforms.

"Attacks on the PC platform were our biggest challenge," says Ideler. "PC gamers tend to be more competitive and community organized. Sometimes communities attack these game platforms to try and give themselves an advantage. However, we needed to protect all other platform players too, so we had to solve the problem on a huge scale. Frustrated gamers make sure their voices are heard on social media—so the performance of our services is very transparent. We have to deliver."

> *"We are still seeing attacks coming at our services, but effective attacks are down by over 90 percent. And, of course, it's also reduced the amount of trouble tickets we have to resolve, lowering our service costs."*
>
> - Stefan Ideler, Chief Technology Officer at i3D.net

i3D.net had successfully combatted previous distributed denial-of-service (DDoS) attacks, which produced high volumes of traffic to congest its connections, by filtering traffic from its transit providers. Yet now it was facing application-specific attacks using UDP traffic. “Traditional approaches were failing,” explains Ideler. “Most enterprise firewall-based solutions rely on filtering TCP traffic, which didn’t help. Also, many of the locations we needed to protect are remote from us. We operate in markets where it’s not easy to import equipment and rapidly adapt our security environment, so the gameplay of tens of thousands of gamers was being disrupted.”

i3D.net wanted to find a way to deploy and manage sophisticated firewalls rapidly at any of its sites, without shipping dedicated hardware to the location.

“Working with Juniper was an experience of real cooperation. They were always thinking of us and what would be the best solution for our problems. It was a very positive experience. And using Junos OS as a single operating system with one CLI across the full range of Juniper solutions makes for an easy learning curve on the new solution.”

- Stefan Ideler, Chief Technology Officer at i3D.net

Technology Solution

i3D.net considered using a scrubbing service, which would require it to send traffic to a centralized data cleansing station, where traffic is analyzed and malicious traffic is removed, but the redirection has a latency impact and it would have been expensive. Instead, it looked at firewall technologies and decided that a virtual firewall solution was the perfect answer.

i3D.net deployed Juniper Networks® vSRX Virtual Firewall to deliver a complete and integrated virtual security solution that includes core firewall, robust networking, advanced security services at Layers 4-7, and automated life cycle management capabilities. It also installed Juniper Sky Advanced Threat Prevention, which uses real-time information from the cloud to provide malware protection and defend against sophisticated cyber crimes such as advanced persistent threats and ransomware. Juniper Sky ATP provides an extra layer of protection on top of antivirus and antispam tools, extending its defense beyond traditional security solutions by detecting never-before-seen malware attachments and stopping them before they hit their target.

“To be honest, we were a little doubtful initially that it could work, as we’d tried physical firewalls unsuccessfully in the past,” recounts Ideler. “But as it was a virtual solution we simply set up the firewall on an existing server in Brazil and started testing, and we were immediately impressed.”

i3D.net is known for its rapid deployment of servers all over the globe and with the vSRX, i3D.net can quickly and easily deploy new virtual firewalls at any new site. Every location can now be equipped with reliable state-of-the-art firewalling in a virtual form factor.

“Working with Juniper was an experience of real cooperation,” says Ideler. “They were always thinking of us and what would be the best solution for our problems. It was a very positive experience. And using Junos OS as a single operating system with one CLI across the full range of Juniper solutions makes for an easy learning curve on the new solution.”

Business Results

i3D.net has already deployed Juniper’s security solutions in Brazil, China, Dubai, Japan, The Netherlands, South Africa, and the United States, and as a result it has significantly reduced the impact of attacks. “We are still seeing attacks coming at our services,” explains Ideler, “but effective attacks are down by over 90 percent. Because the Juniper solution is virtual and easily upgradeable, it is ideal to deploy in these types of locations, many of which are remote to us. We can start small and upgrade as we need to. And, of course, it’s also reduced the amount of trouble tickets we have to resolve, lowering our service costs.”

i3D.net has worked with game developers to determine typical traffic characteristics for their applications to help create traffic profiles by region and rate-limit malicious attack vectors. The number and depth of filters in the Juniper solution has enabled i3D.net to tweak parameters at every level. The Juniper Sky ATP layer allows for fine-tuning of the geographic profile—the GeoIP—which helps to ensure that unwanted traffic doesn’t degrade the end-user gamer’s experience. “There is no reason we should have users based outside LATAM accessing a server in Brazil,” explains Ideler, “so we can rate-limit this unwanted traffic. That alone has reduced attacks by 50 percent, because the attackers can’t generate enough DDoS traffic from within the local country.”

“Frustrated gamers make sure their voices are heard on social media—so the performance of our services is very transparent. We have to deliver.”

- Stefan Ideler, Chief Technology Officer at i3D.net

Next Steps

i3D.net is currently deploying Juniper's virtual security solution in every location where it offers gaming services, and plans to offer the solution inside the same data centers to other clients who provide gaming services.

"We know the hackers will always work on new ways to attack us," concludes Ideler, "but for now we can stay ahead of them. And our enterprise customers have similar requirements. They can also benefit from Juniper Sky ATP's malware detection to prevent new ransomware attacks, for example. Like our gaming attacks, they can appear out of nowhere, but when they do, we know we will be ready."

For More Information

To find out more about Juniper Networks products and solutions, please visit www.juniper.net.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

Engineering
Simplicity