Zscaler offers comfortable and secure support to NEC Group’s 110,000 global cloud users

NEC Corporation (NEC), which develops business globally, has more than 300 group companies all over the world with 110,000 employees. The company is driving a cloud shift to enable work style innovations and DX (Digital Transformation). The reason for renewing our network infrastructure was to provide comfort and security simultaneously, when connecting to the cloud; and the company selected the Zscaler Cloud Security solution.

Enable a cloud shift that supports work style innovations and DX; and also considers sophistication and cloudization of internet gateway as its infrastructure

NEC Group is promoting a “social solution business” globally, that co-creates with customers and society to establish social values such as safety, security, efficiency and fairness. While aiming to create an efficient and sophisticated society in which we can live harmoniously and pleasantly, NEC Group is also accelerating its efforts toward “work style innovations” and “DX”. In this regard, it is necessary for all employees to shift their IT environment to the cloud, as well as promote a multi-device operation in order to realize collaboration and work execution in the digital space. The main idea was to migrate network infrastructure including internet gateway (Web proxy/Sandbox). “A secure cloud environment is essential to realizing a work style that is not constrained by time or place,” says Takeo Tagami, Management Information Systems Division, NEC.

“What we required from Zscaler Cloud Security was a combination of improved comfort and security enhancement within a cloud-centric IT environment that allows for multi-device usage. This was our concept requirement for the cloud security solution.”

NEC Corporation
Management Information Systems Division
Natsuo Tanaka, Manager

“One attractive aspect of Zscaler Cloud Security is that we can deploy the same secure environment designed at the head office in Japan to overseas locations. By connecting from an overseas subsidiary to Zscaler, the same secure environment can be achieved anywhere in the world. This also applies to mobile access, and we believe that it is also contributing to improved productivity through work style innovations.”

NEC Corporation
Management Information Systems Division
Takeo Tagami, General Manager

“The decisive factor in adopting Zscaler Cloud Security is that it enables secure Web access from anywhere, regardless of location or time. Additionally, we were able to provide a unified security policy across domestic as well as overseas locations.”

© 2020 Zscaler, Inc. All rights reserved.
Mr. Tagami, head of security operations, revisits the situation at the time: “When considering an environment where employees access the internet from both inside and outside the company, encryption of web traffic makes it difficult to detect various cyberattacks and malware downloads.” When the company’s internet communication was inspected, “About 90% of web traffic was already SSL. No matter how much you monitor web traffic using conventional security solutions, if you can’t see the SSL communication, it means that the content being communicated is hidden. Also, we found out that approximately 80% of malware communication were using SSL, which is often used for cyberattacks. So at that time, security solutions that did not support SSL visualization could not detect malware. When upgrading the internet gateway, we focused on answering the question: “What do we want to achieve?” One thing was to ease internet traffic by significantly shifting the IT environment from on-premises to the cloud. That is to say, application performance will not be interrupted by security regulations and will be able to facilitate and maintain a user-friendly state that does not result in diminished responsiveness even when the traffic drastically increases. Another thing was to enable analysis necessary to inspect web access for the purpose of strengthening security, and rapidly respond when cyberattacks occur. These two factors are the cornerstones for achieving both comfort and security. None of these could be achieved with traditional security solutions until now,” said Mr. Tagami. “In addition, the focus was placed on extending this value to overseas locations around the world in an effort to achieve the same security policy and countermeasure level. We did not consider deploying security solutions in Japan first and then later deploying to overseas locations, but planned to deploy on a global scale from the beginning, targeting a security solution that can adopt a globally unified environment.”

**Deployed Zscaler Cloud Security that enabled a globally unified security policy, as well as centralized management covering Japan and overseas locations**

In July 2017, the company decided to introduce Zscaler Cloud Security based on the renewed concept as it pertains to internet gateway. “Zscaler Cloud Security provided secure web access regardless of location or time. Moreover, it enabled a unified security policy not only in Japan but also overseas. Furthermore, its ability to achieve both performance and security around the world greatly influenced our decision in terms of infrastructure. These elements played a crucial role in the decision making process. In a nutshell, the ability to enable SLA for improved response performance which is essential to realizing comfort and being able to use the same tenant with the same settings at the nearest service DC (data center) from the global Internet environment, was key to achieving both comfort and security as we expand globally.

“The conventional approach was either to consolidate internet access in Japan (to have the web access environment built and operated in Japan, while enabling access from overseas locations), or to set up a web access environment in overseas locations in accordance with the policies established in Japan. However, the aggregation of internet traffic results in performance degradation which nullifies comfort. In addition, individual operations at overseas locations have created variations in security response levels (the number of cases in these locations are lower than the cases in Japan). To realize our security concept, we used the globally distributed DC of Zscaler to enable secured responses in a distributed manner, and centralize security management. The company deployed Zscaler Cloud Security in October 2017. By utilizing our know-how as a System Integrator (SLER) for many years, we built a system which entailed setting up a cloud environment, building communication equipment that facilitate connectivity from the company’s network, with the help of the Zscaler security solution as well as internal support. When creating the migration scenario, we leveraged Zscaler’s various functions and know-how. Also, when upgrading the environment for 100,000 users, it was necessary to minimize the task of end users as much as possible. We achieved this by combining our accumulated power: a network solution and the Zscaler solution. Although the adoption of the Zscaler solution was venturing onto new grounds for us, it has provided us with enormous support. Through PoC (Proof of Concept) and UAT (User Acceptance Test), we created a viable migration scenario. And for the last three months, we spent some time on user acceptance testing and went live in April 2018. The final switch was not for each location or organization, but for all domestic locations—we switched user traffic for approximately 100,000 employees simultaneously. In doing so, we reduced employees’ PC settings significantly, and contrived ways to silently install certificates for SSL visualization. Also in the unlikely event of trouble, we can switch back to each destination and each connection without bothering employees and minimize the impact on our business” (Mr. Tanaka).
The SSL visualization technology and scalability offered by the Zscaler Cloud Security Solution, improved employee comfort and security

After launching Zscaler Cloud Security in April 2018, there were some challenges due to the scale of migration. Continued measures were necessary after the transition. However, many users indicated that “during the switch they didn’t notice that the web proxy had been changed.” This was a good feedback for the members of the transition team who had tough days before and after switching. “The challenges faced during transition were a cause for concern, but we eventually moved into a stable period that was characterized by smooth internet connection and improved speed, most importantly, during peak periods, which were prone to slow internet connectivity and slower speed. It was nice to know that the users noticed this improvement and appreciated the efforts we put in. Also, there was the benefit of SSL visualization. By enhancing comfort while maintaining security, such as releasing technical SNS sites for research and developers and releasing YouTube for viewing business videos, which were previously subject to severe restrictions, many users’ perception of the IT initiative adopted by the information system department changed. We appreciate the fact that we were able to realize this concept by selecting Zscaler and contributed in offering our users more value.”

*Although web traffic doubled after a year and a half we are still maintaining a favorable condition. This goes to show Zscaler’s great value with respect to the ease of use which guarantees increased performance without the need for additional investment. Also, in the past, some content was invisible due to SSL communication, and we could not control/monitor in detail. For this reason, the only option was to block all useful sites and to give full access to some users who desperately needed to perform their jobs, but at risk. However, with Zscaler Cloud Security, it is possible to flexibly respond to incidents, such as allow only authorized users to log in and browse and prohibit random file upload. Also, depending on the cloud service, there are cases where it is possible to allocate different domains and URLs to each company, and we can select to allow full access to the company’s URL, allow access to the competitor’s URL when relevant departments request authorization, or prohibit the upload of free account URL that may be exploited by Shadow IT or malware. In addition, since the contents of the web access log can be checked in detail using SSL visualization, we have changed the rules for reliable IaaS from ‘regulating because we don’t know what they are doing’ to ‘no pre-regulation based on monitoring’. By visualizing SSL communication, we switched from the inconvenient state of prioritizing regulations on the risk side to a policy of using it freely, exercising control flexibility and secure status monitoring. The SSL visualization technology offered by Zscaler Cloud Security has gone a long way to improve employee comfort and security."

Deploy a secure environment designed in Japan to locations around the world

Following its domestic expansion, the company began full-scale implementation of Zscaler Cloud Security in overseas locations in April 2019. As of December 2019, the number of overseas users reached 6,000 and the company is aiming to deploy to 15,000 users by the end of 2020. “Until now, the policy for internet security management at overseas locations was developed in Japan, but the actual operation was left to the locals. As a result, the level of response was unassessable, and monitoring was challenging. There were some locations where we found it difficult to determine whether or not any security incident occurred, thereby limiting our coverage of individual locations. However, Zscaler Cloud Security does not require local equipment installation, and allows us to directly see the communication status/malware detection status at all deployed overseas locations. It’s easy to see which country’s network is dangerous or secure. According to the company’s internal rules, reporting is necessary when a security incident occurs. But this is only possible when we can detect and understand the cyberattack itself. If we cannot detect it, we cannot confirm its presence, which means we are unable to respond or establish a report.”

Web access response has improved to the level where it can be proven quantitatively. This has improved productivity in the company at large. “NEC has 110,000 employees in Japan alone, and with the existing on-premises solutions, it has always been a game of cat and mouse to handle the increasing traffic. Although we had initially improved our response level, it deteriorated significantly after several years. This triggered user complaints about the network. After switching, the download time was greatly reduced by 60-70%—Zscaler Cloud Security guarantees improved response performance to users. Therefore, reducing the need to constantly invest in managing increased traffic is a huge benefit for NEC.”
"Moreover, advanced analysis technology and know-how are required to detect increasingly sophisticated cyberattacks. By visualizing the local situation and globally expanding the sophisticated analysis system originally operated at the head office, we have been able to speed up risk detection and local alerts. Also, malicious communication can be promptly cut off centrally. If you want to deploy this kind of security infrastructure to overseas locations using on-premises solutions, you have to replicate the exact same solution at the head quarters in Japan in each overseas location. Aside from large-scale locations, it will be unrealistic to execute this in locations with very few employees. By simply connecting from existing local communication equipment or installing an application, Zscaler can provide a secure environment across all overseas locations similar to the environment designed at the head quarters in Japan. When looking at infrastructure deployment and maintenance, this is a very efficient option."

By shifting business tools to the cloud, secure internet gateway has become the core function of corporate networks

In the future, the network will change significantly. In order to drive a cloud-first strategy and multi-device usage, NEC Group is shifting its structure from the conventional on-premises data center-centric solution to a cloud-centric solution. The shift will mainly be to IaaS and PaaS, and some will remain on-premises. System-to-system communication that was previously executed at the data center, including the system that moved to SaaS and the company’s cloud environment, will be distributed on a different basis in the future. "At the end of 2019, about 100,000 employees moved to Office 365® Zscaler’s control function for Office 365® automatically improved connectivity. It was a very large traffic transition, but there were no performance problems". In addition to SaaS, the use of cloud platforms such as IaaS and PaaS will be accelerated in the future. "We believe that NEC Group employees will be able to use secure internet services from multiple devices wherever they need it, instead of using internet services on the intranet". In doing so, easy internet access should not be compromised, even for security sake. Compatibility is a prerequisite. Zscaler Cloud Security is responsible for monitoring internet access on network and user basis, managing by policy as well as dynamically determining "which cloud service will be used by which user." Standard business tools such as email scheduler, video conferencing, collaboration tools like SNS, Office 365® or core systems like Salesforce®, accounting, SCM, sales management etc., will shift to SaaS which is a major type of cloud service. Also, corporate IT needs to consider the migration of individual systems specialized for developing their environment and business. The shift will mainly be to IaaS and PaaS, and some will remain on-premises. System-to-system communication that was previously executed at the data center, including the system that moved to SaaS and the company's cloud environment, will be distributed on a different basis in the future. Zscaler’s roadmap shows an outbound CASB that will monitor and manage cloud-to-cloud communications in the future. This kind of functional enhancement adds more value to the solution. NEC Group has three pillars:

• Work style innovations, that frees employees from time and place
• DX (Digital Transformation), which uses the latest digital tools, and
• Information security to realize proper security

"In order to achieve these, internet connection will be the core function of the corporate network. By introducing Zscaler Cloud Security, which manages our network boundary with the cloud, it does only serve as a tunnel to facilitate migration to the cloud, but we have also positioned it as the core infrastructure for cloud utilization."

About Zscaler
Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.