CANALINI
CONSULTING GROUP

CUSTOMER CASE STUDY
LEGAL

Prestigious multinational law-firm modernizes and increases the security of their messaging environment by seamlessly migrating to Microsoft Exchange 2016 and leveraging Citrix ADC for advanced security and geo-redundancy.

CHALLENGE

A law firm employing more than 1,800 attorneys and staff was in the early stages of upgrading their Microsoft Exchange environment from 2010 to 2016. Previously, a Citrix ADC was used to load balance all connections to backend Exchange servers, but it was not performing any SSL Offload or authentication. While the Exchange 2010 environment was highly available in each local datacenter, the customer wanted additional inter-site redundancy, data center failover automation, and Exchange service connection standardization for their Citrix ADC. Our customer aimed to improve resiliency with a multi-site setup along with moving authentication and SSL Offload to Citrix ADC appliances to improve their network's availability and security posture.

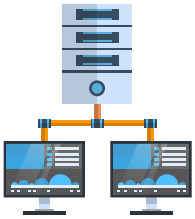
SOLUTION

Canalini Consulting put together an interdisciplinary team to strategize then configure a custom solution maximizing the capabilities of the Microsoft and Citrix platforms. Working together with the client's internal IT team, we were able to deliver a new set of system capabilities:

- Inter-site failover with Global Server Load Balancing (GSLB)
- Certificate-Based Authentication with Citrix ADC
- Secure Sockets Layer (SSL) Offload on Citrix ADC

RESULTS

- Inter-site failover with GSLB allows our customer to automatically and seamlessly switch over to a reliable backup and lessen or eliminate negative impact on users between two datacenters. Additionally, GSLB intelligently balances network traffic across their different mailbox servers to ensure a balanced workload that can greatly impact network latency.
- Certificate-Based Authentication configured with Citrix ADC using Kerberos Constrained Delegation (KCD) to enable one application to access resources hosted on a different server. Single Sign-On was also configured with Microsoft Exchange 2016 so users authenticate at the perimeter before gaining access to Microsoft Exchange resources.
- Secure Sockets Layer (SSL) Offload on Citrix ADC was configured for Microsoft Exchange to support Content Switching for multiple Microsoft Exchange services to be accessible through a single IP address. Citrix ADC is also able to view encrypted traffiic, site health, and take action based on policy expressions and AppExpert policies.



NETWORK

Automatic and seamless switch to a backup and balanced network traffic

IDENTITY ACCESS MANAGEMENT

An added layer of security to verify a user, device, or machine before granting access to the network

SECURITY

Be in the know with what your network activity and take policy-based actions to mitigate threats

CLOUD BASED. CLIENT FOCUSED.