CANALINI
CONSULTING GROUP

Case Study:

Enhanced Security & Resiliency for On-Premise Exchange

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 Off-load 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 and configure a custom solution that maximized 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 allowed 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 balanced network traffic across their different mailbox servers to ensure a balanced workload that greatly impacted network latency.

Certificate-Based Authentication was 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 authenticated 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 was also able to view encrypted traffic, site health, and take action based on policy expressions and AppExpert policies.

AVAILABILITY

Leveraged geo-redundant ADCs to deliver highly available Exchange services

IDENTITY ACCESS MANAGEMENT

Leveraged certificate-based authentication to verify user and device identity

SECURITY

Offloaded encryption and authentication at the perimeter for verification & authorization prior to granting network access

CLOUD BASED. CLIENT FOCUSED.