How We Secured a Healthcare Client's Network Mid-Acquisition and Divestiture

Written by: Usama Houlila, founder of CrossRealms

A large healthcare client, created through a partial divestiture of a much larger organization, contracted CrossRealms to design a solution for securing traffic to and from the larger organization in addition to securing the new entity with its varied Acute Care Hospitals and administrative offices. These types of projects present challenges from a technical, administrative, business and patient care perspective, to name a few, and have a direct impact on one another. For this case study, I will limit the scope to the technical solutions we created within the business challenges, which can be summed up as follows:

1- **How do we transition operational security for the new entity away from the larger organization?** In this case, the larger organization had a well-established Information Technology department with proven processes and procedures. The new entity must transition and potentially re-architect those functions
2- **Who will oversee the migration and how will the larger organization support those efforts?** In this case, the new entity took charge of leading the efforts and they quickly moved to secure the larger organization's commitment to the success of this project by defining and acquiring the necessary resources from the beginning
3- **What type of monitoring, alerting, logging controls need to be created/installed?** Most of the tools used by the larger organization were expensive and cumbersome. The new entity had a smaller footprint and could benefit from all the latest innovations in the security and logging space, such as Splunk.

When examining the above issues, it's important to remember that our healthcare clients face the challenge of our work coinciding with their patient care. Unlike any other vertical, there is a potential impact to people's lives and so every solution, assumption, or decision must be studied with a focus towards its potential impact on patient care. We decided to organize the project resources into three separate teams to improve our chances for success and speed up the process where possible. These teams consisted of:

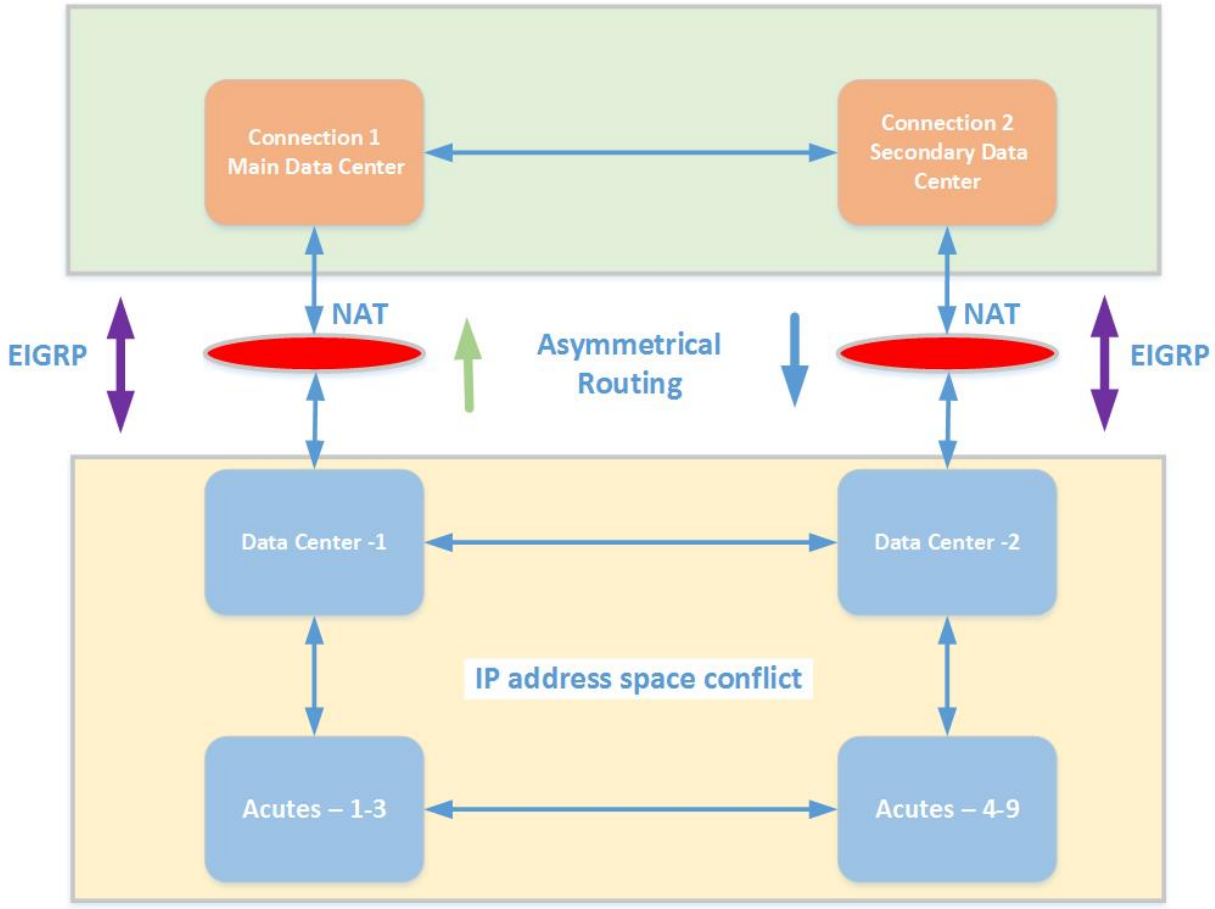
- A management team, led by a director level executive from the two organizations, including CrossRealms
- A project management team led by CrossRealms
- And a technical team led by a senior engineer from CrossRealms, and the two entities

Once the resources were assigned, we immediately initiated an assessment with the objective of identifying solutions for the above challenges in addition to any new items the assessment might uncover. Due to the sensitive nature and confidentiality of healthcare, I'm removing any technical details that are specific to this organization and instead focusing on the issues that were relevant for this project and are common within the healthcare industry.

The following were the major new items discovered by the assessment:

1- The “perimeter” with the larger organizations had firewalls running in Layer 3 mode with NAT enabled for many but not all the networks. Since these firewalls were managed by the larger organizations, any solution we designed had to avoid creating additional NAT for those segments otherwise we would break the applications.
2- Asymmetrical routing was used for some routes because those networks were part of projects in motion, i.e. long term and not close to completion. Since firewalls need to track connection oriented packets end to end, this scenario presented a challenge in how to create a solution that could be easily adjusted over time without having to redesign as the projects moved forward. In addition, this asymmetrical routing was designed using EIGRP between the core switches of the new entity and the larger Healthcare system so the firewalls needed to be able to pass EIGRP packets unhindered.
3- The combined new entity had some overlapping IP address space in their Acute Care Hospitals, and migration was not an option because it would be too disruptive and require orchestration with many vendors.

My initial reaction was to point out the fact that, technically, to get this accomplished, a compromise would be required by either consulting the other organizations to migrate their configuration away from NAT and/or consulting any of the Acute Care Hospitals to migrate their IP schema. In this instance, we were able to mitigate any compromises by using newer and more advanced firewall technologies in conjunction with a simple and elegant trick of CIDR (Classless Inter-Domain Routing). Let’s get to the details:



Choosing the firewall was the most significant initial decision because all the design solutions and run-books depend on that. We started by developing the requirements based on the assessment which were as follows:

1- The firewall must be able to function completely in Layer 1 (pass traffic without having to route and/or NAT), which would prevent any finger pointing in the future in case of a problem with an application, routing or otherwise. Another advantage for running firewalls in Layer 1 is that it allows for an extremely quick resolution if something were to break.
2- It must have the ability to execute NAT in Layer 1 since we still have to NAT selective traffic as an intermediate step.
3- It should allow for Asymmetrical routing while still inspecting traffic for proper controls.
4- It must possess the ability to pass multicast traffic (EIGRP).
5- The firewall must inspect traffic in-line at speeds exceeding 2 Gb/sec with all firewall features active.

The above requirements allowed us to narrow the choices based on technology, licensing, and price to either the Palo Alto Network firewalls and/or Fortinet. We consulted with our references in the healthcare field about their experience with both firewalls. Palo Alto networks proved more credible because the Fortinet firewalls have limited GUI capability in configuring NAT in Layer 1 and limited forwarding capability as part of their performance. One healthcare engineer informed me that they could reliably only expect 40-50% of the advertised capacity of the Fortinet firewalls.

Now that the firewalls were selected, we designed the solution based on a high availability Active-Active configuration. This allowed us to inspect asymmetrical and multicast traffic (both firewalls share the session information in active-active configuration) and since they are in Layer 1, we opted to allow any to any traffic first and then slowly added the necessary policies restricting traffic. One interesting fact about the Palo Alto firewalls is that they are able to inspect traffic for malware, viruses, and threats in Layer 1. So even though we started off with an allow-any-to-any policy, inspection and filtering started on day one.

The second item was IP address overlap and routing. After studying the routes carefully (1384 in total), we identified that some of the overlap was in the wireless networks, which was easy to change. The other overlap was with networks that were external to the organization. To resolve this issue, we created CIDR routing (much larger pool of networks) to route between the major hospitals. For the specifically overlapping networks, we created smaller IP address ranges that forwarded traffic in a way to avoid NAT.

Next, we had to resolve the issue of management and monitoring for this new security platform. Both items were addressed by installing a panorama-centralized management and monitoring tool for Palo Alto networks in conjunction with Splunk Enterprise Siem with log collection, correlation, alerting and analytics.

Finally, we needed to bridge the technical knowledge gap for the new organization with the Palo Alto security platform. To resolve that, we opted to have weekly four-hour training classes for six weeks covering the entire Palo Alto platform .These trainings proved to be extremely productive because we now had access to six more individuals that were then equipped to configure, deploy and troubleshoot any issues within an extremely short timeframe. Initially, the project was projected to take almost twelve months, but to the excitement of management and the CrossRealms team, the project was completed in seven months.

The account of this case is boiled down to a simplified version. The work consisted of a large IT department and a series of discovery, planning, and technical meetings. Though tedious, the meetings allowed us to discuss the assumptions together, decide on the best option for each phase forward, and assess the risks correctly. Some of the solutions incorporated came from the IT department of the new organization involved, which speaks volumes about the IT skillsets in healthcare