STAFF REPORT

March 2, 2022
File Number 0600-10

SUBJECT

CITYWIDE FIREWALL REPLACEMENT

DEPARTMENT

Information Systems

RECOMMENDATION

Request the City Council adopt Resolution No. 2022-40 authorizing the Deputy City Manager/ Director of Information Systems, or his designee, to procure and establish a citywide firewall replacement.

Staff Recommendation: Approval (Information Systems: Rob Van De Hey)

Presenter: Ken Conradie, Network Manager

FISCAL ANALYSIS

After analyzing several of the industry's top market solutions, comparing them extensively, and reaching out to industry peers to solicit feedback and review, it has been determined that the City of Escondido ("City") should upgrade its existing firewall by purchasing two Palo Alto PA-32060 Next Generation Firewalls which will cost $250,000.00. The decision matrix and a more comprehensive cost analysis is located within Attachment "A." The majority of this funding, $200,000, was approved by Council through American Rescue Plan Act (ARPA) funding on September 29, 2021 in Resolution No. 2021-146. The remainder of the purchase costs will be drawn from the Internal Services Funds from the Information Systems department.

BACKGROUND

The City's current SonicWALL firewalls are deployed at the core of the network and are the most important pieces of cyber security technology currently in place to protect the City's technology infrastructure. These firewalls provide the connectivity, security, and resiliency that the City needs to operate its municipal area network and effectively deliver digital municipal services to our community. Due to high costs and budget challenges we have been trying to delay our hardware replacement cycle of these units to ensure the highest return on investment (ROI) possible. When it comes to cyber security, the technology moves very quickly and while the software that these firewalls run is current, the hardware itself has aged to the point that it cannot effectively handle the increasing demands of the City. Staff is seeking approval to purchase the next five-year solution for the City. Additionally, staff has already identified a funding source for this project using a combination of ARPA funds previously approved by council for this purpose and Internal

Service Funds. The following information outlines the research and work performed to support this decision. There are also additional documents that support the research performed.

The current firewalls are underperforming. The City currently sees most of the symptoms and impacts of this in applications that do not tolerate latency, like staff working remote, video conferencing, and voice related technologies. City staff has experienced this during Zoom or 3CX virtual meeting with a choppy voice or pausing video. We are also seeing many staff facing web applications slow to a crawl, which also impacts productivity. The City puts high demands on its staff to produce and when technology slows them down, it affects morale. Although there are other examples like this, the last one to highlight is the risk behind cyber security attacks. Distributed Denial of Service ("DDOS") attacks are ever-evolving and our hardware is showing its age in attempting to keep up with the latest threats.

The City has been utilizing SonicWALL Next Generation firewalls for about seven years. Normal expected life of this type of network hardware is about five years. The SonicWALL SuperMassive 9200 series has been showing its age recently by underperforming and experiencing errors in processing traffic. The most concerning of which is that this security platform is falling behind current standards, which introduces a risk level beyond our tolerance.

The Network Systems Administration ("NSA") division of Information Systems has been working closely with our firewall vendor, SonicWALL, on a multitude of performance and firmware issues that have arisen over the past year or more. Our goal is to get the highest ROI possible on any investment the City makes. NSA Staff have reached the point that our continued work with the current firewall vendor (SonicWALL) is unfortunately no longer producing the results we need and expect, and we are experiencing major network slowdowns and outages as a result. After months of working very closely with the vendor on possible solutions, they are now recommending that we replace the aging SuperMassive 9200 pair with a pair of their latest generation model, the SonicWALL NSSP 13700. This model upgrade represents a major capital investment to the City – which triggered us to do our due diligence in comparing all best of breed products in this space.

In order to replace the aging hardware, we conducted research of the leading firewall solution vendors (including SonicWall) to find the right technology that meets the City's needs. This has been a several month's long process to identify the right path forward for the City. The process included reaching out to industry peers via MS-ISAC (Multi-State Information Sharing and Analysis Center® (MS-ISAC®), reviewing independent studies of the top brands, soliciting feedback and diligently evaluating and comparing the latest next generation firewall offerings from several vendors. In evaluating the options, we looked closely at the top three vendors that met our initial criteria. SonicWALL (NSSP 13700 that has been recommended), Fortinet (The FortiGate 1800F and the FortiGate 1101E) and Palo Alto (The PA-3260 and the PA-5220). NSA staff compared the specs of these platforms, and their alignment with various criteria we determined as critical for the needs of the City. After evaluating the solutions using an in-house developed comparison matrix (see attached), our research indicated that the Palo Alto units would likely best meet the needs of the City now and through the next hardware cycle. We found that Palo Alto

emerged as the most performant of the three, by employing a “single pass” architecture in evaluating traffic for threats and signatures they seemed to be more efficient than the other solutions. The other vendors’ products, although rated for similar performance, show slower ACTUAL packet processing times in real world applications, seemingly due to requiring multiple evaluation passes per packet. This clear distinction established the reason for a single full “proof of concept” evaluation as part of our due diligence.

After the above research, we identified a right-sized option in the Palo Alto PA-3260 model. Working with the vendor, Palo Alto, we then moved into a testing and “proof of concept” phase to get firsthand experience with this specific hardware as well as evaluate the vendor support during the “proof of concept” phase. This is a long process that usually is limited to a test environment, but our failing SonicWALL firewalls have forced us to push these Palo Alto test units into real world production use (with vendor approval). So far, the Palo Alto units have performed well above expectations.

As a result of this research and testing, Network & Systems Admin (NSA) Division is now recommending that the City purchase a pair of new Palo Alto 3260 firewalls to replace the current pair of SonicWALL SM9200 units. We are recommending this due to their superior performance, increased security processing power, and the improved reliability this will bring the City’s network.

RESOLUTIONS

a. Resolution No. 2022-40

ATTACHMENTS

a. Attachment “A” – Firewall Replacement Matrix