



## Legislation Text

---

**File #:** 18-336, **Version:** 1

---

Staff Report for a Resolution of the City Council for the City of San Leandro to Approve a Consulting Services Agreement with ConvergeOne for Cisco Next-Generation Firewall Installation, and to Make a Finding for a Sole Source Procurement of Cisco products

### **SUMMARY AND RECOMMENDATIONS**

Staff recommends that the City Council approve a resolution authorizing the City Manager to execute an agreement with ConvergeOne to install and configure upgraded Cisco firewall technology. Staff also recommends that the City Council make a finding for a sole source procurement of Cisco products. The contract is valued at a not-to-exceed amount of \$104,000.00.

### **BACKGROUND**

The City of San Leandro's network firewall infrastructure, which currently uses Cisco ASA firewalls, lacks features such as intrusion detection and prevention, as well as redundancy (the City does not have two identical firewalls in place), making the system vulnerable to attack and hardware failure. This project will install redundant Cisco Firepower 2140 Next-Generation firewalls enabling new threat defense systems and protection from hardware failure.

### **Analysis**

The City's current firewall technology is based on Cisco's flagship ASA firewall system. Traditional firewalls such as the Cisco ASA work by blocking or allowing network and internet traffic based on a set of rules established by the network administrator (i.e., IT Division). For many years this technology has been the gold standard in network firewall defense.

However, in recent years, new cyber threats to enterprise and municipal networks have evolved. In the most extreme example, the City of Atlanta was attacked by a ransomware virus that took down nearly 1/3 of City services, including core functions like police and courts. City officials now estimate it may cost more than \$9.5 million to fully recover from the attack.

While there is no way to 100% secure a network from being attacked, new technologies have been developed to help address today's cybersecurity threat landscape. These include algorithm-based malware detection, content filtering, and automated intrusion detection and prevention. Together these new technologies are commonly referred to as "Next Generation" firewall technology and these new services run in addition to traditional, rules-based systems.

The City's current network firewalls also suffer from a lack of redundancy and failover capability. While the City has one primary Cisco 5500 ASA Firewall, the backup firewall is a Cisco 5120. This was done for budgetary reasons because the Cisco 5120 is far less expensive than the 5500 series. However, because they are not identical models, the failover between firewalls is a manual process

and must involve human intervention. This makes the City's network firewalls vulnerable to service disruption in the event of a power outage or hardware failure.

For these reasons, staff recommends replacing these firewalls with redundant Cisco Firepower 2140 Next-Generation firewalls. The City negotiated an agreement, which includes the full suite of "Next-Gen" security functionality and includes identical models, which can be configured for automatic and instantaneous failover to avoid service disruption. The firewalls have a maximum throughput of 8Gbps/second, providing significant bandwidth and scalability for years to come.

The City worked closely with ConvergeOne to develop a highly detailed network design, and scope that meets the City's exact requirements. In the past, the City has received highly qualified, competitively proposals from ConvergeOne (formerly Strategic Products & Services) on similar network projects. Staff is highly satisfied with the outcomes of these projects in terms of quality, pricing, service, and support. Staff recommends awarding this project to ConvergeOne based on ConvergeOne's extensive and proven track record of success and knowledge of the City's existing infrastructure. Staff also recommends that the City Council make a finding for a sole source procurement of the Cisco products recommended by ConvergeOne, pursuant to California Public Contract Code section 3400.

### **Previous City Council Actions**

- Reso 2016-043 - On April 18, 2016, the City Council approved a Consultant Services Agreement with Strategic Products and Services, LLC. to install and configure upgraded network infrastructure in the amount of \$144,646.95.
- Reso 2017-102 - On July 17, 2017, the City Council approved a Consultant Services Agreement with Strategic Products and Services, LLC. to Upgrade the Cisco Telephony System for an Amount Not to Exceed of \$295,835.61.

### **Legal Analysis**

- The City Attorney's office reviewed and approved the consultant services agreements.

### **Fiscal Impacts**

- The total one-time cost of the firewall hardware systems is \$74,642.50. This includes a combination of hardware costs, software configuration, and design services.
- The ongoing hardware maintenance and Firepower subscription, which includes 24/7/365 support from the manufacturer, Cisco Systems, and algorithm-based malware detection, content filtering, and automated intrusion detection and prevention services will be \$29,112.75 per year. This cost will be partially offset by equipment currently under maintenance that will be replaced as part of this project.

### **Budget Authority**

- The Finance Director determined there are sufficient funds in the 2018-19 adopted operating budget, Account 688-13-121-7410 for \$104,000.00.

**PREPARED BY:** Tony Batalla, Information Technology Manager, City Manager's Office  
2600546.1