South Bay Cities Council of Governments

February 10, 2020

TO: SBCCOG Steering Committee

FROM: Chandler Sheilds, SBCCOG Staff

SUBJECT: Firewall/Unified Threat Management (UTM) to Support SBCCOG's Connection to South Bay Fiber Network (SBFN)

Adherence to Strategic Plan:
Goal D: Organizational Stability. Be a high performing organization with a clear path to long-term financial health, staffing continuity, and sustained board commitment.

SUMMARY OF REQUEST

In order for the South Bay Cities Council of Governments' (SBCCOG) office to join SBFN, it must invest in a firewall/UTM to accommodate and protect the increased bandwidth provided by the new network.

BACKGROUND & ANALYSIS

SBCCOG currently has a firewall/UTM, two wireless access points, and a switch to facilitate reliable and safe internet use, which were formerly managed by SBCCOG's I.T. managed services provider, SugarShot. However, the license for the firewall/UTM is due to expire in March and in order to facilitate the increased bandwidth provided by SBFN (as well as by the office's interim Internet Services Provider, Spectrum) the SBCCOG will need to immediately upgrade its firewall/UTM. SBCCOG's current I.T. managed services provider, SHARP has proposed two options that include 3-year licenses, which have different costs (see attached for details and cost-benefit analysis):

- Option 1: SonicWALL TZ 600 ($3,750)
- Option 2: SonicWALL NSA 2650 ($6,200)

SHARP recommends the second option and additionally purchasing a High-Availability (HA) as a secondary unit that acts as a complete failover unit if the primary hardware fails, which would bring the total cost for the three-year period to $8,250. Labor cost to install the hardware will require 2 hours of SHARP's time at a rate of $165/hour.

The City of Redondo Beach currently employs 2 SonicWALL NSA 5600s for its municipal facilities, which is a more robust model of the recommendation above.

RECOMMENDATION

SBCCOG Board Chair to approve firewall/UTM expenses and associated labor costs not to exceed $8,580 to support the SBCCOG office's role in SBFN.

Cost-Benefit Analysis – Firewall/UTM

I. Executive Summary

a. The purpose of this document is to outline the need for a Firewall/UTM appliance, including financial and other potential impacts to South Bay Environmental Services Center (SBESC).

b. A Firewall/UTM acts as a router (i.e., networking/Internet), as well as a security appliance to protect the network from cyber threats on the perimeter of the network.

c. While it is more commonly called a "firewall," these devices are technically called Unified Threat Management (UTM) devices. A firewall is only one piece of software running on a UTM; a UTM includes many other security services and software for various forms of cyber threats.

d. On average, threat actors are present on a compromised network over 200 days before an organization becomes aware the threat exists. During this time, they are stealing data, inserting themselves into financial conversations (wire fraud), and encrypting data for ransom (ransomware) among other forms of attack.

e. Please see our "15 Ways" document (page 3) for a breakdown of the modern cyber attack surface, including what needs to be protected to prevent most security breaches.

II. Issue

a. As depicted in our "15 Ways" document, the evolution of cyber threats today warrants a layered approach to cybersecurity. Firewalls/UTMs are the most basic level of perimeter defense for a network.

b. A Firewall/UTM protects the entry point (or "gateway") to the network, which is SBESC's Internet connection in this case. The types of attacks prevented include: ransomware and other malware, botnet attacks, Distributed Denial-of-Service (DDoS) attacks, spam, and zero-day (not yet discovered) attacks among others.

c. Without a Firewall/UTM, the organization lacks the most basic defense against active attacks coming in through the Internet, as well as the necessary visibility to address precursors (indicators of potential security incidents) and proactively prevent attacks.

d. While an ISP modem/router or home router does not filter web content, a Firewall/UTM can. Not filtering content (e.g., pornography, drugs, weapons, alcohol/tobacco, etc.) can result in preventable personnel issues.

III. Recommendation

a. We recommend SonicWALL Firewall/UTMs for several reasons. Principally:

   i. They score very high in security testing.

   ii. They are popular, which means most technologies will have documentation on how to incorporate into a SonicWALL-managed network.

   iii. They are relatively inexpensive compared to other manufacturers.

b. **Option #1:** SonicWALL TZ 600 (with 3-Year Security Services & Support Licensing)

   i. The TZ series is SonicWALL's entry-level class of Firewall/UTMs.

ii. The TZ 600 is the most powerful of the TZ series, and it is appropriate to handle web traffic based on the number of users SBESC has.

iii. However, it does not have the advanced features that may be necessary in the future to fully utilize the eventual fiber network.

iv. Cost: Roughly **$3,750** (depends on available options)

c. **Option #2:** SonicWALL NSA 2650 (with 3-Year Security Services & Support Licensing)

i. The NSA series is SonicWALL's mid-range firewall series. It is the next step up from the TZ series.

ii. The NSA 2650 is the least expensive model in this series.

iii. However, it comes with advanced switching features, as well as the ability to connect fiber (1Gig/2.5Gig connections) directly into it.

1. This may be the best way to connect to the eventual fiber network.
2. We can investigate whether this is necessary if we can procure information regarding the fiber hand-off.

iv. Additionally, SBESC can purchase High-Availability (HA) - this is a secondary unit that acts as a complete failover unit if the primary unit fails.

v. Cost:

1. With HA: Roughly **$8,250** (depends on available options)
2. Without HA: Roughly **$6,300** (depends on available options)

d. Due to our 40+ year relationship with our distributor, we can procure these devices at rates well below retail cost and pass that savings on to SBESC.

e. These devices typically last five years, so a 3-year license is usually where we start in case SBESC needs to upgrade before the end of the device's life.

f. Alternatively, we can provide numbers for 1-year, 2-year, 3-year, 4-year, or 5-year licenses.

g. If budget allows, we highly recommend **Option #2 (With HA)**, as it will be the most future-proof and stable.

IV. Justification

a. The cost of a data breach for any sized organization is roughly $200,000 on average. That cost includes: cost for remediation, downtime, and reputation loss among others.

b. Unique to SBESC is the impact downtime may potentially have on the local environment. It is not difficult to intuit that what SBESC does is incredibly important, especially regarding health and economy.

c. Considering those factors, it is our expert opinion that the cost of potential data breaches far outweighs the nominal cost of procuring a Firewall/UTM.

V. Team

NAME	POSITION	RESPONSIBILITIES
Vertis Hayes	SHARP, Project Engineer	Configure and deploy hardware
Nick Champagne	SHARP, Project Manager	Keep project on schedule
Chandler Sheilds	SBESC, Environmental Services Analyst	Confirm satisfactory deployment

15 Ways To Protect Your Business From A Cyber Attack!

SHARP®

SHARP BUSINESS SYSTEMS

□ Security Assessment

It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?

Date: ________________

□ Spam Email

Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.

□ Passwords

LOGIN

****

Apply security policies on your network. Examples: Deny or limit USB file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.

□ Security Awareness

Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.

Did you know?

1in5 Small businesses will suffer a cyber breach this year.

81% Of all breaches happen to small and medium sized businesses.

97% Of breaches could have been prevented with today's technology.

□ Advanced Endpoint Detection & Response

Protect your computer's data from malware, viruses, and cyber attacks with advanced endpoint security. today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script based threats and can even rollback a ransomware attack.

□ Multi-Factor Authentication

Utilize Multi-Factor Authentication whenever you can including on yournetwork, banking websites, and evensocial media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected

□ Computer Updates

Keep Microsoft, Adobe, and Java products updated for better security. We provide a"critical update" service via automation to protetion your computers from the latest known attacks.

□ Dark Web Research

Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials have been posted for sale.

□ SIEM/Log Management (Security Incident & Event Management)

Uses big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements

□ Web Gateway Security

Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds - before they reach the user.

□ Mobile Device Security

Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.

□ Firewall

Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!

□ Encryption

Whenever possible, the goal is toencrypt files at rest, in motion (think email) and especially on mobile devices

□ Backup

Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP.

□ Cyber Insurance

If all else fails, protect your income and business with cyber damage and recovery insurance policies.