

שדרוג מערכת FIREWALL
מפרט טכני להצעות מחיר
חיים שרף

פרויקט:
מסמך:
כתיבה:

נספח ה' לתנאי המכרז - מפרט טכני מיוחד (נספח א' לחוזה)

מכרז להספקה והטמעת
מערכת חומת אש (Firewall)
והספקת מוצרי אבטחת מידע



דצמבר 2009

תוכן העניינים

פרק 1 – כללי

פרק 2 – תאור מצב קיים

פרק 3 – טכני - דרישות מערכת

פרק 4 – מימוש

1. כללי

- 1.1. אחוזות החוף בע"מ (להלן: "החברה") מזמינה בזאת להציע הצעות להספקה והטמעת מערכת "חומת אש" (Firewall) והספקת מוצרי אבטחת מידע (להלן: "הפרויקט").
- 1.2. מערכת ה-Firewall צריכה לספק את מרכיבי האבטחה הבאים :

- Firewall
- IPS
- Proxy
- Mail-Relay
- URL-Filter
- Content-Checker
- SSL-VPN
- מערכת ניהול
- מערכת OTP

• מערכת הקלטות ל-VPN Session

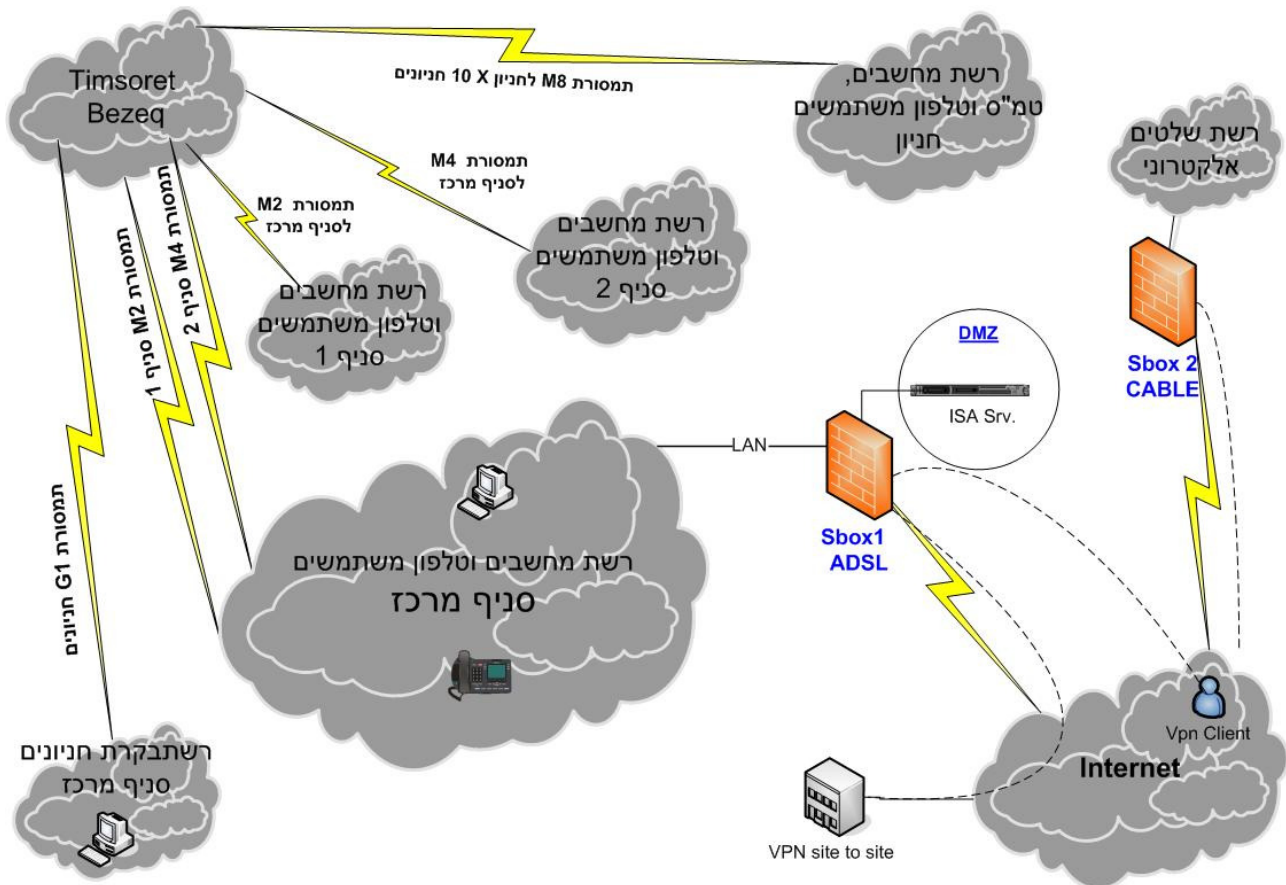
• רישיונות, עידכוני תוכנה, עידכוני חתימות

• תוספות והתאמות מיוחדות הנדרשות לצורך אינטגרציה

- 1.3. תמצית ההצעה (תמצית מנהלים), יש לצרף "תמצית מנהלים".
- על תמצית המנהלים להיות מדויקת, תכליתית ולהכיל מידע ממוקד וענייני שיסיע בבחינת ההצעה לפרוייקט כולל תמצית תועלות, יתרונות וכדומה.
- 1.4. המערכת צריכה לענות על כל הדרישות המפורטות בבקשה זה וכן לענות על התקנים והסטנדרטים המקובלים בתחום אבטחת המידע.
- 1.5. המענה למפרט הטכני יוגש במענה מותאם באופן מלא לסעיפי המפרט (כל תשובה תנתן במסגרת הסעיף שלגביו היא רלבנטית כולל הסברים ותרשימים נדרשים, חלוקת הסעיפים תשמר כפי שהיא).
- 1.6. טכנולוגיה
- 1.6.1. ההצעה תכלול נתונים טכניים וספרות רלוונטית של כל הציוד המסופק הנכלל במערכת.
- 1.6.2. הציוד המוצע יהיה ציוד חדש בלבד ובעל גרסאות התוכנה המעודכנות מטעם היצרן.
- 1.6.3. כל המוצרים והיישומים (חומרה / תוכנה) יהיו מוצרי מדף הכוללים תמיכה ושירות של היצרן או נציג היצרן בארץ.
- 1.7. יש לפרט ולספק פרטים מלאים על מפרט חומרה / תוכנה למערכת המוצעת.

2. תאור מצב קיים

2.1. תרשים רשת – מצב קיים



2.2. רכיב ה- Firewall הקיים מיושם באמצעות שני רכיבי S-BOX (כבלים ו-ADSL).

2.3. רכיב ISA-2004 משמש כ- Proxy ועבור שירות OWA למשתמשים חיצוניים מהאינטרנט. פתרון ה- ISA-2004 הקיים אינו עונה לדרישות האבטחה של הלקוח לכן המציע נידרש לספק פתרון חדש ולא להתבסס על המערכת הקיימת.

2.4. ברשת מתגי LAN מסוג Nortel L2.

2.5. מתג ראשי (Backbone) מדגם Nortel-5510 בתצורת L3. ברשת סיגמנטציה פנימית באמצעות VLAN, קישור ה- VLAN's נעשה באמצעות המתג הראשי.

- 2.6. מתגי Nortel הינם מדגמים שונים (2526, 470, 460, 5510, 5520).
- 2.7. שרתים ותחנות קצה מבוסס מערכת הפעלה Microsoft.
- 2.8. שרת דואר ארגוני Exchange-2003.
- 2.9. נעשה שימוש בתשתית Terminal-Server 2003 עבור גישה למערכות מהאינטרנט ומשתמשים פנימיים מהסניפים
- 2.10. ברשת כ- 7 שרתים מרכזיים.
- 2.11. ברשת מוגדרים כ- 50 משתמשים פנימיים.
- 2.12. נעשה שימוש בתוכנת אנטיורוס - Symantec.
- 2.13. מרכזיית טלפונים מבוססת מרכזית IP של חברת Nortel דגם BCM 400 הפועלת ע"ג סיגמנט VLAN ניפרד.
- 2.14. הסניפים מקושרים באמצעות קווי תמסורת L2 לרכיב FCD (או OS בעתיד) של "בזק" המותקן באתר הראשי.
- 2.15. חניונים – כיום פועלים 10 חניונים ממוחשבים הכוללים מערכות מחשב, טלפון וטלויזיה במעגל סגור. החניונים מקושרים באמצעות קווי תמסורת למרכז. עיקר המידע שעובר ע"ג קווי התמסורת כיום היינו Video ממצלמות האבטחה.
- 2.16. "רשת בקרת חניונים" – רשת ניפרדת המיועדת לניהול מיחושב חניונים. בכל חניון קיימת מערכת מחשבים ואפליקציה מרכזית המדווחת למערכת הניהול במרכז.
- 2.17. "רשת שילוט אלקטרוני" – רשת תקשורת לניהול שילוט אוטומטי המציג את זמינות החניון. העדכונים מתבצעים ע"ג תשתית הסלולר של "אורנג". ניהול המערכת מתבצע באמצעות VPN Client.

3. פרק טכני – דרישות מערכת

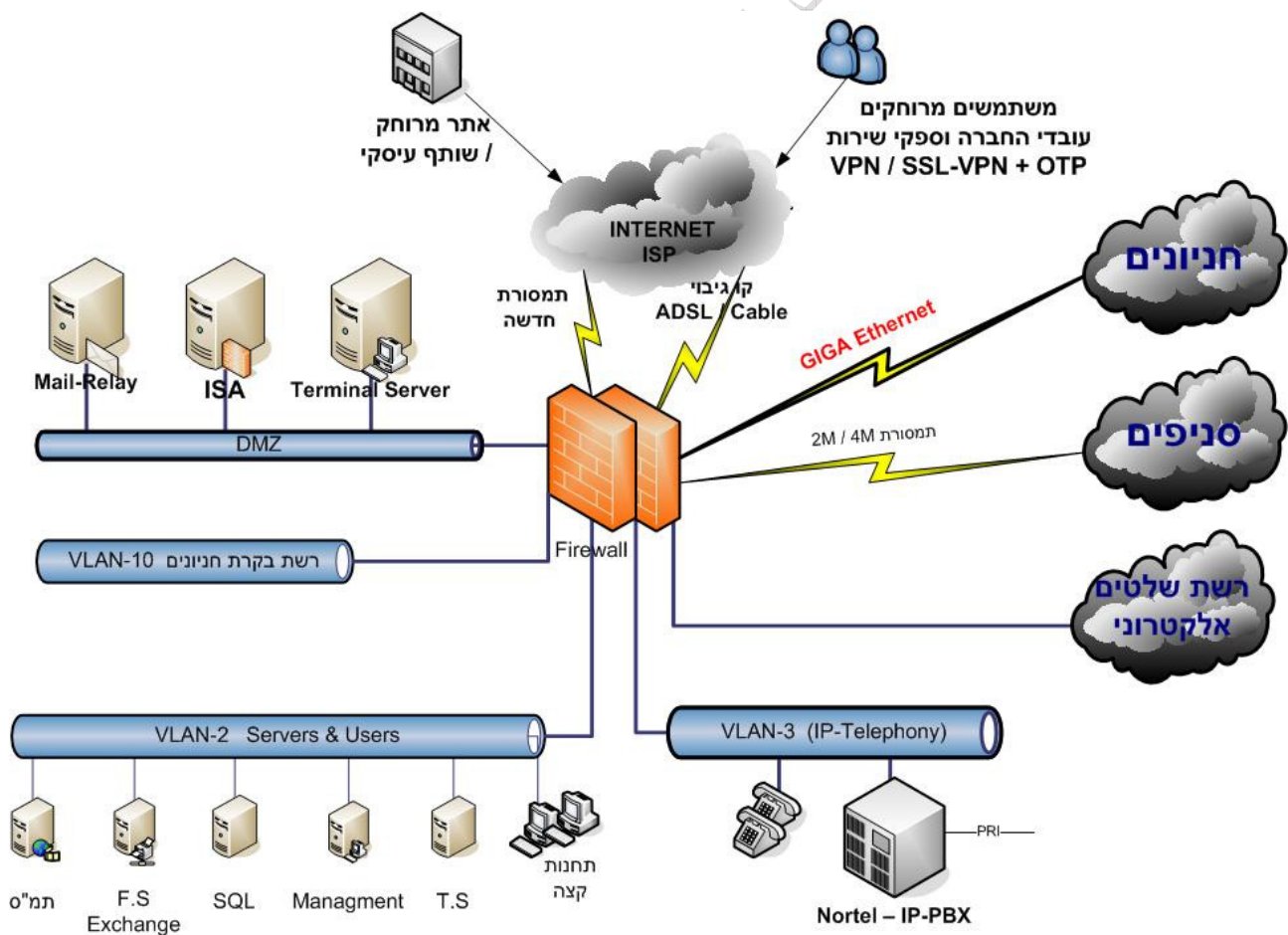
בפרק זה על המציע להתייחס לכל סעיף וסעיף ולפרט בהרחבה לגבי מערכת ה-Firewall, רכיבי הפתרון וכיצד יסופק השירות במסגרת הפרוייקט והתמיכה השוטפת במערכת.

3.1. ארכיטקטורה - רשת חדשה

3.1.1. החברה מבקשת ליישם ולשדרג את הרשת הקיימת כפי שמתואר בסעיף 2.1, לרשת

החדשה כפי שמתואר בסעיף 3.1.4.

3.1.2. תרשים רשת חדשה



3.1.3. החברה מבקשת להדגיש, התרשים בסעיף 3.1.3 היינו תרשים כללי בלבד לצורך התייחסות המציע. המציע נידרש להתייחס ולאשר את תאימות הפתרון הטכני שהציע לדרישות החברה ולהציג תרשים המתאר את פתרון מערכת ה-Firewall שהציע.

3.1.4. להלן הסברים לתרשים רשת חדשה, על המציע להתייחס בהרחבה:

3.1.4.1. חניונים וסניפים מקושרים כיום בתמסורת L2 למתג LAN מסוג Nortel בסניף הראשי, המתג מוגדר ב-L3 ומבצע ניתוב בין רשתות ה-VLAN'S. יש לפרט כיצד ברשת החדשה התמסורות יקושרו למערכת ה-Firewall שאמורה לבצע ניתוב L3 על בסיס חוקים שיקבעו עם החברה.

3.1.4.2. ברשת הפנימית קיימת סיגמנטציה באמצעות מתג LAN מסוג Nortel לסיגמנטים הבאים: VLAN-10 (voice), VLAN-3 (data), VLAN-2 (מרכז בקרת חניונים).

3.1.4.3. יש לפרט כיצד במערכת ה-Firewall החדשה יבוצע הניתוב ב-L3 ב-FW וניתן יהיה לאכוף חוקים שיקבעו עם החברה.

3.1.4.4. קו האינטרנט כיום ADSL, בכוונת החברה לשדרג את הקו לתשתית תמסורת מהירה יותר ולהשתמש בקו ה-ASDL (או הכבלים) כגיבוי – יש לפרט כיצד המערכת החדשה תתמוך בדרישה זו.

3.1.5. המציע נידרש להתייחס לממשקים ולביצועי הרשת החדשה ולספק הסבר טכני מפורט כיצד מערכת ה-Firewall החדשה תתמוך בנושא.

3.2. מפרט דרישות למערכת Firewall

להלן דרישות מנדטוריות למערכת Firewall, המציע נדרש המציע להתייחס בפירוט ולהציג את אופן המימוש והרכיבים לפתרון כל אחת מהדרישות המפורטות להלן. ניתן להרחיב את המענה באמצעות הוספת מסמכים טכניים של היצרנים – כנספחים בלבד ולא לצורך המענה הטכני.

3.2.1. בסעיף זה נידרש המציע להציג ולפרט באמצעות תרשימים את ארכיטקטורת הפתרון ורכיבי מערכת ה-Firewall שהציע במענה הטכני.

3.3. רכיב Firewall

3.3.1. רכיב ה-Firewall יהיה מסוג Stateful Firewall של אחד מהיצרנים הבאים:

Cisco, Checkpoint, Juniper, Fortinet או שווה-ערך.

- 3.3.2. בסעיף זה יש לפרט בהרחבה על יצרן דגם, גרסת ה- Firewall המוצע ותכונותיה. ניתן לצרף בנוסף מסמכי יצרן – כנספח בלבד.
- 3.3.3. יש לספק מכלול Firewall בתצורה של שרידות מלאה. הגיבוי יתבצע בתצורה של Active-Passive או Active/Active ע"פ החלטת החברה.
- 3.3.4. יש לפרט את יכולת התמיכה בתצורת שרידות מלאה בין מודולים באותה מכונה ובין מודולים בין שתי מכונות נפרדות. לדוגמא: גיבוי ספקי כח, רכיב IPS, SSL-VPN, וכו'.
- 3.3.5. יש לספק Firewall עם תמיכה בשכבות L2-L7.
- 3.3.6. יש לספק Firewall עם תמיכה בפרוטוקולי ניתוב סטאטי ודינאמי – RIP, BGP, OSPF.
- 3.3.7. יש לספק Firewall עם 8 מבואות נחשת בתקן Ethernet:
- מינימום שתי מבואות של GIGA Ethernet, ועוד 6 מבואות נוספים של 10/100Mbps.
- 3.3.8. יש לספק Firewall עם תמיכה ברחבה של ממשקי Ethernet נוספים. יש לפרט כיצד ימומש.
- 3.3.9. יש לספק Firewall עם תמיכה ב-Vlan's. תמיכה ב-Vlan's נידרשת עבור קישור אתרים מרוחקים באמצעות תמסורת L2 לאתר הראשי. מערכת ה-Firewall תידרש לתמוך בניתוב הקישורים על בסיס חוקים שיקבעו במסגרת האפיון של הפרוייקט.
- בסעיף זה יש לפרט כיצד מערכת ה-Firewall החדשה תתמוך בדרישה זו לרבות התייחסות לממשקים בצידוד הקצה של בזק FCD (או OS), כתובות IP, ניתוב וכו'.
- 3.3.10. יש לספק Firewall עם תמיכה במינימום של 100 פרוטוקולים מובנים במערכת לצורך יצירת חוקים.
- 3.3.11. יש לספק Firewall עם תמיכה בחסימת קבצים מיישומי P2P ו- Instant messaging control לדוגמא: messenger, icq, Kazaa, Skype.
- 3.3.12. יש לספק Firewall עם תמיכה בהצפנת תקשורת: PPTP, L2TP, VPN (client vpn), IP-SEC, IPSEC VPN Tunnel. תמיכה בהצפנת תקשורת SSL-VPN, ניתן להציע גם כפתרון חיצוני לרכיב ה-Firewall – יש לפרט.
- 3.3.13. יש לספק Firewall עם תמיכה בפרוטוקול DHCP ו-DHCP-Relay.
- 3.3.14. יש לספק Firewall עם תמיכה ב-Multicast.
- 3.3.15. יש לספק Firewall עם תמיכה ב-VoIP ופרוטוקולי תקשורת נוספים לרבות SIP, H.323 וכו'.

3.3.16. יש לפרט כיצד תתמוך מערכת ה-Firewall בממשק בין מרכזית ה-IP של Nortel למשאבי הרשת בסיגמנט מערכות המידע (Exchange). בנוסף מערכת ה-Firewall נידרשת לתמוך בהעברת Voice לשלוחות טלפון IP מרוחקות באתרי הקצה.

3.3.17. יש לספק Firewall עם תמיכה בניתוב דינאמי בין קווי תקשורת ומעבר לקווי גיבוי באופן אוטומטי. לדוגמא: מעבר מתשתית תמסורת לקו גיבוי ADSL בקישור החינונים לאתר הראשי.

3.3.18. יש לספק Firewall עם תמיכה בזיהוי ומניעת ניסיונות תקיפה. יש לפרט יכולות הגנה ומניעת התקפות DoS / DDoS attack, Syn attack.

3.3.19. יש לפרט יכולת הגנה על תשתיות תקשורת אלחוטיות.

לדוגמא: במידה והלקוח יבקש לחבר למערכת ה-Firewall תשתית תקשורת אל-חוטית עבור גלישת אורחים לאינטרנט דרך קווי התקשורת של החברה.

3.3.20. יש לספק Firewall עם תמיכה בניהול רוחב פס באמצעות מנגנוני Bandwidth - management (download and upload), תמיכה בהפקת דוחות על עומסים בקווי התקשורת ויכולת אכיפה רוחב פס לפי סוג אפליקציה.

3.3.21. יש לספק Firewall עם יכולת שמירת לוג אירועים פנימי בשרת ה-Firewall לתקופה של 90 יום לפחות. במידה ולא ניתן לשמור לוג אירועים פנימית בשרת נידרש להציע פיתרון לשרת Syslog חיצוני (תוכנה בלבד).

3.3.22. יש לספק Firewall עם תמיכה בהגדרת משתמשים פנימי ויכולת סינכון מול LDAP חיצוני Microsoft Active Directory.

3.3.23. יש לספק Firewall התומך במנגנון הזדהות (One Time password) OTP עבור פתרון הזדהות חזק בגישה מרחוק של משתמשים / ספקים מהאינטרנט.

3.3.24. יש להציג מסמכי הקשחה למערכת ה-Firewall ו/או מסמכי Best Practices להקשחה של יצרן הציוד במידה וה-Firewall אינו מבוסס חומרה סגורה.

3.4 מפרט דרישות פונקציונליות ממערכת Firewall מרכזי:

3.4.1. כללי.

3.4.1.1. להלן דרישות מנדטוריות אליהן נדרש המציע להתייחס בפירוט ולהציג את הדרך והאמצעים לפתרון כל אחת מהדרישות המפורטות בסעיף 3.4.

3.4.1.2. במידה ושרת ה-Firewall אינו תומך באחת או יותר מהדרישות בסעיף 3.4, רשאי המציע להציע פתרונות אבטחה באמצעות רכיבים חיצוניים (ל-Firewall).

3.4.1.3. שיקולים נוספים – על המציע לקחת בחשבון שתינתן עדיפות למערכת עם מינימום רכיבים ומערכת קלה לתפעול ותחזוקה.

3.4.1.4. במידה ורכיב הינו חלק אינטגרלי משרת ה-Firewall שהוצע בסעיף 3.3, יש לספק פתרון שרידות מלא גם לאותו הרכיב כחלק ממכלול ה-Firewall. לדוגמא: במידה ורכיב ה-IPS מובנה בשרת ה-Firewall, נידרש לספק פתרון מגובה לרכיב ה-IPS בשני ה-Firewall שהוצעו בסעיף 3.3.

3.4.2. IPS

3.4.3. נידרש לספק (intrusion prevention) IPS – אקטיבי עם יכולת ניטור ושליחת התראה אוטומטי באמצעות המייל. יכולת מניעת התקפות DNS poisoning, port scanning, DDoS/DoS, וכד'.

3.4.4. נידרש לספק IPS עם יכולת זיהוי התקפות ע"פ חתימות ואנומליות.

3.4.5. נידרש לספק IPS עם עדכוני חתימות שוטפים מהיצרן.

3.4.6. רכיב ה-IPS נידרש לתמוך בקצב מינימלי של 300Mbps לפחות.

3.4.7. רכיב ה-IPS נידרש לתמוך בניטור תעבורה בין רשתות שונות (לדוגמא: רשת חניונים, אינטרנט וכד').

3.4.8. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה-IPS – יש לפרט.

3.4.9. SSL-VPN

3.4.10. נידרש לספק פתרון SSL-VPN כרכיב חיצוני או פנימי ב-Firewall. יש לפרט בהרחבה.

3.4.11. רכיב ה-SSL-VPN נידרש לתמוך ב-Reverse-Proxy לצורך ההפעלת יישומים מהרשת הפנימית (לדוגמא RDP, OWA וכד').

3.4.12. רכיב ה-SSL-VPN נידרש לתמוך בשלב ראשון ב-25 משתמשים רשומים עם יכול הרחבה ל-100 משתמשים ללא צורך בשדרוג חומרה אלא רישוי בלבד.

3.4.13. רכיב ה-SSL-VPN נידרש לתמוך בזיהוי משתמשים חזק על בסיס פתרון ה-OTP שהוצע.

3.4.14. רכיב ה-SSL-VPN נידרש לתמוך ביכולת הגדרת פורטל (תפריט) כניסה, לפי פרופיל משתמשים והרשאות גישה ליישומים הפנימיים.

3.4.15. רכיב ה-SSL-VPN נידרש לתמוך בהזדהות חזקה של משתמשים באמצעות רכיב OTP חיצוני ויכולת זיהוי המשתמשים באמצעות LDAP פנימי ו- חיצוני לדוגמא : Microsoft Active Directory.

3.4.16. יש לפרט כיצד רכיב ה-SSL-VPN יתממשק למערכת ה-OTP.

3.4.17. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה-SSL-VPN – יש לפרט.

3.4.18. Proxy

3.4.19. נידרש לספק פתרון Proxy עבור האצת מהירות הגלישה ושיפור חווית המשתמשים בגלישה לאתרי אינטרנט. יש לפרט.

3.4.20. פתרון ה-ISA-2004 הקיים אינו עונה לדרישות האבטחה של הלקוח המציע נידרש לספק פתרון חדש ולא להתבסס על המערכת הקיימת.

3.4.21. פתרון Proxy נידרש להיות עם Cache פנימי של 30 Giga לפחות.

3.4.22. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה-Proxy – יש לפרט.

3.4.23. Mail-Relay

3.4.24. יש לספק פתרון Mail-Relay לסינון ובדיקת תעבורת מיילים נכנסים ויוצאים לאינטרנט משרת Exchange הפנימי. הדגש העיקרי הינו על יכולת בדיקת וירוסים וסינון מיילים נכנסים. יש לפרט.

3.4.25. יש לספק Mail-Relay עם יכולת שילוב מספר מנועים של יצרנים שונים של Antivirus and Antispyware .

3.4.26. יש לספק פתרון Mail-Relay ל-100 משתמשים מבלי לשדרג את החומרה.

3.4.27. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה-Mail-Relay – יש לפרט.

3.4.28. Content Checker

3.4.29. נידרש לספק פתרון Content Checker עבור סינון ובדיקת תוכן ניכנס. יש לפרט.

לדוגמא: יכולת חסימה ע"פ קטגוריות, תמיכה בשפות לרבות עיברית וכד'.

3.4.30. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה-Content Checker – יש לפרט.

3.4.31. URL Filter

3.4.32. נידרש לספק פתרון URL Filter מרכזי. יש לפרט.

3.4.33. פתרון URL Filter נועד למנוע גישה לאתרים לא מורשים ע"פ מדיניות החברה.

3.4.34. פתרון URL Filter נידרש להיות עם עדכונים שוטפים מהיצרן.

3.4.35. נידרש לספק פתרון URL Filter עם יכולת חסימה ע"פ קטגוריות, תמיכה בשפות לרבות עיברית.

3.4.36. נידרש לספק פתרון ניהול והפקת דוחות לרכיב ה- URL Filter - יש לפרט.

3.5 דרישות ביצועים למערכת Firewall (הדרישה לכל רכיב Firewall בניפרד)

3.5.1. Firewall Performance - מעל 300Mbps

3.5.2. IPS Throughput - מעל 300Mbps

3.5.3. Firewall Packets Per Second - מעל 80,000

3.5.4. Concurrent VPN Tunnels - מעל 200

3.5.5. Max Concurrent Sessions - מעל 30,000

3.5.6. Max Security Policies - מעל 500

3.5.7. Max Security Zones - מעל 40

3.5.8. Max Virtual LANs per port - מעל 40

3.6 מערכת ניהול ובקרה

3.6.1. המציע נדרש לספק מערכת ניהול, שליטה ובקרה מרכזית למערכת החדשה. יכולת ניהול רכיבי המערכת באמצעות מערכת ניהול מלאה הכוללת: פתיחה וסגירת שירותים, הגדרה / גריעת חוקים, הפקת דוחות וסטטיסטיקה לפי בחירה, ניטור המערכת וזיהוי כשלים בזמן אמת וכד'.

3.6.2. יש לספק מערכת ניהול לרכיב ה- Firewall (סעיף 3.3) ורכיבים מסעיף 3.4 שהם חלק אינטגרלי מרכיב ה- Firewall.

3.6.3. המציע נידרש לפרט בהרחבה על יכולת מערכת ניהול השליטה והבקרה המוצעת.

3.6.4. יש לספק מערכת ניהול קלה וידידותית למשתמש.

3.6.5. יש לספק מערכת ניהול שתותקן בתחנת Console אחת עם יכולת שליטה מלאה ברכיבי המערכת המנוהלים.

3.6.6. יש לספק מערכת ניהול עם מנגנון ניהול הרשאות משתמשים ע"פ פרופילים, לדוגמא:

- Admin – בכל יכולות שליטה מלאה במערכת.
 - Operator – בעל יכולת צפייה בנתוני המערכת.
- 3.6.7. יש לספק מערכת ניהול לרכיבי המערכת המנוהלים באמצעות ממשק WEB מאובטח.
- 3.6.8. יש לספק מערכת ניהול מרכזית שממשק הניהול שלה יהיה רק באמצעות פרוטוקולי תקשורת מאובטחים כגון: SSH-V2, SSL-VPN. יש לפרט.
- 3.6.9. יש לספק מערכת ניהול שניתן להפיק ממנה דוחות מפורטים מובנים במערכת ודוחות שניתן להגדיר ע"פ דרישה.

O.T.P (One Time Password) 3.7

החברה מבקש ליישם פתרון הזדהות חזק של משתמשים מרשת האינטרנט. יש לספק פתרון מערכתי בלבד לתצורת גישה ב- VPN Client ו- SSL-VPN, להלן הדרישה הטכנית למערכת.

- 3.7.1. יש לספק פתרון אינטרטיבי למערכת ה- Firewall לצורך הזדהות חזקה OTP מרשת האינטרנט באמצעות פרוטוקול Client-VPN, SSL-VPN.
- 3.7.2. יש לפרט כיצד תתבצע האינטרגציה בין רכיב ה- OTP למערכת ה- Firewall וה- SSL-VPN המוצעת.
- 3.7.3. יש לספק מענה להזדהות של - 25 משתמשים בו זמנית.
- 3.7.4. יש לפרט יכולת הרחבה מעל 25 משתמשים, תינתן עדיפות לפתרון שדרוג באמצעות רישוי בלבד ללא החלפת חומרה.
- 3.7.5. יש לפרט ולספק פתרון הזדהות OTP באמצעות אחד או יותר מהפתרונות הבאים:
- SMS
 - USB Token
 - אחר ו/או שילוב של מספר דגמים של התקנים
- 3.7.6. יש לספק ממשק ניהול לרכיב ה- OTP. יושם דגש על פתרון קל לתחזוקה והפעלה פשוטה מצד המשתמש המרוחק.

3.8. מערכת הקלטה

החברה מבקשת ליישם מערכת הקלטה מרכזית לצורך הקלטה ותיעוד Session פעילות של משתמשים שנכנסו לרשת הפנימית מהאינטרנט (לאחר תהליך ההזדהות).

3.8.1. יש לספק פתרון הקלטה ל- Session של משתמשים המתחברים מהאינטרנט לרשת הפנימית דרך מערכת ה- Firewall .

3.8.2. יש לספק מערכת הקלטה לפרוטוקול RDP המשמש את החברה לצורך השתלטות מרחוק על תחנות קצה או שרתים. יש לפרט תמיכה בפרוטוקולים נוספים.

3.8.3. יש לספק מערכת הקלטת Session של שני משתמשים בו זמנית, יש לפרט יכולת הרחבה למערכת.

3.8.4. יש לספק מערכת הקלטה לכל רצף המסכים של פעילות המשתמש מרגע ההתחברות למערכת ועד ההתנתקות.

3.8.5. יש לפרט זמן הקלטה מקסימלי.

3.8.6. יש לספק מערכת הקלטה עם חוקים כך שניתן יהיה לקבוע לפי שם המשתמש שהתחבר מרחוק – כן או לא להקליט במערכת.

3.8.7. יש לספק מערכת הקלטה שתשמור את קבצי ההקלטה בפורמט הנתמך ב- Windows Media Player גרסה 10 ומעלה.

3.8.8. יש לפרט דרישות לתצורת מחשב (חומרה / תוכנה / מע' הפעלה) לצורך הפעלת המערכת. את המחשב תספק החברה.

3.8.9. יש לפרט באיזה סיגמנט תותקן מערכת ההקלטה במערכת ה- Firewall החדשה.

3.8.10. יש לספק מערכת הקלטה על ממשק מנהל מערכת כולל: הגדרות תצורה, הפעלה שוטפת, ניטור, הצגת הקלטות וכד'.

4. הגשת הצעות ומימוש

פרק זה מתאר את אופן הגשת ההצעה במכרז (בכפוף לאמור בתנאי המכרז) וכן את התהליך שבו תוקם המערכת, תוטמע ותופעל באתר החברה. הקמת המערכת, הטמעתה ותפעולה יעשו בהתאם לתכנית עבודה מפורטת כפי שתוסכם בין החברה למציע.

4.1. שיתוף פעולה

4.1.1. פעילות המציע תלויה במומחים טכניים של החברה אשר יהיו רשאים לפקח על עבודת המציע הזוכה.

4.1.2. המציע ישתף פעולה באופן מלא עם נציג החברה ו/או מפקח מטעמה המייצג את החברה.

4.1.3. המציע יעדכן את החברה בכתב בסטטוס התקדמות הפרוייקט.

4.1.4. המציע יעביר דו"ח סטטוס פרוייקט שבועי ללקוח.

4.2. המציע

על המציע לפרט בהצעתו כדלקמן:

4.2.1. פירוט בדבר כל הגורמים המעורבים בהצעתו, יצרן הציוד, ספקים מקומיים או/ו קבלני משנה, טיב הקשרים שלו עמם, חלוקת המטלות לפי נושאים והמבנה הארגוני של צוות הפרוייקט.

4.2.2. שם אחראי ההצעה אליו יפנו נציגי החברה בקשר להצעה ו/או שאלות טכניות בנוגע למענה.

4.3. צוות ההקמה

4.3.1. המציע יעסיק מינימום 5 עובדים מקצועיים בתחום אבטחת המידע והאינטגרציה.

4.3.2. המציע יתאר את מבנה צוות ההקמה המתוכנן לפרוייקט, ויצוין את הרכבו בהיבט של כוח אדם מקצועי והיכולות הטכניות של אנשי הצוות.

4.3.3. המציע ימנה מנהל פרויקט מטעמו, כגורם המוסמך מול מנהל הפרוייקט מטעם הארגון. יש לכלול בהצעה את שם מנהל הפרוייקט המיועד ואת קורות חייו, כולל מידע על ניסיונו בפרוייקטים דומים.

4.3.4. מנהל הפרוייקט מטעם המציע ישתף בישיבות מעקב של הפרוייקט בתדירות שתקבע. ישיבות המעקב יתקיימו במשרדי החברה.

4.4. במסגרת ההצעה יכללו השירותים הבאים:

4.4.1. תכנון הפרוייקט ושלב המעבר.

4.4.2. ניהול הפרוייקט.

4.4.3. הובלת המערכת על כל חלקיה, ביטוח, התקנתה והפעלתה באתר שתיעד לו לשם כך החברה.

4.4.4. אינטגרציה של המערכת עם כל מערכות החברה.

4.4.5. בדיקות קבלה.

4.4.6. תיק תיעוד והדרכה בדבר הפעלת הציוד.

4.5. פירוט העלויות

מחיר כל פריט בפרק עלויות יכלול בתוכו, בין היתר, את המרכיבים הבאים, ללא עלות נוספת:

4.5.1. מחיר כל רכיבי הציוד, החומרה והתוכנה

4.5.2. אספקה, הובלה וביטוח

4.5.3. כל ההיטלים והמיסים (למעט מע"מ)

4.5.4. התקנה והטמעה מלאה באתר החברה

4.5.5. ביצוע הגדרות והפעלה מלאה

4.5.6. אחריות ושירות באתר החברה לתקופה של 24 חודשים בזמני התגובה בהתאם להוראות הבקשה

4.5.7. הכנת מסמכי SOW ותכנון מפורט

4.5.8. השתתפות בישיבות תכנון מוקדם

4.5.9. תיעוד

4.5.10. הדרכה מלאה

4.5.11. עדכון גרסאות תוכנה וחומרה במהלך תקופת האחריות

4.5.12. כל דרישה אחרת המצוינת בבקשה או בהסכם ההתקשרות

4.5.13. בדיקות קבלה

4.5.14. המציע ייקח אחריות על מערכת אבטחת המידע הקיימת החל משלב ביצוע השדרוג (כלומר, במקרה של תקלה בציוד קיים המציע יטפל בתקלה על חשבון)

4.6. יישום כולל של המערכת

4.6.1. ביצוע הפרויקט יעשה בשלבים. בסיום כל שלב יוגשו לאישור החברה התפוקות והמסמכים הנדרשים לאותו שלב. המשך ביצוע השלב הבא יהיה מותנה באישור בכתב מהחברה לגבי השלמת השלב הקודם לשביעות רצונה. יתכנו שלבים שיבוצעו במקביל והכל בהתאם לתכנית העבודה שתאושר.

4.6.2. השירות הנדרש הינו ניתוח, תכנון מלא, הקמה והטמעה של המערכת, האמורה להחליף את המערכות הקיימות בחברה. על המציע יהיה להציג תוכנית שדרוג מערכת אבטחת המידע תוך ביצוע שלב המעבר ללא השבתה.

4.6.3. על המציע ללמוד (על חשבוננו) את מכלולי מערכות המידע של הלקוח לרבות מבנה הרשת כולל כתובות IP, השרתים, אבטחת המידע, ולהציג בפני המזמין מסמך תכנון מפורט ליישום הפרוייקט.

4.7. לוחות זמנים

עמידה בלוח זמנים הוא עקרון חשוב של הסכם היישום. המציע נידרש להקים את המערכת ברציפות ובתקופה שלא תעלה על האמור בסעיף 8 לחוזה. בסעיף זה יש לפרט ולהציג לו"ז כללי להקמת המערכת ע"י המציע.

4.8. מעבר למערכת המוצעת

המציע יפרט ויציג תוכנית פעולה מפורטת לניתוק מערכות התקשורת והאבטחה הנוכחיות המשמשות את החברה, וחיבור המערכת החדשה, תוך פגיעה מינימאלית בזמינות השירותים למערכות החברה ועובדיה.

4.9. מסמכי תכנון מפורטים

המציע הזוכה יכין תוכנית עבודה מפורטת (SOW) אשר תהיה כפופה לאישור החברה. בנוסף יכין המציע הזוכה מסמך תכנון מפורט (Detail Design) שיכיל שרטוטים מפורטים של הפתרון, השיטה, לוחות זמנים, שלבים, תיעוד ושירות. לכל שלב יצורף מערך בדיקות קבלה/ביצועים.

מסמך Detail Design יכלול לפחות את הפרקים הבאים:

1. תקציר מנהלים
2. תאור מצב קיים - סקר ומיפוי אתר (כתובות IP, VLANs, ניתוב, חוקים, פרוטוקולים וכד')

3. תוכנית עבודה וניהול פרוייקט המעבר (Roll-back, GANT LLD, וכד')
4. תכנון מערכת אבטחת מידע חדשה
 - תרשים רשת חדשה
 - תכנון מידור והפרדת סיגמנטים
 - תכנון ניתוב תקשורת ב-L3
 - תכנון קישור סניפים מרוחקים (ע"פ המתאר החדש)
 - תכנון ביצועי המערכת
 - תכנון שרידות מערכת
 - תכנון אינטגרציה כללית למערכת לרבות מערכות וממשקים חיצוניים ל-FW.
5. תכנון כתובות IP + VLANs + Protocols
6. תכנון חוקים על בסיס מצב קיים ודרישות נוספות של החברה
7. תכנון הגדרות וקונפיגורציה מערכת אבטחת מידע
8. תכנון הקשחת מערכות
9. תכנון גישה מרחוק של עובדים וספקים באמצעות VPN ובשילוב Token
10. תכנון מערכת שליטה ובקרה
11. פרק אינטגרציה ושילוב מערכות (כולל התייחסות לרכיבי אבטחת מידע נוספים, ציוד תקשורת, יישומים וכד')
12. תכולת ציוד חומרה / תוכנה לאספקה כולל מפרטים טכניים
13. דרישות מהמזמין (חשמל, תשתית כבילה, לו"ז להשבתת מערכות וכד')
14. לו"ז והתארגנות צוות הפרוייקט מצד המציע והמזמין
15. תוכנית בדיקות קבלת למערכת - Checklist.
16. נהלי תחזוקה ותפעול המערכת לדוגמא: חוקים, משתמשים חיצוניים וכד'
17. ניהול סיכונים – הערכת סיכונים תפעוליים וטכנולוגיים בפרוייקט.

4.10. הפעלת המערכת

ההתקנות באתר החברה יבוצעו לאחר הגעת הציוד ובדיקת תקינותו, בתיאום עם החברה. לכל שלב ביישום תוקצה תקופת הרצה שלאחריה יבוצעו בדיקות סופיות ומעבר לעבודה מבצעית.

4.11. בדיקות קבלה

4.11.1. לאחר התקנת הציוד באתר, יבדוק המציע את הציוד ואופן התקנתו לשם וידוא פעילותו התקינה ושילובו התקין במערכות החברה. מסירת הפרוייקט תתבצע רק לאחר אישור מבחני הקבלה על ידי החברה.

4.11.2. הבדיקות יכללו: בדיקת התאמת תעודת משלוח, בדיקת התאמת הציוד להזמנה ולמענה המציע, בדיקת אופן התקנת הציוד ופעולתו על פי מסמך התכנון המפורט שהגיש ואושר ע"י החברה (Detail Design), הרצת מערכת והשתלבות במערך המחשוב של החברה, בדיקת עומסים ומיפוי התנהגות המערכת, בדיקת שרידות והתאוששות, ניהול ובקרת מערכת, (בדיקות יכולת שליטה ובקרה בציוד וכד').

4.11.3. נציגי החברה יורשו להשתתף בתהליך הבדיקה לפי דרישתם טרם התחלתה.

4.11.4. על המציע לאשר שהחברה רשאית לבצע בדיקות חוסן נוספות (Pen-Test) למערכת טרום אישורה הסופי וזאת ע"פ שיקול דעתה הבלעדי. במידה וימצאו ליקויים – על המציע יהיה לתקנם כחלק מהפרוייקט ועל חשבונו.

4.11.5. בדיקות אינטגרציה - המציע יבצע יחד עם החברה בדיקות מערכת. החברה תהיה רשאית לבצע בדיקות אבטחה נוספות של הציוד לאחר התקנתו והמציע יעמיד איש מקצוע מטעמו לצורך סיוע בבדיקות החברה.

4.12. תפעול המערכת

4.12.1. המציע יפרט את הדרך בה יבטיח פעולה רצופה ותקינה של המערכת. הפירוט יכלול את מערך התפעול המלא של מרכיבי המערכת בשילוב המערכות הקיימות בחברה.

4.12.2. המציע יפרט כיצד תופעל מערכת הבקרה למערכת ה-Firewall וכלל רכיבי אבטחת המידע שסופקו בפרוייקט.

4.12.3. המציע יפרט את מערך התמיכה (Help Desk) שלו, לרבות כוח אדם, שעות פעילות, רמת שירות וכד'.

4.13. תיק תיעוד

המציע יפרט את תיקי התיעוד שיספק למערכת, דרכי השימוש בהם ונהלי הפעלתם. כן יוכן תיק תיעוד למערכת שיכלול בין היתר את המרכיבים הבאים: הסברים על המערכת, תצורה כללית של המערכת, נהלי הפעלה, נהלי הוספת שינויים במערכת, נהלי תחזוקה וטיפול מונע, פרטי נותן השירות, נהלי עבודה מול המוקד, נהלים לטיפול בציוד, תיעוד ציוד טכני, תיעוד יצרן.

4.14. הדרכה

4.14.1. המציע יציג תוכנית הדרכה מפורטת לכל סוג ציוד המוצע בפתרון.

- 4.14.2. ביצוע ההדרכה הינו באחריות המציע וכחלק בלתי נפרד מתמחור ההצעה.
- 4.14.3. מטרת ההדרכה להכשיר ברמה הטובה ביותר את מנהל הרשת של החברה התפעול הציוד.
- 4.14.4. ההדרכה תכלול – הדרכה תוך כדי שלב ההקמה (OJT) ובגמר הספקת המערכת הדרכה נוספת בהיקף 40 שעות. יש לפרט את מכלול ההדרכה שתסופק ע"י המציע לחברה.

4.15. סיום הפרויקט

סיום הפרויקט יאושר רק לאחר סיום אינטגרציה, הגדרות, בדיקות קבלה ותיעוד מלאים ולאחר אישור תקינות הציוד והמערכת ע"י החברה. החל ממועד זה תחל תקופת האחריות.

4.16. רמת השירות וטיפול בתקלות

- 4.16.1. המציע יתאר תהליך פתיחת תקלה בארגונו ומהלך הפתרון, הצעדים הננקטים בכל מצב ומשך הזמן לכל מהלך כאמור.
- 4.16.2. המציע יתאר תהליך תמיכה מרחוק באמצעות מוקד התמיכה.
- 4.16.3. המציע מתחייב לספק ציוד חדש, זהה או מתקדם יותר במידה ומתברר שלציוד קיימת בעיה עקרונית שפתרונה על ידו לא צלח. בעיה עקרונית תוגדר כבעיה שכל המאמצים בכלל זה החלפת רכיבים, שינוי הגדרות ושדרוגי תוכנה לא הביאו לכלל פתרון הבעיה.
- 4.16.4. המציע יהיה אחראי ויתקן כל תקלה שתתגלה ו/או תתרחש במערכת. כל התיקונים יתבצעו באתר החברה בלבד.
- 4.16.5. המציע ינהל רישום סטטוס פניות השירות, במידת הצורך יהיה ניתן לקבל סטטוס הטיפול בפניות. מספר הנכס יהיה המספר המוביל במעקב אחר הציוד.