ארכיטקטורת אבטחת מידע

מערכת שליטה, בקרה וקשר למענה חירום

Alpha Team · גרסה 1.0 · יולי 2026

מסמך זה מתאר את שכבות ההגנה במערכת, מהמכשיר בשטח ועד לשרתים. הוא מנוסח **ללא כתובות רשת, שמות מארחים או מיקומים גיאוגרפיים** של תשתית. פרטים אלה נמסרים בנפרד, לגורם מאושר, תחת הסכם סודיות.

1 עקרון התכנון

המערכת בנויה בשכבות עצמאיות. **כשל או פריצה של שכבה אחת אינם חושפים את השכבות שמתחתיה.** מכשיר גנוב אינו מקנה גישה לרשת; גישה לרשת אינה מקנה יכולת האזנה לקשר; והאזנה לקשר של ארגון אחד אינה חושפת ארגון אחר.

#	שכבה	מה היא מגדירה
1	**זהות המכשיר**	מי מורשה בכלל לדבר עם המערכת
2	**הצפנת קשר קולי**	מה עובר באוויר ומי יכול לפענח
3	**תעבורת נתונים**	TLS מול השרת ואימות לכל בקשה
4	**שכבת התקשורת**	APN פרטי · מנהרת IPsec · בקרת יציאה
5	**הרשאות והפרדה**	הפרדת ארגונים · תפקידים · אימות קולי

2 שכבת המכשיר — זהות ואספקה

לכל מכשיר בשטח **מזהה ייחודי וקבוע** הנקבע בעת ההקצאה ונשמר בצורה עמידה לאיפוס. המזהה משויך לארגון יחיד; מכשיר שאינו משויך אינו מתקבל לרשת אלא נכנס לרשימת המתנה לאישור מנהל.

- **רשימת חסימה** — מכשיר שאבד או נגנב נחסם מרכזית ונדחה בכל נקודת כניסה, גם אם הותקנה בו התוכנה מחדש.
- **נעילת שם** — שם שנקבע על ידי מנהל אינו ניתן לשינוי מהמכשיר עצמו.

- **בקרת ערוצים** — ניתן לנעול מכשיר לערוץ יחיד ולמנוע ממנו מעבר לערוצים אחרים.

3 שכבת הקשר הקולי — הצפנה

תעבורת ה-PTT מוצפנת **ברמת המטען**, ולא רק ברמת התעבורה.

רכיב	מימוש
אלגוריתם	**AES-GCM** — הצפנה מאומתת, סודיות ושלמות יחד
גזירת מפתח	**SHA-256** ממפתח בסיס וממזהה החדר
היקף המפתח	**מפתח נפרד לכל ערוץ**
אכיפת סכימה	סכימת שידור מוגדרת פר-ערוץ ונאכפת בממסר

המשמעות של מפתח פר-ערוץ: מכשיר שהצטרף לערוץ אחד אינו יכול לפענח תעבורה של ערוץ אחר, גם אם הוא קולט אותה. ההפרדה בין ערוצי חירום, מבצע ושגרה היא הפרדה קריפטוגרפית ולא רק לוגית.

השימוש ב-GCM אומר שכל מנה נושאת תג אימות. שינוי של ביט אחד גורם לדחיית המנה ולא לפענוח שגוי — כלומר המערכת עמידה בפני **הזרקה או שינוי** של תעבורה, לא רק בפני האזנה.

> **הצהרה מדויקת על היקף ההגנה**
>
> ההצפנה מגנה על התעבורה מהמכשיר ולאורך הרשת. **מפתחות הערוצים נגזרים ממפתח בסיס המצוי בידי התשתית שלנו** — כלומר זו **אינה** הצפנת קצה-לקצה שבה גם מפעיל המערכת אינו יכול לפענח. אנו מציינים זאת במפורש. ארגון הזקוק למודל שבו גם הספק אינו יכול לפענח — זהו שינוי ארכיטקטוני מוגדר, וניתן לדון בו.

4 תעבורת נתונים אל השרתים

כל תעבורת הניהול, המיקום, האירועים והמדיה עוברת ב-**HTTPS**. חיבורים חיים נסגרים על **TLS 1.3 עם AES-256-GCM**. גרסאות TLS מיושנות נדחות על ידי השרת.

אימות: כל בקשה נושאת אסימון. קיימת הפרדה בין אסימון מכשיר לאסימון משתמש-מוקד, ולכל אחד היקף הרשאות שונה. אסימון אינו מקנה גישה לארגון אחר.

ממשקים פנימיים בין רכיבי התשתית אינם חשופים לאינטרנט. הם מוגבלים ברשימת היתר ברמת הרשת ובנוסף דורשים סוד משותף. בקשה שאינה עומדת בשני התנאים נדחית.

5 שכבת התקשורת הסלולרית

המכשירים בשטח פועלים על **כרטיסי SIM ייעודיים בניהול Monogoto**, ולא על מנוי סלולרי רגיל.

מה שזה משנה: תעבורת המכשירים אינה יוצאת לאינטרנט הפתוח מהאנטנה. היא מנותבת דרך **נקודת גישה פרטית (APN)** אל תשתית מבודדת, ומשם ב**מנהרת IPsec מוצפנת** אל השרתים שלנו.

מכשיר ← APN פרטי ← מנהרת IPsec ← תשתית Alpha Team ← בקרת יציאה

פרמטרי המנהרה: IPsec במצב מנהרה, אימות בסוד משותף, הצפנת AES, שלמות SHA, ו-Perfect Forward Secrecy — חשיפה של מפתח אחד אינה מאפשרת פענוח של תעבורה שהוקלטה בעבר.

בקרת יציאה — רשימת היתר עם חסימה כברירת מחדל. מה שיוצא מהמכשירים מוגבל ליעדים שאושרו במפורש. כל יעד אחר **נחסם ונרשם**.

> **מדוע זה מהותי ללקוח**
>
> חומרת רדיו מסחרית מכילה לעיתים רכיבי תוכנה של היצרן הפונים לשרתים חיצוניים מיוזמתם. בארכיטקטורה זו **פנייה כזו אינה עוזבת את הרשת** — היא נופלת בבקרת היציאה ונרשמת ביומן. ההגנה הזו היא **תכונה של המנהרה**: מכשיר הפועל על מנוי סלולרי רגיל, מחוץ למערך הזה, אינו מוגן על ידה.

פענוח שמות (DNS) מופנה אף הוא לשרת הפנימי שלנו, כך שגם ערוץ זה אינו משמש כדרך יציאה עוקפת.

6 הרשאות והפרדה בין ארגונים

הפרדה מלאה בין לקוחות. לכל ארגון בסיס נתונים נפרד, מפתחות ערוצים נפרדים והרשאות נפרדות. גישה חוצת-ארגונים מתאפשרת **רק** במסלול חירום מוגדר ומתועד.

תפקידים: מנהל-על, מנהל ארגון, מנהל תת-ארגון, מוקדן, צופה. פעולות ניהוליות דורשות תפקיד מתאים, והבדיקה נעשית בשרת בכל בקשה.

אימות קולי לפקודות בעלות השלכה גבוהה — פתיחת אירוע ושיגור כוחות מאומתים מול טביעת הקול של המפעיל הרשום למכשיר. **מכשיר גנוב מספק הצפנה תקינה אך קול שונה.**

תיעוד: פעולות ניהול ורישוי נרשמות ביומן ביקורת עם מבצע, תפקיד, זמן ופרטי הפעולה.

7 מה איננו טוענים

מסמך אבטחה שווה כמשקל הדברים שהוא מסייג. ארבעה סייגים:

1. **אין הצפנת קצה-לקצה במובן החזק.** מפתחות הערוצים נגזרים ממפתח בסיס המצוי בידי התשתית (סעיף 3).

2 **ההגנה הסלולרית חלה רק על מכשירים במערך ה-SIM הייעודי.** מכשיר על מנוי רגיל יוצא לאינטרנט ללא בקרת היציאה.

3 **קובץ התצורה מונה גם גרסאות TLS מיושנות, אף שהשרת דוחה אותן בפועל.** נבדק מול השרת: TLS 1.0 ו-1.1 נדחים; רק 1.2 ו-1.3 מתקבלות. ניקוי השורה מתוכנן — לא בשל חשיפה קיימת, אלא כדי שהתצורה תתאר את המצב במדויק ותישאר נכונה גם אם רכיב הצפנה בסיסי יוחלף.

4 **לא בוצעה בדיקת חדירה חיצונית עצמאית.** הממצאים במסמך זה נובעים מסקירה פנימית של הקוד והתצורה.

8 סיכום

שכבה	הגנה עיקרית
מכשיר	זהות עמידה · רשימת חסימה מרכזית · נעילת ערוץ
קשר קולי	AES-GCM · מפתח נפרד לכל ערוץ · הגנה מפני שינוי והזרקה
נתונים	TLS 1.3 · אסימון בכל בקשה · ממשקים פנימיים ברשימת היתר
תקשורת	APN פרטי · IPsec עם PFS · חסימה כברירת מחדל + יומן
הרשאות	הפרדת ארגונים · תפקידים · אימות קולי לפקודות קריטיות

עקרון המפתח: בכל שכבה, מצב ברירת המחדל הוא **סגור**. גישה, יעד או פעולה נדרשים להיות מותרים במפורש — ומה שלא הותר, נחסם ונרשם.

לפרטי תשתית, כתובות רשת ותצורה מלאה — נדרשת פנייה נפרדת תחת הסכם סודיות.
sales@alpha-poc.co.il · +972-3-9190902 · **Alpha Team**