44-45 lantronics.qxd 30/10/2008 09:39 Page 44

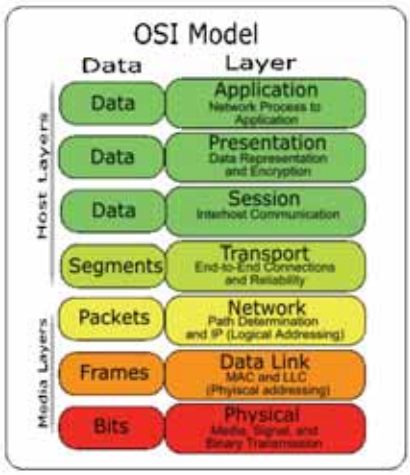
LANTRONIX®

האתגרים של אבטחת גישה מרחוק עבור מערכות משובצות

האתגרים של אבטחת רשתות עם גישה מרחוק

שיקולי אבטחה היו מאז ומתמיד סוגיה מרכזית בפריסה של פתרונות גישה מרחוק, והקשיים מחמירים עוד יותר כאשר הפתרונות חייבים לכלול תמיכה עבור מערכות משובצות. יישומים מוצלחים חייבים לספק בקרת גישה ואימות אפקטיבית ויש לוודא שהנתונים מאובטחים במהלך המעבר דרך הרשת. שיקולים נוספים צצים ועולים כאשר התקני היעד מתארחים על רשתות מרוחקות המנוהלות על-ידי אחרים. במקרים כאלה חשוב לוודא המערכות שלכם אינן פותחות את הרשת המארחת לאיומים מבחוץ.

אבטחת רשת אפקטיבית איננה מתבססת על טכנולוגיה אחת או על רכיב אחד ספציפי. כדי שתהיה יעילה עליה להיות בנויה בגישה של שכבות, כלומר, כמה קווי הגנה התורמים לפתרון הכולל. במאמר זה נסקור כמה טכנולוגיות שכיחות המשמשות את מי שמפתחים פתרונות לגישה מאובטחת מרחוק, לצד כמה מהאתגרים הבולטים שעליהם צריך להתגבר כאשר מיישמים פתרונות כאלה בשטח. בנוסף נבחן מוצר מסחרי אחד המתמודד עם האתגרים הללו בדרך חדשנית וחסכונית. עם מעט תשומת לב ניתן לספק גישת רשת יעילה ומאובטחת לפריסות גישה מרחוק, מה שמאפשר קיומם של מודלי שירות חדשים ושיפור היכולות של הלקוח.



מודל ה-OSI Seven Layer Networking Model

בקרות גישה מבוססות רשת

בקרות גישה מבוססות רשת משמשות כדי להבטיח שרק אורחים מורשים יצליחו להתחבר להתקנים המרושתים שלכם. בקרת גישה כזו לובשת בדרך-כלל צורה של firewall בשכבה 2 או בשכבה 3, המסנן החוצה כל חיבור לא נאות עוד בטרם יצליח להגיע ציוד שלכם.

פלטפורמת הניהול MANAGELINX היא פתרון ניהול מרחוק M2M המסוגל לספק גישת אינטרנט קלה ומאובטחת מרחוק לכל פיסת ציוד עם יכולותIP - אפילו כאשר ציוד זה ממוקם מאחורי FIREWALLS מרוחקים או VPN.

Firewalls יכולים לעבוד בשכבה 2 (המכונה גם שכבת קישור נתונים במודל ה-OSI Seven Layer Networking Model) או בשכבה 3 (המכונה במודל שכבת הרשת).

פתרונות בשכבה 2 מתוארים לעתים כ-"firewalls נסתרים" - הם אינם נראים כמו דילוג נתב לשכבת הרשת, תחת זאת הם מספקים יכולת סינון על-גבי חיבור גישור שקוף בין שתי נקודות קצה ברשת. Firewall בשכבה 2 יכול לכלול רשימות בקרת גישה (Access Control Lists) המאפשרות למפעיל לשלוט בחיבורים אל התקנים ספציפיים או מההתקנים, או למנוע תנועה של פרוטוקולי רשת ספציפיים. לדוגמה, תוכלו להגדיר מערכת כזו כך שתחסום תנועה המבוססת על block IP אל מארח ספציפי, ובה-בעת תתיר תנועה המבוססת על Novell Netware IPX.

Firewalls בשכבה 3, מכונים גם firewalls מבוססי מבואה, ופועלים בשכבת ה-TCP. כשהמנהלן מתקין firewall בשכבה 3 הוא מגדיר רשימות בקרת גישה המאפשרות או חוסמות חיבורים על-בסיס מבואות וכתובות IP עם מקור ויעד מוגדרים. ישנם firewalls המכונים "firewalls בשכבה 3/שכבה 4" ופועלים על-ידי בחינת התכנים של מנות בשכבה 3 לצורך השגת מידע נוסף שיסייע בקבלת ההחלטות.

סוגיות חשובות עבור בקרות גישה בשכבת הרשת

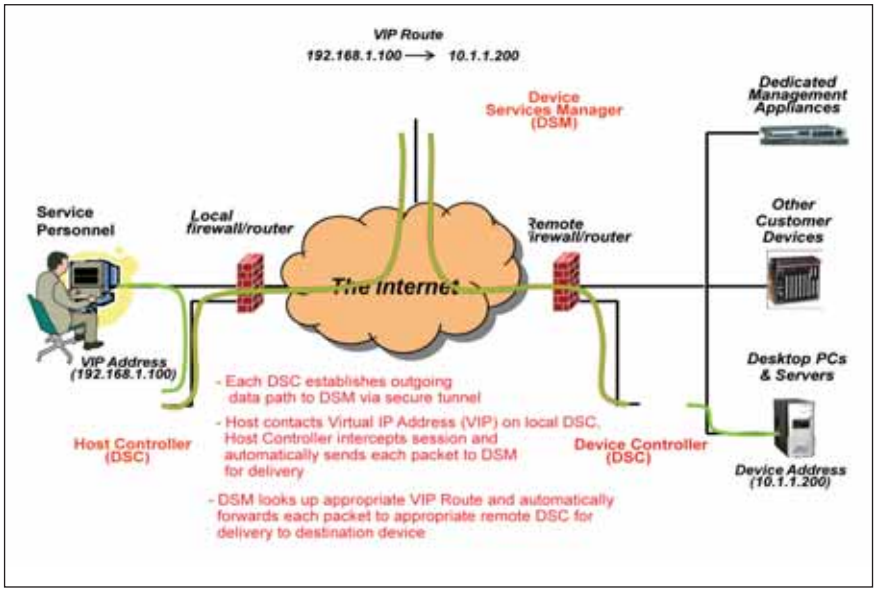
ההצלחה של טכנולוגיית ה-firewall בהתמודדות עם איומים חיצוניים לרשת גובה מחיר מסוים - פריסה אוניברסלית של firewalls החמירה מאוד את הקושי הטמון באספקת גישה מרחוק להתקני רשת.

ה-firewalls אמנם יעילים ולרוב מציעים רמות טובות של ביצועים, אך ההגדרה והניהול שלהם מורכבים והם מצריכים זכויות אדמיניסטרטיביות על רשת מוגנת. כאשר מתקינים firewall בשכבה 3 נהוג לאפשר חיבורים להתקן רק על אותן מבואות שיודעים מראש שיהיו בשימוש. זה מוביל לעתים קרובות לבעיות כאשר רוצים לאפשר שירות חדש והמבואה הדרושה חסומה.

גישה מרחוק עם VPNs

התגובה הראשונית של תעשיית הרשתות לאתגרים ההולכים וגוברים של גישה מרחוק הייתה ה-VPN (רשת פרטית וירטואלית). כפי ששמה מרמז, ה-VPN ממירה את הקווים החכורים הייעודיים, הקישורים הסלולריים או חיבורים פיסיים יקרים

44-45 lantronics.qxd 30/10/2008 09:39 Page 45



ManageLinx VIP Access - תיאורית ההפעלה

אחרים, במנגנון מאובטח שעל-גביו ניתן לתעל תנועה מהתקן מרוחק אל רשת היעד תוך שימוש בחיבור רשת קיים.

סוגיות חשובות הקשורות ל-VPNs

כמו עם firewalls, גם התקנה והפעלה של VPN משלכם מצריכה זכויות של מנהלן רשת. גם IPSec וגם SSL VPNs הן פתרונות המבוססים על הכוונה של IT ומשמשים מנהלני רשת כדי לשלוט בגישה אל הרשתות שלהם. כלומר, התקנה של התקן כזה בכל מיקום מרוחק שהוא היא בדרך-כלל לא אופציה בת-קיימא למי שרוצים לאפשר גישה מרחוק להתקנים על רשתות של אנשים אחרים. סוגיה נוספת הקשורה לפתרונות SSL VPN היא האתגר הטמון בצורך להחזיק מספר גבוה של הרשאות אבטחה ברמת המשתמש עבור כל טכנאי תמיכה שצריך לגשת לציוד במספר רב של מיקומים.

סוגיה אחרונה וחשובה הקשורה ל-VPNs כאשר מדובר בהענקת גישה לאורח היא שברגע שחיבור ה-VPN נוצר, האורח המרוחק הופך למעשה לצומת נוסף על הרשת המרוחקת. זה יכול להפוך לבעיה כאשר המטרה היא להעניק זכויות גישה מוגבלות לאורחים ספציפיים. אחד הפתרונות הוא לאגד התקנים אורחים על ה-LAN שלהם עצמם, אבל זה בלתי אפשרי כאשר הציוד שלכם מתארח על רשתות המצויות מחוץ לשליטה האדמיניסטרטיבית שלכם. כיוון שכך, מרגע החיבור, PC אורח נגוע אחד מסוגל לתקוף כל התקן אחר שנמצא על LAN מרוחקת.

The ManageLinx VIP Access Solution

פלטפורמת הניהול **ManageLinx** היא פתרון ניהול מרחוק M2M המסוגל לספק גישת אינטרנט קלה ומאובטחת מרחוק לכל פיסת ציוד עם יכולות IP - אפילו כאשר ציוד זה ממוקם מאחורי firewalls מרוחקים או VPN. קל מאוד להתאים את הפלטפורמה לקשת רחבה של משימות ניהול, והיא מתאימה במיוחד לגישה ולניהול של מערכות משובצות הממוקמות על רשתות אורחות מרוחקות ובמצבים אחרים שבהם אין לצוות התמיכה זכויות מנהלן על רשת מרוחקת.

אבטחת גישה מרחוק עבור מערכות משובצות. מערכת ה-Managelinx VIP Access היא כלי מאובטח, קל לשימוש וכדאי כלכלית המציע גישה מרוחקת להתקנים המצויים מאחורי firewalls

רכיב ה-**ManageLinx VIP Access**, הממתין בימים אלה לאישור פטנט, מספק גישת רשת שקופה בשכבה 3 לכל פיסה של ציוד מרוחק ללא צורך בתוכנת לקוח מיוחדת או בהגדרה מחדש של הרשת. כיוון שה-ManageLinx VIP Access מסוגל לעבוד עם כל יישום בעל יכולות TCP/IP המופעל על כל אורח או מערכת הפעלה, הוא שימושי במיוחד לפריסות של מערכות משובצות שבהן אין אפשרות ללקוחות VPN ייעודיים או לתצורות רשת מיוחדות.

ה-ManageLinx קל במיוחד לפריסה. מודול התצורה שלו, המבוסס על כונן USB Flash, מאפשר תצורה אוטומטית לגמרי של הגדרות רשת, הרשאות אבטחה ופרמטרים חיוניים נוספים, מה שמבטל את הצורך בצוות מיומן או בציוד מיוחד בזמן ההתקנה. ה-ManageLinx עובד על חיבורי אינטרנט קונבנציונליים אפילו עם מבואה אחת בלבד פתוחה ל-WAN, ואינו מצריך הגדרה מחדש של ה-firewall של רשת היעד. כיוון שה-ManageLinx VIP Access מסוגל להשתמש בחיבורי אינטרנט קיימים, הוא מבטל את הצורך בקווי טלפון אנלוגיים ייעודיים או בכיסוי סלולרי, מה שמוביל לחיסכון משמעותי בעלויות.

שיקולי אבטחה עם תמיכה במערכות משובצות

כיוון שה-ManageLinx VIP Access פועל בשכבת הרשת והתקשורת בין כתובת VIP לבין התקן נקודת קצה היא אוטומטית לגמרי, קל לשלב התקנים משובצים במערכת. כיוון שאין צורך בלקוחות ייעודיים או בתוכנה מיוחדת כדי לגשת למערכת, היישום של גישת רשת הוא קל ופשוט. מתכנתי מערכות משובצות משתמשים במנגנוני תכנות מסורתיים של TCP/IP - פשוט פותחים חיבור לכתובת ה-VIP והמערכת תיצור ותנהל את החיבור להתקן המרוחק בצורה אוטומטית.

מסקנות

מערכת ה-ManageLinx VIP Access היא כלי מאובטח, קל לשימוש וכדאי כלכלית המציע גישה מרוחקת להתקנים המצויים מאחורי firewalls. כלי זה מתאים במיוחד לשימוש עם מערכות משובצות או בתרחישי פריסה שבהם אין למפעיל זכויות מנהלן על מערכות מרוחקות. תשומת לב מיוחדת הוקדשה להבטיח שהמערכת תתמודד עם סוגיות מוכרות הקשורות לבקרת גישה בשכבת הרשת ולפתרונות VPN מוכרים. המערכת משתמשת בטכנולוגית הצפנה חדשנית כדי לספק תשתית ניהול אפקטיבית Network Layer Access Control-I משופרת. כיוון שהמערכת איננה מצריכה לקוחות ייעודיים והיא קלה ופשוטה לפריסה, היא יעילה במיוחד כאשר רוצים לספק יכולת גישה מרוחק למערכות משובצות או לכל מערכת שאיננה נהנית ממומחיות רשת בזמן הפריסה או התחזוקה.

מידע נוסף אודות פתרון הגישה מרחוק עם ManageLinx VIP Access, לרבות דף נתונים טכניים ומקרים לדוגמה של שירותי מוצרים מרוחקים, ניתן למצוא באתר החברה:

/http://www.lantronix.com/device-access