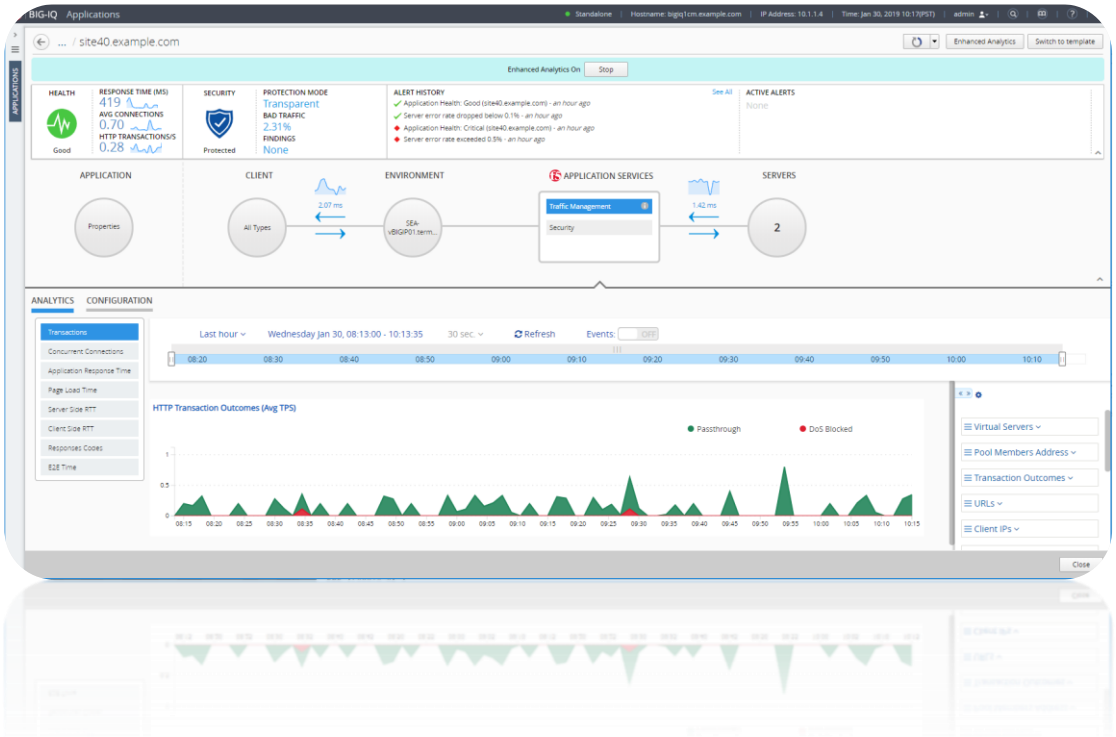
F5 Networks פתרונות



CONTENTS

https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf

איזון עומסים חכם לשרתים ושירותי אפליקציה מתקדמים - Local Traffic Manager (LTM)

https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf

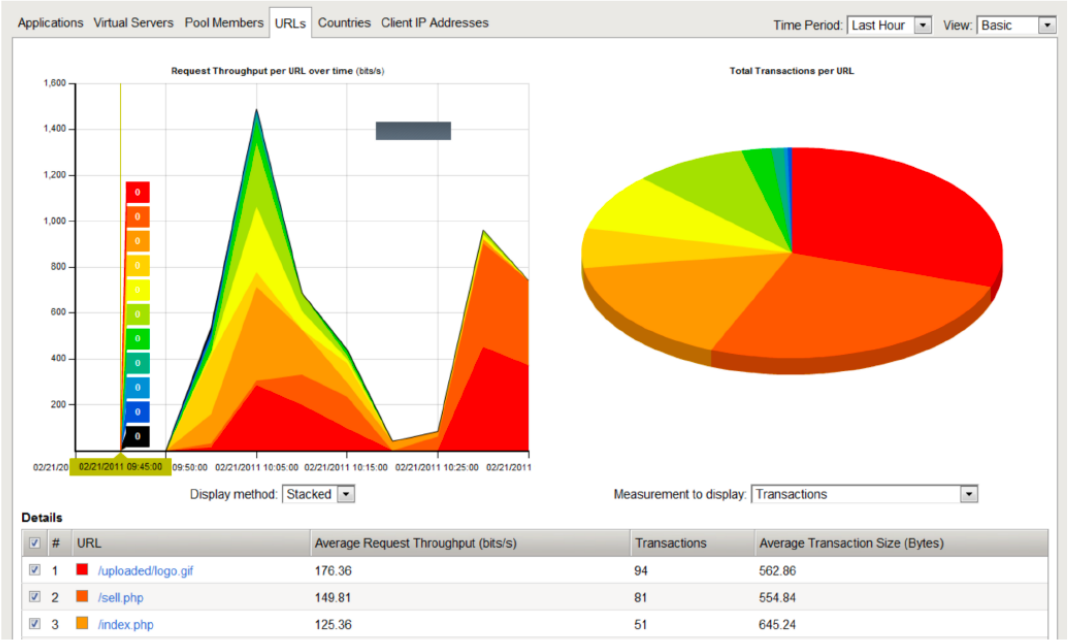
מודול ה- LTM מספק שירותי איזון עומסים חכם לשרתים, שירותי אפליקציה ואופטימיזציה, אנליטיקה ודווח.

יתרונות השימוש במודול ה- LTM:

1. ריבוי שיטות דגימה (בדיקות תקינות) אמתיות ומדויקת של השרתים ברמה האפליקטיבית ותמיכה בקסטומיזציה מלאה של נתוני הדגימות ומדדי ההצלחה פר שירות.
2. החלטה לגבי בריאות / תקינות המשאב (אפליקציה, שרת, שירות) על בסיס שילוב של מספר בדיקות למשאבים שונים.
3. איזון עומסים מתקדם ומדויק בין השרתים לפי קריטריונים שונים.
4. יכולת שליטה על הפניית התעבורה על ידי חוקים מתקדמים ב- Layer 7, הנותנת מענה לצרכים ייחודיים של האפליקציה או לדרישות המשתמשים (והמפתחים).
5. ניהול תעבורת ה- TLS (SSL) בצורה מאובטחת - מימוש ההצפנה נעשה בצורה עצמאית ולא נסמך על ספריות צד שלישי כדוגמת OpenSSL. בצורה זו המערכת מוקשחת ומוגנת יותר ולא חשופה לפגיעויות הרבות שמתפרסמות על ספריות קוד פתוח. בנוסף ניתן לשלוט בצורה מדויקת על הפעלת ה- Ciphers השונים ולעבוד עם המנגנונים המתקדמים ביותר על מנת לשמור על רמת אבטחת המידע.
6. הפעלת Persistence (Stickiness) לכיוון השרתים על פי מנגנונים מתקדמים כגון Cookie, Header, Universal, RDP ועוד.
7. שיפור חווית המשתמש על ידי פרופיל האצה - מרמת פרוטוקולי התקשורת (TCP/UDP) והאצה אפליקטיבית על ידי מנגנוני Caching, Compression וכו'.
8. HTTP/2 Gateway – מאפשר לארגון לספק שירותי HTTP/2 בצורה מהירה תוך מינימום שינויים בצד האפליקציה ושאר רכיבי התקשורת / אבטחת מידע.
9. תמיכה מלאה בפרוטוקול ה- WebSocket כחלק משירותי המערכת.
10. תכנות ה- Data Plane לשליטה בתעבורה בזמן אמת באמצעות ממשק פיתוח על גבי המערכת (iRules) התומך בשתי שפות תכנות: TCL ו- Node.js (כולל npm).
11. מענה מיידי לתיקון פרצות ו- Zero-day Vulnerabilities ללא תלות ביצרן או שדרוג גרסאות.
12. תכנות ה- Control Plane לשליטה מלאה על הגדרות ופונקציונליות המערכת באמצעות REST API ו- SDK.

יתרונות השימוש במודול ה- Analytics:

1. המערכת תנטר בזמן אמת ובאופן קבוע את חווית המשתמש והאפליקציות השונות.
2. המערכת תתריע בצורה פרואקטיבית על ירידה בחווית המשתמש או תקלות תקשורת / אפליקציה באמצעות מייל או Syslog.
3. זירוז משמעותי של זמן תחקור וטיפול בתקלות ע"י הספקת נתוני תקשורת, מצב המערכת ומצב האפליקציות השונות.
4. הפקת דוחות יזומים וקבועים הכוללים אוסף של נתוני תעבורה כגון URLs, Geolocation, Latency, Throughput ועוד.
5. יכולת הקלטת תעבורה על פי מאפיינים אפליקטיביים של בקשות מצד המשתמש או תשובות השרתים.
6. יצוא נתוני המודול למערכות ניטור וניתוח חיצוניות כגון Splunk, ELK וכו'.



https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf

איזון עומסים בין אתרים גיאוגרפיים והגנה על תשתיות DNS

https://www.f5.com/pdf/products/big-ip-dns-datasheet.pdf

מודול ה- DNS יבצע איזון עומסים בין האתרים השונים (למשל אתר ראשי ואתר DR). המערכת תכיר בכל רגע נתון את הסטטוס המדויק של כל אחד מהאתרים, אילו שירותים פעילים ובאיזה רמה בכל אתר. כך תוכל לנתב את המשתמשים תמיד למשאב הנכון ביותר.

יתרונות השימוש במודול ה- DNS:

1. אינטגרציה מלאה עם מערכות איזון העומסים הפנימיות, זיהוי אוטומטי של האפליקציות המוגדרות במערכות הפנימיות על מנת לפשט את תהליך ההגדרות.
2. תקשורת למערכות איזון העומסים הפנימיות מאפשרת הבנה מדויקת של סטטוס האפליקציות, הפניית תעבורה על פי מדיניות דינמית לפי פרמטרים שונים פר שירות.
3. ניהול אתרי ה- DR בתצורות Active / Active או Active / Standby פר אפליקציה או שירות ולפי מדיניות ייחודית וגמישה.
4. איזון עומסים על קווי האינטרנט מול מספר ספקיות ISPs בתעבורה יוצאת ונכנסת אל רשת הארגון.
5. יכולות ניטור ודגימת איכות הקווים, ממשקי הנתבים ומשאבים שונים באינטרנט דרך הקווים.
6. החלטה לגבי בריאות / תקינות המשאב (אפליקציה, שרת, שירות, קו) על בסיס שילוב של מספר בדיקות למשאבים שונים.
7. הגנה מלאה על תשתית ה- DNS, הרכיב משמש כ- DNS Firewall עם בדיקת הבקשות, ווידוא תקינות הפרוטוקול, אכיפה של State והגבלה של כמות הפניות על פי סוגים שונים.
8. תמיכה מלאה ב- DNS Caching, ביצוע Zone Transfer, ניהול רשומות DNS ויכולות מתקדמות נוספות.
9. זיהוי DNS Tunneling, תמיכה מלאה והאצה של DNSSEC.
10. יכולות תכנות המערכת מאפשרות גמישות מקסימלית בטיפול בתעבורת DNS.

https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf

מנוע Web Application Firewall (WAF) מוסמך רא"ם להגנה אפליקטיבית - Application Security Manager (ASM)

https://www.f5.com/pdf/products/big-ip-application-security-manager-ds.pdf

יתרונות השימוש במודול ה- WAF:

1. רכיב ה- WAF יבצע הגנה אפליקטיבית רב-שכבתית על אפליקציות ה- Web (HTTP/S) של הארגון. המערכת מאפשרת לימוד אוטומטי של ה- Policy ומתן מענה לאיומים מתקדמים על ידי שילוב של הגנת נגטיבית, פוזיטיבית ואנומליות.
2. ארכיטקטורת ה- Full Proxy מאפשרת הגנה מלאה גם עבור תעבורה המוצפנת במנגנונים המודרניים החזקים שנדרשים כיום בתקינה החדשה - עבודה במצב של Forward Secrecy כפי שמחייב תקן TLS 1.3, HTTP/2.
3. יכולות בדיקת תוכן מעמיקות לרבות פרמטרים, URLs, Headers, מטודות גישה ועוד.
4. יכולת מוכחת של חתימות התקפות רלוונטיות עם גיבוי של צוות מחקר מקומי הפועל בסניף בישראל.
5. הגנה על תשתיות API לרבות XML Firewall, תמיכה ב- REST API Security, פרוטוקול ה- WebSocket ועוד.
6. וידוא ובדיקת תוכן קבצי ה- XML, JSON לפי Schema, חתימות, וביצוע Spike Arrest בגישה לשירותי API.
7. הגנה מפני התקפות DDoS ברמת האפליקציה - Layer 7 ע"י שימוש בניתוח התעבורה ותגובות האפליקציה.
8. הגנה מפני בוטים (Bots) ורכיבים אוטומטיים הסורקים או תוקפים את האפליקציה כגון רכיבי IoT פרוצים או כלי תקיפה ייעודיים בשימוש זדוני.
9. הגנה מפני שליפת מידע (Web Scraping), ניסיונות התחברות אוטומטית (Brute-force) ודליפת מידע רגיש.
10. הארכיטקטורה מאפשרת מניפולציה של הבקשות ואף הזרקת קוד JavaScript Challenge לכיוון הדפדפן לצורך זיהוי מתקדם של מתקפות או הפלת ה- Bot-ים.
11. חלק אינטגרטיבי ברכיב איזון העומסים ומודולים נוספים על בסיס אותה מערכת ההפעלה, כך שלא נדרש לנהל מערכת נוספת וניתן להפעיל את ההגנה על אפליקציות כפרופיל נוסף.
12. זיהוי של Device ID מאפשר זיהוי של הדפדפן איתו המשתמש ניגש לאפליקציה. ניתן להשתמש ב- Device ID עבור זיהוי של אנומליות ויצירת מדיניות גישה.
13. הגנה מפני Zero-day Attacks ע"י שימוש ביכולות ה- Programmability.
14. יכולת יצירת מדיניות עסקית מותאמת אישית (Custom Business Logic) להגבלת הגישה על בסיס שילוב של מספר תנאים לפי צרכי הארגון (לדוגמא הגבלת ביצוע פעולה מסוימת מכתובת / דפדפן אחד לפרק זמן מסוים וכו').

https://www.f5.com/products/security/advanced-waf

מנוע מתקדם להגנה אפליקטיבית ייחודית - Advanced WAF (aWAF)

https://f5.com/products/security/advanced-waf

יתרונות השימוש במודול ה- aWAF:

1. הגנה מפני התקפות DDoS ברמת האפליקציה - Layer 7 ע"י שימוש ב- Behavioral Analysis ולימוד אנומליות.
2. הגנה על מידע רגיש כגון נתוני הגישה (שם משתמש + סיסמא) ע"י הצפנה נוספת של הערכים בשכבת האפליקציה.
3. הגנה מפני איומי Man in the Browser בצורה שקופה ע"י הזרקת JavaScript ושכתוב הדפים ללא התקנות בצד המשתמש.
4. הגנה מפני בוטים (Bots) ורכיבים אוטומטיים זדוניים גם בגישה לאפליקציות מובייל Native ע"י שימוש ב- Anti-Bot Mobile SDK ללא חשיפת קוד המקור או כתיבת קוד ידנית.
5. הגנה מפני איומי Credential Stuffing, המנצלים בסיסי נתונים אמתיים שדלפו לרשת לאחר פריצות בחברות כגון Yahoo, Equifax, eBay, Target, Uber ועוד.

https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf

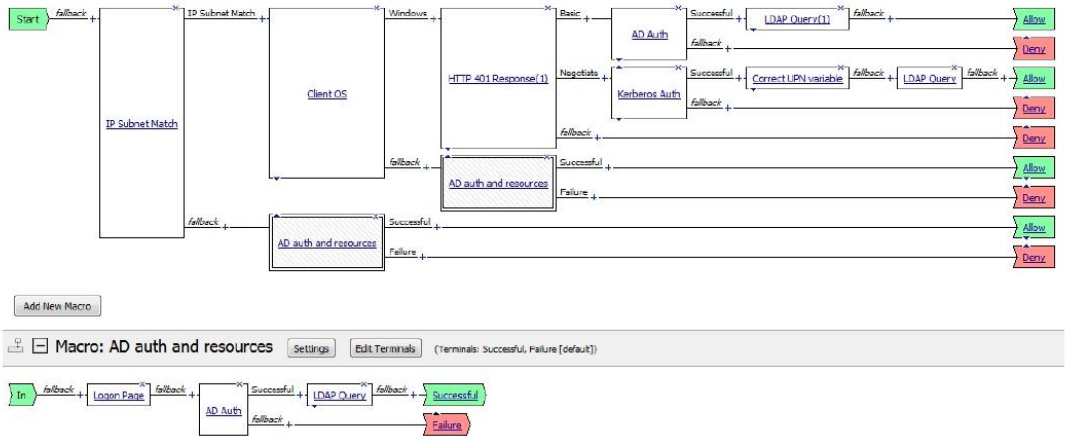
פתרון הזדהות וגישה אחודה - Access Policy Manager (APM)

https://www.f5.com/pdf/products/big-ip-access-policy-manager-ds.pdf

מודול ה- APM יוצר נקודת שליטה מרכזית על הגישה לאפליקציות הארגון. המודול יאפשר הפעלת שירותי הזדהות חזקים בהתאם לרמת הסיכון והשירות. המערכת תאפשר הפעלת רמות הרשאה שונות בתוך אפליקציה בודדת תוך אכיפה מבוססת שייכות המשתמש לקבוצות וביצוע Single Sign-on.

יתרונות השימוש במודול ה- APM:

1. תמיכה בריבוי פרוטוקולי ההזדהות ומתן הרשאות כגון AD, LDAP, RADIUS, SAML כולל חיבור באמצעות API.
2. ביצוע SSO עבור המשתמש במגוון שיטות כגון Basic, Form, Kerberos, NTLM, SAML או שיטות מותאמות אישית.
3. המערכת תנטר את כל בקשות המשתמשים לצורך Audit וזיהוי סיכונים.
4. הגדרת הזדהות באמצעות MFA כגון OTP, שימוש בכרטיס חכם או תעודה, מובייל וכו'.
5. הפעלת Federation מול הגופים השונים מאפשרת חווית שימוש ב- SSO תוך שמירה על רמת האבטחה.
6. ניהול נוח בממשק גרפי המראה את ה- Flow של המשתמש בתהליך הזיהוי.
7. SSL VPN מלא למערכות הפעלה שונות כולל Linux, macOS, Windows ותמיכה במובייל.
8. פורטל הזדהות דינמי למשתמשים אשר מהווה נקודת כניסה מרכזית לארגון.



https://www.f5.com/products/security/advanced-firewall-manager

פתרון הגנה רשתית ו- Advanced Firewall Manager (AFM) - DDoS

https://www.f5.com/pdf/products/big-ip-advanced-firewall-manager-datasheet.pdf

יתרונות השימוש במודול ה- AFM:

1. Data Center Firewall המבוסס על ארכיטקטורת ה- Full Proxy וניתוק התקשורת בין צד משתמש לצד האפליקציה.
2. בדיקה מעמיקה של פרוטוקולי תקשורת כגון HTTP/S, DNS, SIP, TCP, ICMP ועוד.
3. ניהול תעבורת ה- TLS (SSL) בצורה מאובטחת.
4. ניהול חוקי גישה ברמת שירותי אפליקציה - חוקי ה- FW מוצמדים להגדרות אפליקטיביות כולל פרוטוקולי Layer 7.
5. הגנה רב שכבתית מפני התקפות DoS ו- DDoS מבוססי Layer 3/4.
6. חתימות להתקפות DDoS ידועות, ספים אוטומטיים (או ידניים) ברמת Packets, כמות תעבורה, אחוזי גדילה ועוד.
7. הגנה מפני התקפות מסוג Flood, Sweep, Teardrop, Smurf ועוד.
8. תמיכה בחסימת תעבורה בצד ספק האינטרנט ע"י שימוש ב- Remotely Triggered Black Hole Filtering (RTBH).
9. פתרון היברידי המשלב שירות Scrubbing מבוסס ענן (F5 Silverline) לתמיכה בהתקפות Volumetric DDoS.
10. הגנה על ערוצי SSH כולל סינון תעבורה, הגבלת גישה ומניעת ביצוע פעולות ברמת משתמש.
11. תמיכה בתכנות ה- Data Plane לשליטה ואכיפת התעבורה בזמן אמת באמצעות ממשק פיתוח על גבי המערכת (iRules).
12. דו"חות, לוגים ואנליטיקה של אירועי אבטחת מידע בזמן אמת.

שיטת רישוי וחבילות

https://www.f5.com/pdf/licensing/good-better-best-licensing-overview.pdf

Features and Capabilities	Good	Better	Best
BIG-IP® Local Traffic Manager™			
Load balancing and monitoring	●	●	●
Application visibility and monitoring	●	●	●
L7 intelligent traffic management	●	●	●
Core protocol optimization (HTTP, TCP, HTTP/2, SSL)	●	●	●
SSL proxy and services	●	●	●
IPv6 support	●	●	●
Programmability (iRules®, iCall™, iControl®, iApps®)	●	●	●
ScaleN™ (on-demand scaling of performance and capacity)	●	●	●
BIG-IP® APM® Lite (user authentication, SSL VPN for 10 concurrent users)	●	●	●
SYN flood DDoS protection	●	●	●
Software Services			
Advanced routing (BGP, RIP, OSPF, ISIS, BFD)	Optional	●	●
BIG-IP® DNS			
Global server load balancing		●	●
DNS services		●	●
Real-time DNSSEC solution		●	●
Global application high availability		●	●
Geolocation		●	●
DNS DDoS attack prevention		●	●
BIG-IP® Advanced Firewall Manager™			
High-performance ICSA firewall		●	●
Network DDoS protection		●	●
Application-centric firewall policies		●	●
Protocol anomaly detection		●	●
BIG-IP® Application Security Manager™			
PCI-compliant web application firewall			●
Web scraping prevention			●
Integrated XML firewall			●
Violation correlation and incident grouping			●
Application DDoS protection			●
BIG-IP® Access Policy Manager®			
500 concurrent user sessions; scalable up to 200,000			●
BYOD enablement			●
Full proxy for VDI (Citrix, VMware)			●
Single sign-on enhancements (identity federation with SAML 2.0)			●