CYBER DEFENSE

❖ حسین ملک زاده

مشاور و تحلیل گر ارشد امنیت سایبری

کارشناس ارشد امنیت اطلاعات ازدانشگاه Sapienza Universityرم – ایتالیا

مدرس و عضو هیات علمی دانشگاه بین المللی نورث وست Northwest International University

مدرس و عضو هیات علمی دانشگاه نیوجرسی New Jersey International Open University

مدرس و عضو هیات علمی موسسه دانشگاهی DEI Institute - Online Universityآفریقا

دارای مدرک دکترا مدیریت امنیت سایبری DBA - Cyber Security Management از دانشگاه بین المللی نورث وست

ممیز و سرممیز امنیت اطلاعات ISMS ISO27001-2013

دارای مدارک سطح عالی امنیت اطلاعات CISSP , CISA

دارای مدرک مشاور ارشد امنیت سیستمی SSCP

طراح – مشاور و مجری پروژه¬های شبکه و امنیت اطلاعات ISMS , SOC , NOC

دارای بیش از ۲۴ سال سابقه آموزشی – اجرایی و مدیریتی درزمینه پروژه¬های شبکه و امنیت در داخل و خارج از کشور

مدرس دوره¬های تخصصی شبکه و امنیت با بیش از دوازده هزارساعت تدریس درموسسات داخلی و بین المللی

دارای تحصیلات و مدارک بین المللی :

MCSE , CCNA ,CCNA Security , CCNP , CEH , CISSP , CWNA , ISMS , SSCP, GSNA

عضوانجمن مهندسین کامپیوتر و فناوری آمریکا IEEE , ACM

مولف کتاب هنر هک کردن انسان در حوزه امنیت در مهندسی اجتماعی Social engineering

www.Hosseinmalekzadeh.com

Mobile: 09153133217

E-mail: Hoseeinmalekzadeh@Gmail.com

Telegram Channel : https://t.me/HosseinMalekzadeh

http://www.linkedin.com/in/hosseinmalekzadeh

@HOSSEINMALEKZADEH2015

@HOSSEINMALEKZADEH

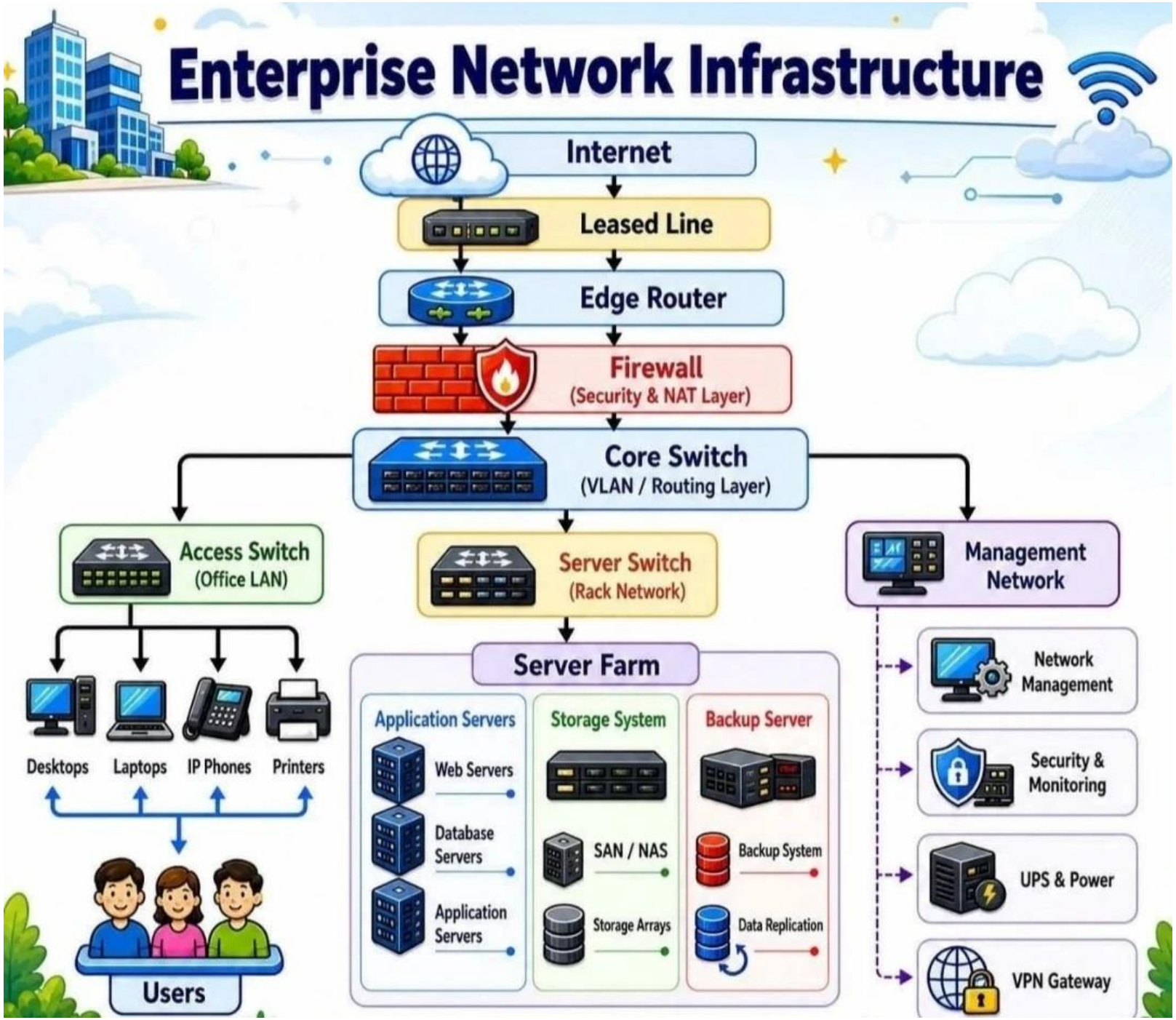
By. Hossein Malekzadeh

Cyber Security Consultant and Manager

www.Hosseinmalekzadeh.com

Mobile : 09153133217

- **فرض کنید یک سازمان دارای این زیرساخت است:**
- اینترنت
- روتر مرزی
- فایروال
- DMZ
- شبکه داخلی کاربران
- شبکه سرورها
- دیتابیس
- سیستم مانیتورینگ
- هدف ما این است که **در هر لایه شبکه مکانیزم دفاعی مناسب طراحی و پیاده‌سازی کنیم.**


Enterprise Network Infrastructure
Internet
Leased Line
Edge Router
Firewall
(Security & NAT Layer)
Core Switch
(VLAN / Routing Layer)
Access Switch
(Office LAN)
Server Switch
(Rack Network)
Management Network
Desktops
Laptops
IP Phones
Printers
Users
Server Farm
Application Servers
Web Servers
Database Servers
Application Servers
Storage System
SAN / NAS
Storage Arrays
Backup Server
Backup System
Data Replication
Network Management
Security & Monitoring
UPS & Power
VPN Gateway

- **اینترنت و لینک ارتباطی**
- **این لایه جایی است که ترافیک خارجی** وارد سازمان می‌شود. تمام ترافیک قبل از رسیدن به شبکه داخلی باید فیلتر و پاک‌سازی شود. استفاده از سرویس‌های Anti-DDoS و جلوگیری از IP Spoofing ضروری است.
- **تهدیدات:**

- DDoS attacks
- BGP hijacking
- DNS poisoning
- ISP-based man-in-the-middle attack
- Traffic interception
- Malicious traffic floods

- **حملات رایج:**
- حملات حجمی مثل UDP flood، SYN flood
- حملات مبتنی بر DNS (NXDOMAIN flood، amplification attack
- MITM روی لینک اگر رمزنگاری وجود نداشته باشد

- **Edge Router (در لبه سازمان)**
- **روتر نقطه کنترل مسیر ترافیک** و اولین سد امنیتی منطقی است. بستن سرویس‌های مدیریت و محدودسازی SNMP/SSH الزامی است.
- **ریسک‌ها:**
- سوءاستفاده از پروتکل‌های مسیریابی (OSPF, BGP)
- حمله به ACLها
- brute-force روی SNMP یا Telnet/SSH
- route injection / spoofing
- **حملات رایج:**
- ICMP redirect attack
- ARP spoof در برخی سناریوها
- Exploitهای مربوط به IOS

- **Firewall لایه امنیتی و NAT**
- فایروال قلب امنیت شبکه است. ترافیک باید بر اساس اصل **Zero-Trust** کنترل شود. تمام دسترسی‌ها از **DMZ**، **Server Farm**، **LAN** و اینترنت از این لایه عبور می‌کنند.
- **ریسک‌ها:**
- غلط پیکربندی شدن ruleها (misconfiguration)
- تونل شدن ترافیک مخرب از طریق پورت‌های مجاز (tunneling443 Port)
- حملات bypass
- حملات brute-force روی VPN gateway
- Exploitهای zero-day بر روی Firewall
- **سناریوهای حمله:**
- Session hijacking
- Web shellاز طریق پورت‌های باز
- حملات VPN credential harvesting

- **Core Switch لایه VLAN/Routing**
- **تقسیم‌بندی شبکه Segmentation** در این لایه انجام می‌شود. کاربران از سرورها جدا می‌شوند، چاپگرها جدا، VoIP جدا، DMZ جدا، شبکه مدیریت جدا. هر ارتباط باید policy-based باشد.

- **ریسک‌ها:**
  - حملات VLAN hopping
  - DHCP spoofing / DHCP starvation
  - MAC spoofing
  - ARP poisoning در شبکه داخلی
- **حملات رایج:**
  - Double tagging VLAN hopping
  - CAM table overflow
  - Man-in-the-middle داخل LAN
  - Rogue DHCP server

- **Access Switch (Office LAN)**

- **ریسک‌ها:**
  - اتصال دستگاه آلوده کاربران
  - حملات داخلی (Insider Threat)
  - BYOD بدون کنترل امنیتی
  - دسترسی فیزیکی به پورت‌های شبکه

- **حملات رایج:**
  - Port hijacking
  - Rogue AP اکسس‌پوینت غیرمجاز
  - Network scanning از سوی کاربران
  - حملات lateral movement میان کلاینت‌های شبکه

- **BYOD** مخفف **Bring Your Own Device** است؛ یعنی کارمندان با **دستگاه شخصی خودشان** (لپ‌تاپ، موبایل، تبلت) به شبکه سازمان وصل می‌شوند.
- وقتی می‌گوییم **«BYOD بدون کنترل امنیتی»** یعنی این دستگاه‌های شخصی **بدون هیچ سیاست یا مکانیزم امنیتی** اجازه اتصال به شبکه داخلی را دارند.

- **چرا خطرناک است؟**
- دستگاه شخصی معمولاً تحت کنترل IT سازمان نیست. بنابراین ممکن است:
- سیستم **Patch نشده** باشد
- **آنتی‌ویروس یا EDR** نداشته باشد
- قبلاً **بدافزار** گرفته باشد
- روی **Wi-Fi عمومی ناامن** استفاده شده باشد
- **داده‌های سازمانی بدون رمزنگاری** روی آن ذخیره شود

- وقتی چنین دستگاهی وارد شبکه می‌شود، عملاً یک **نقطه نفوذ بالقوه** برای مهاجم ایجاد می‌کند.

- **مثال واقعی حمله**
- سناریوی رایج:

1. کارمند با **لپ‌تاپ شخصی** به Wi-Fi شرکت وصل می‌شود.
2. لپ‌تاپ قبلاً به یک **بدافزار یا Trojan** آلوده شده است.
3. بدافزار داخل شبکه شروع به **اسکن IPها و سرویس‌ها** می‌کند.
4. اگر سروری آسیب‌پذیر باشد، مهاجم می‌تواند به آن نفوذ کند.
5. بعد از آن **Lateral Movement** در شبکه انجام می‌دهد.

- در بسیاری از حملات **Ransomware** نقطه ورود دقیقاً همین بوده است.

- **BYOD بدون کنترل امنیتی = اتصال دستگاه شخصی کارمندان به شبکه سازمان بدون بررسی امنیتی**

- که می‌تواند باعث شود:
- بدافزار وارد شبکه شود
- داده‌های سازمانی نشت کند
- مهاجم از آن به‌عنوان نقطه نفوذ استفاده کند

بررسی مهمترین سناریوهای اتفاق افتاده در تهدیدات BYOD

- **دستگاه شخصی آلوده می‌شود**
- یک کارمند، لپ‌تاپ شخصی خودش را هم برای کارهای شخصی و هم گاهی برای کار سازمان استفاده می‌کند.
- **مثلاً یکی از این اتفاق‌ها افتاده:**
- یک نرم‌افزار کرک‌شده نصب کرده
- روی لینک فیشینگ کلیک کرده
- فایل آلوده دانلود کرده
- از Wi-Fi عمومی ناامن استفاده کرده
- نتیجه:
- روی سیستم او یک **Trojan / Backdoor** نصب می‌شود، ولی کاربر متوجه نمی‌شود.

- **دستگاه وارد شبکه سازمان می‌شود**
- کارمند لپ‌تاپ شخصی را به یکی از این روش‌ها به شبکه شرکت وصل می‌کند:
- اتصال به **Wi-Fi داخلی**
- اتصال با کابل به پورت شبکه
- اتصال از طریق **VPN**
- وصل کردن موبایل/لپ‌تاپ شخصی به محیط کاری

- **اگر سازمان کنترل امنیتی BYOD نداشته باشد:**
- هیچ بررسی روی سلامت سیستم انجام نمی‌شود
- مشخص نیست دستگاه آلوده است یا نه
- ممکن است مستقیم وارد VLAN کاربران شود
- یعنی مهاجم حالا یک **جای پا داخل شبکه** دارد.

- **بدافزار شروع به شناسایی شبکه می‌کند**
- بدافزار داخل لپ‌تاپ شروع می‌کند به:
- شناسایی IPهای داخلی
- پیدا کردن سرورها
- جست‌وجوی Share Folderها
- اسکن سرویس‌هایی مثل:
  - SMB
  - RDP
  - SSH
  - دیتابیس‌ها
  - Active Directory
- این مرحله را معمولاً **Discovery** می‌گویند.

- **سرقت اطلاعات و اعتبارنامه‌ها**
  - اگر روی لپ‌تاپ:
  - پسوردها در مرورگر ذخیره شده باشد
  - کاربر قبلاً به سرویس‌های سازمانی لاگین کرده باشد
  - توکن VPN یا Session فعال وجود داشته باشد
  - بدافزار می‌تواند:
- **Credentialها را سرقت کند**
  - کوکی‌ها و Sessionها را بدزدد
  - اطلاعات ورود به فایل‌سرور، ایمیل، یا حتی پنل‌های مدیریتی را استخراج کند
  - اگر کاربر دسترسی بالایی داشته باشد، حمله خیلی خطرناک‌تر می‌شود.

- **حرکت جانبی در شبکه**
- حالا مهاجم فقط روی یک لپ‌تاپ نیست. او سعی می‌کند به سیستم‌های دیگر برسد:
- اتصال به Shareهای شبکه
- حمله به سرورهای ضعیف
- استفاده از پسوردهای تکراری
- سوءاستفاده از RDP/SMB
- رسیدن به Domain Controller یا File Server
- این همان **Lateral Movement** است.
- اگر Segmentation ضعیف باشد، مهاجم از VLAN کاربر به سرورها نزدیک می‌شود.

- **غیرفعال کردن دفاع‌ها**
- قبل از اجرای باج‌افزار، مهاجم معمولاً این کارها را می‌کند:
- غیرفعال کردن آنتی‌ویروس یا EDR
- حذف یا پاک کردن لاگ‌ها
- شناسایی سرور بکاپ
- سرقت داده‌های مهم
- ایجاد Backdoor برای ماندگاری
- **چرا؟**
- چون حملات جدید فقط رمزگذاری نیستند؛ معمولاً **Double Extortion** هستند:

1. اول داده را می‌دزدند
2. بعد سیستم‌ها را رمزگذاری می‌کنند
3. تهدید می‌کنند که اگر باج ندهید، داده را منتشر می‌کنیم

- **حمله به فایل‌سرورها و بکاپ**
- در این مرحله مهاجم:
- File Serverها را هدف می‌گیرد
- Shareهای مشترک را رمزگذاری می‌کند
- Backup Repository را پیدا می‌کند
- اگر Backup آنلاین و قابل‌دسترس باشد، آن را هم حذف یا رمزگذاری می‌کند

- **اینجا بزرگ‌ترین اشتباه** سازمان‌ها مشخص می‌شود:
- **Backup از نظر فنی وجود دارد، ولی امن و ایزوله نیست.**

- **اجرای باج‌افزار**
- در نهایت باج‌افزار در چندین سیستم اجرا می‌شود:
- سیستم کاربران
- فایل‌سرورها
- سرورهای اپلیکیشن
- دیتابیس‌ها
- ماشین‌های مجازی
- **پیامدها:**
- فایل‌ها قفل می‌شوند
- سرویس‌ها از دسترس خارج می‌شوند
- عملیات سازمان متوقف می‌شود
- هزینه بازیابی بسیار بالا می‌رود

- **چرا BYOD در این سناریو مهم بود؟**
- چون **نقطه ورود اولیه** از یک دستگاهی بود که:
- تحت مدیریت IT نبود
- بررسی امنیتی نشده بود
- EDR سازمانی نداشت
- Patch نشده بود
- مستقیم به شبکه وصل شد
- یعنی مهاجم بدون اینکه از فایروال اینترنتی عبور کند، از **داخل شبکه** شروع کرد.

ضعف‌هایی که باعث موفقیت در حمله شدند

۱. نبود NAC

هیچ‌کس بررسی نکرده دستگاه سالم است یا نه.

۲. نبود VLAN جدا برای BYOD

دستگاه شخصی وارد همان شبکه‌ای شده که کاربران یا حتی سرورها در آن هستند.

۳. نبود MFA

Credential دزدیده‌شده به‌راحتی قابل استفاده بوده.

٤. ذخیره پسورد در مرورگر یا سیستم

بدافزار توانسته رمزها را استخراج کند.

۵. نبود EDR

فعالیت مشکوک روی لپ‌تاپ شناسایی نشده.

Segmentation .ضعیف

مهاجم خیلی راحت از User Network به Server Network رسیده.

۷. Backup ناامن

نسخه‌های پشتیبان هم از بین رفته‌اند.

- **کاربران (Users)**
- کاربران با لپ‌تاپ، دسکتاپ و IP Phone به این لایه وصل می‌شوند. کنترل هویت کاربر و جلوگیری از اتصال دستگاه ناشناس مهم‌ترین وظایف این بخش است.

- **ریسک‌ها:**
- مهندسی اجتماعی
- بدافزارها
- فیشینگ ایمیل
- باج‌افزار
- سرقت اعتبار (credential theft)
- **حملات رایج:**
- Keylogger
- Phishing / Spear-phishing
- Password spraying
- فایل‌های Word/Excel/ZIP آلوده
- حملات مرورگر (drive-by download)

- **Server Switch/ Server Farm**
- این لایه باید کاملاً ایزوله و محافظت‌شده باشد. دسترسی به سرورها فقط از طریق Coreو با قوانین بسیار محدود انجام می‌شود. وجود WAFالزامی است.

- Web servers
- Database servers
- Application servers
- SAN/NAS
- Backup server

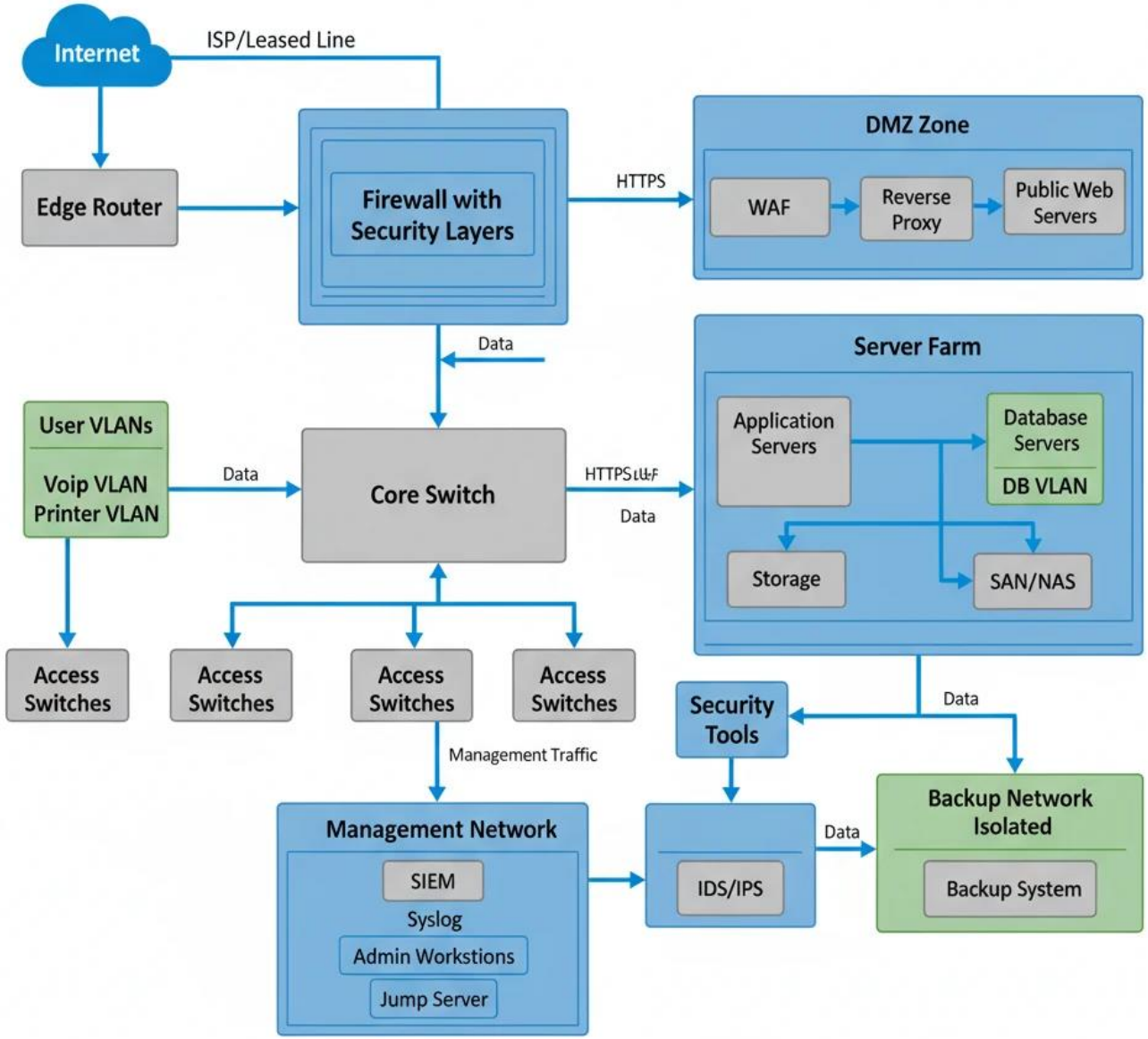
- **ریسک‌ها:**
  - SQL Injection – Web attacks
  - RCE (Remote Code Execution)
  - حملات روی پورت‌های دیتابیس (3306/1433/1521/27017 ...)
  - حمله به Storageو NAS
  - سرقت داده‌های بکاپ یا تخریب بکاپ‌ها
- **حملات رایج:**
  - حملات 10OWASP Top روی Web
  - حمله به hypervisor یا VM escape
  - حملات روی backup system برای جلوگیری از بازیابی
  - Data exfiltration (خروج داده‌ها)

- **شبکه مدیریتی (Management Network)**
- تمام ترافیک، لاگ‌ها و رخدادها جمع‌آوری و تحلیل می‌شود. این لایه وظیفه کشف حملات، بررسی رفتار مشکوک، و هشداردهی را دارد.

- Network Management
- Security Monitoring (SIEM/NIDS/NIPS)
- UPS & Power
- VPN gateway

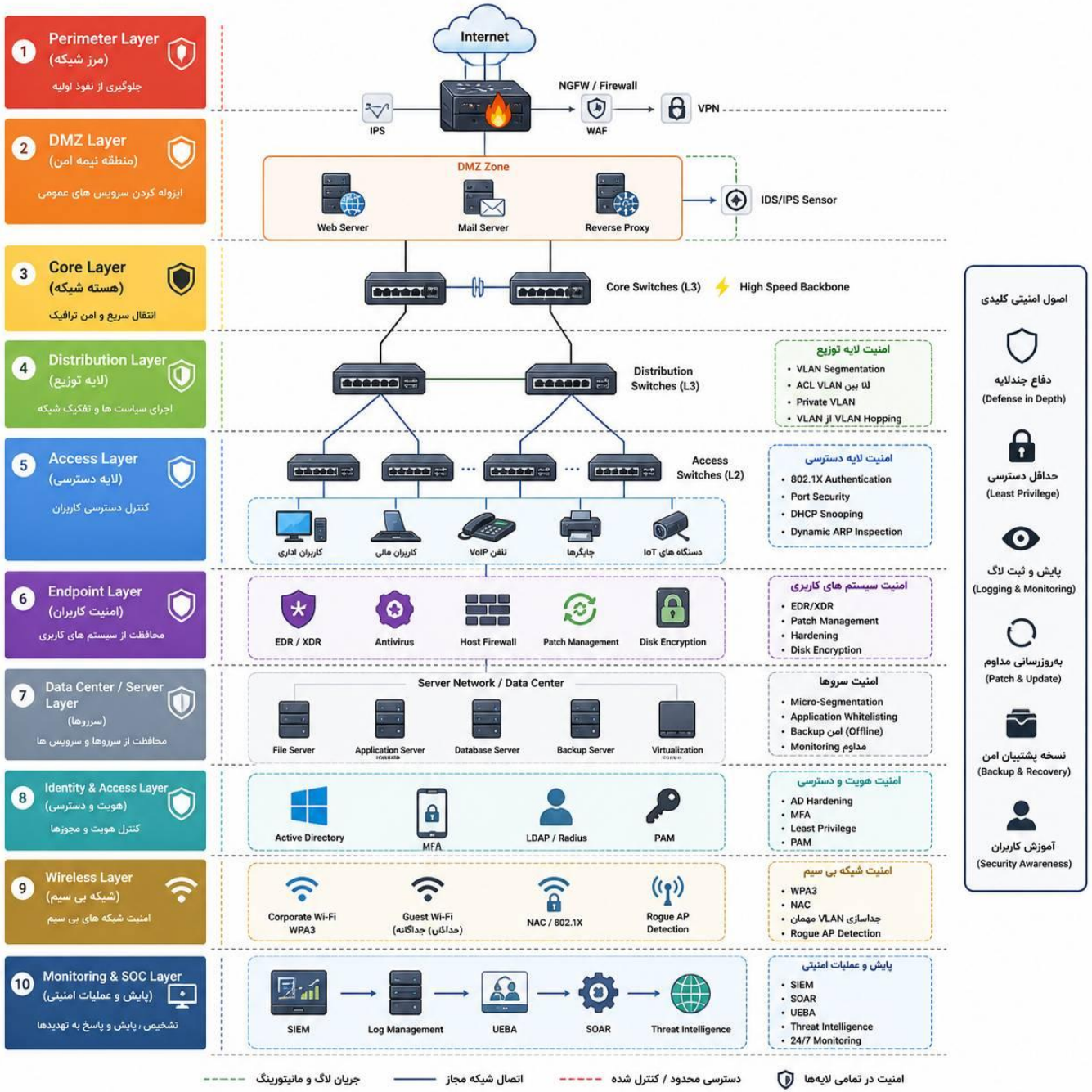
- **ریسک‌ها:**
- حمله مستقیم به سیستم‌های مدیریتی (بیشترین سطح دسترسی)
- دسترسی غیرمجاز به SIEM و حذف لاگ‌ها
- Exploit روی پنل مدیریتی سوییچ/فایروال
- حمله به VPN و سرقت توکن‌ها
- **حملات رایج:**
- حمله به APIهای مدیریتی
- Credential stuffing روی سرویس‌های مدیریت
- Flawed segmentation → دسترسی کاربر ساده به شبکه مدیریت
- تزریق کانفیگ مخرب به تجهیزات

- **تهدیدات بین لایه‌ای (Cross-Layer Threats)**
- حملاتی که کل ساختار را هدف قرار می‌دهند:
- Ransomware حمله به کل شبکه، انتشار از طریق SMB/RDP
- Supply chain attacks
- Zero-day exploits
- Data exfiltration از لایه اپلیکیشن به اینترنت
- حملات داخلی (Insider Threat)
- ضعف در Network Segmentation (نفوذ از کاربر به دیتاسنتر)



نقشه پیشنهادی شبکه امن سازمانی

- اگر بخوای **«امن‌سازی لایه‌به‌لایه»** رو درست اجرا کنی، باید هر لایه هم کنترل‌های خودش رو داشته باشه و هم به لایه‌های بالا/پایین وابسته نباشه. این یعنی اگر یک لایه **Fail** شد، کل شبکه باز نشه (همون **Defense in Depth** واقعی).

- ✗ **بیشترین نفوذها** از Access Layer شروع میشه
- ✗ **۸۰٪ سازمان‌ها** VLAN رو درست ایزوله نکردن
- ✗ **لاگ‌ها هست** ولی مانیتورینگ نیست
- ✗ **MFA** هنوز کامل پیاده‌سازی نشده

طراحی امن لایه به لایه شبکه سازمانی
(Defense in Depth)