Technologie pro monitorování a bezpečnost datové sítě

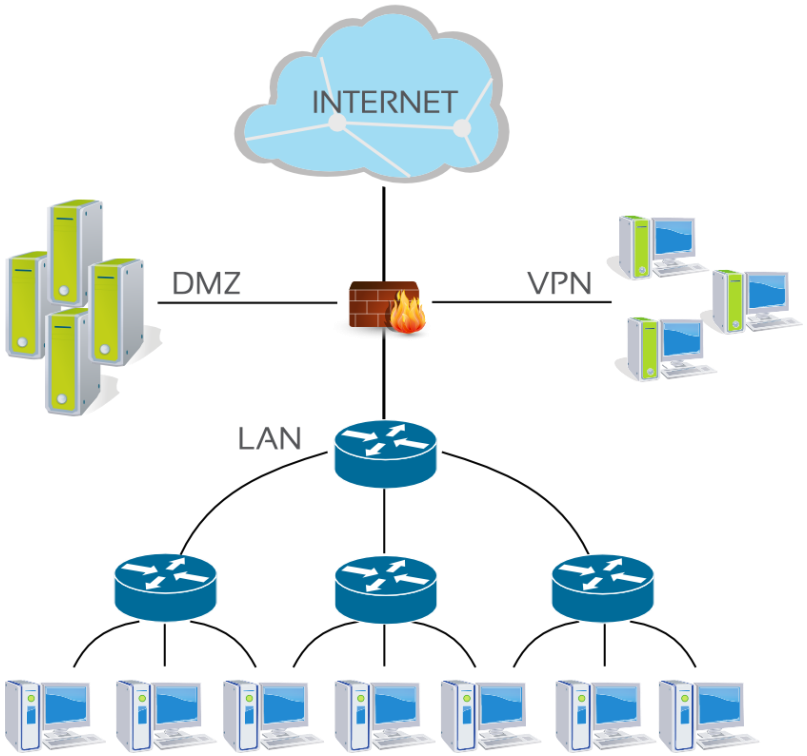
Pavel Minařík

seminář AFCEA

20.6.2012, Praha

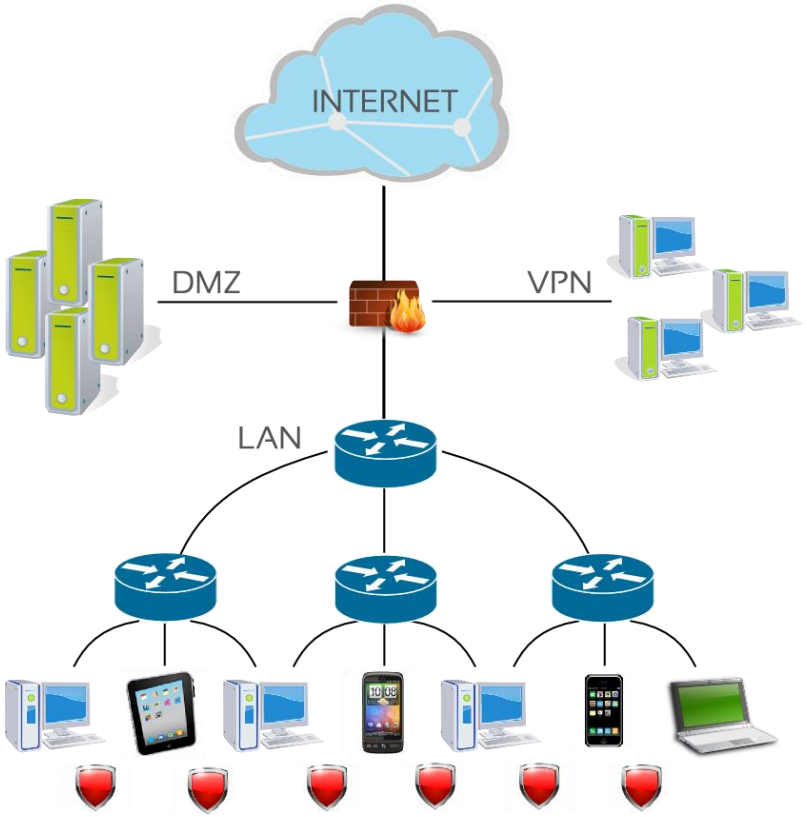
Perimetr

- Firewall, IDS/IPS, UTM, aplikační firewall, web filtr, email security, vzdálený přístup



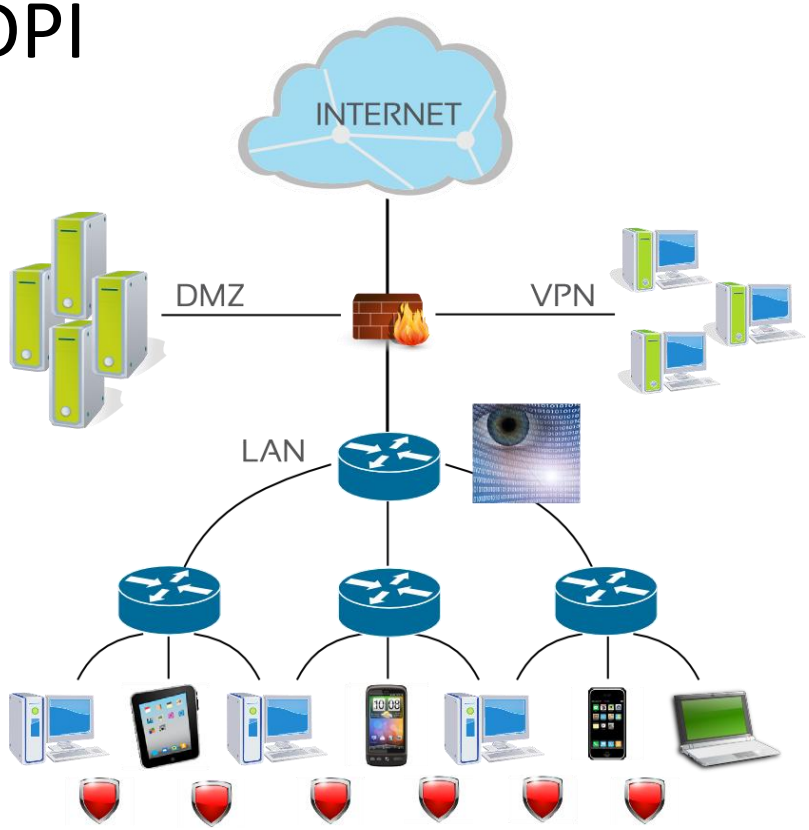
Koncové stanice

- Antivir, personální firewall, antimalware, antirootkit, endpoint DLP



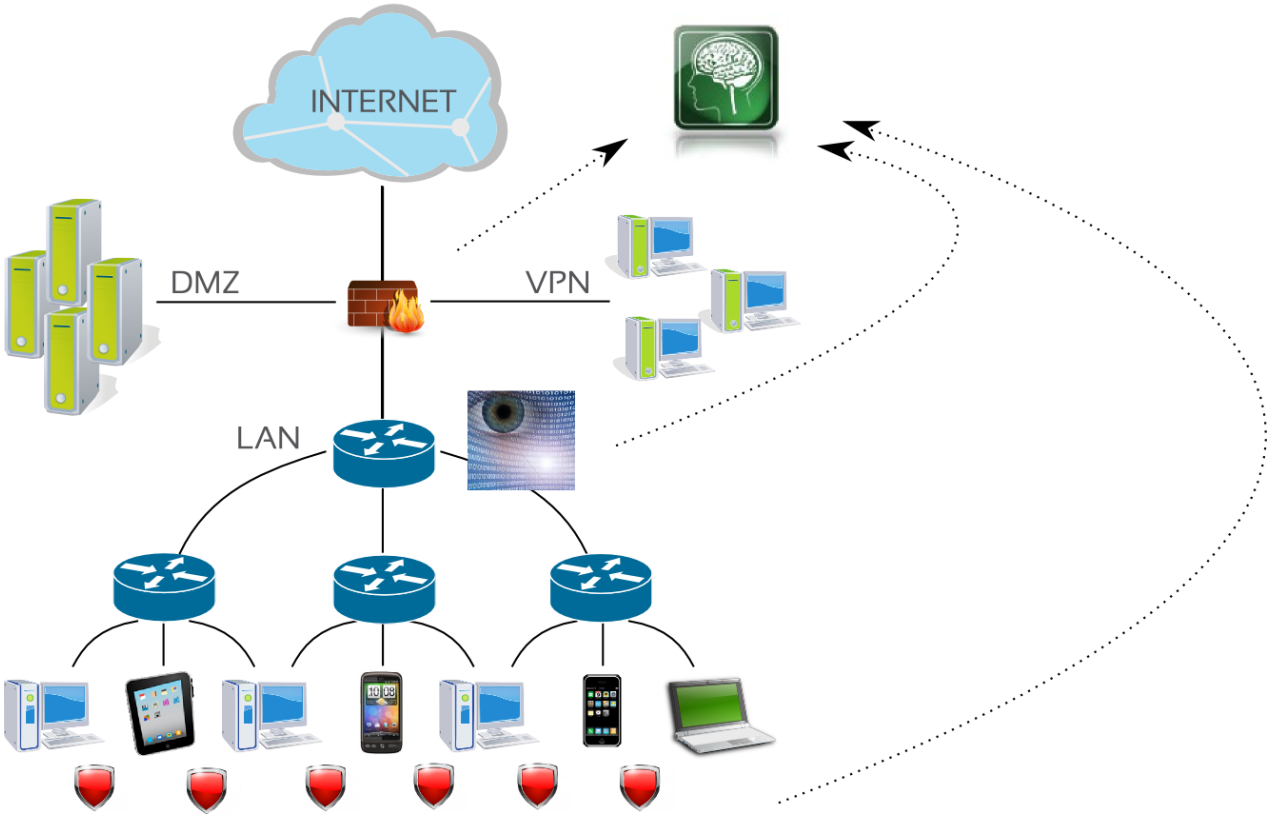
Vnitřní síť

- Network traffic visibility – flow monitoring, NBA –behaviorální analýza, automatická detekce anomálií, DPI



Centrální sběr a korelace dat

- SIEM, log management

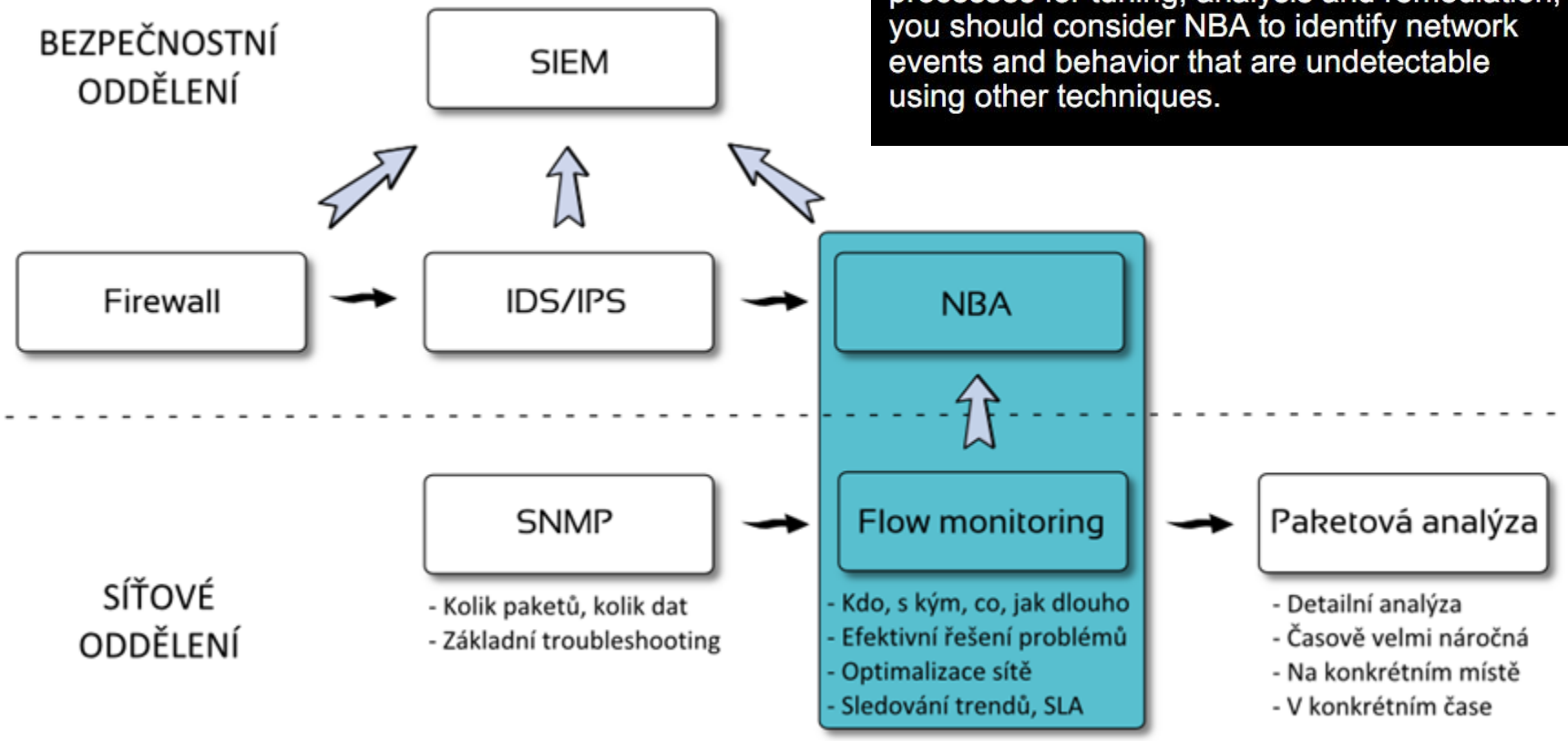


Komplexní pohled a doporučení

Gartner:

Recommendation

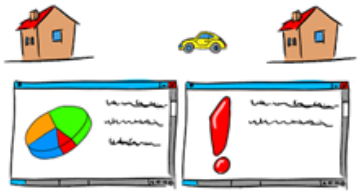
After you have successfully deployed firewalls and intrusion prevention systems with appropriate processes for tuning, analysis and remediation, you should consider NBA to identify network events and behavior that are undetectable using other techniques.



Flow vs. SNMP

Flow Monitoring

- Kdo, s kým, co, jak dlouho komunikoval, kolik přeneseno dat
- Kompletní přehled o dění v síti včetně struktury provozu
- Možnost rozkrýt až na úroveň jednotlivých komunikací
- Efektivní troubleshooting - umožní vyřešit většinu síťových problémů
- Navíc:
  - Informace pro optimalizaci sítě
  - Bezpečnostní monitoring
  - Performance monitoring
  - Sledování trendů
  - Reporting, SLA



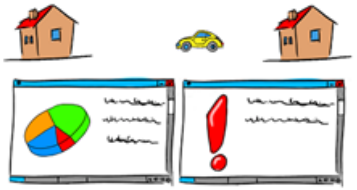
SNMP

- Kolik paketů, kolik bajtů proteklo přes daný port
- Pouze základní informace o množství provozu
- Nevím o jaký provoz se jedná, vím jen jeho množství
- Základní troubleshooting – teče/neteče/kolik

Flow vs. paketová analýza

Flow Monitoring

- Analýza na úrovni komunikací – agregované, ale bez ztráty důležité informace
- Distribuovaný dlouhodobý monitoring pro pokrytí celé sítě
- Rychlé a efektivní
- Přehled o dění v celé síti, ale i detailní pohled na jednotlivé komunikace
- Nevyžaduje expertní znalosti
- Účinné i pro šifrovaný provoz



Paketová analýza

- Detailní analýza – na úrovni jednotlivých paketů a jejich aplikačního obsahu
- Monitoring konkrétního místa v konkrétním čase (kde je problém)
- Časově velmi náročné
- Nutná znalost toho „co hledám“ – jinak nutné analyzovat obrovská množství dat
- Především pro experty
- Neúčinné pro šifrovaný provoz

NBA vs. IDS/IPS

NBA (Network Behavior Analysis)

- Detekce změny chování, detekce podezřelého chování
- Založeno na analýze IP statistik
- Detekce i dosud neodhalených hrozeb (APT, Zero-Day útoky, …)
- Nepoužívá signatury útoků
- Analýza perimetru, LAN i WAN, odhaluje i vnitřní hrozby
- Účinné i pro šifrovaný provoz
- Pasivní - podklad pro akce v síti

IPS (Intrusion Prevention System)

- Detekce útoků vyhledáváním aplikačních vzorů v paketech
- Založeno na L7 aplikační analýze
- Obrana proti známým hrozbám – již dříve odhalené a popsané
- Závislé na DB vzorů od výrobce
- Obrana pouze na perimetru sítě, neúčinné proti vnitřním hrozbám
- Neúčinné pro šifrovaný provoz
- Možnost aktivního zablokování

Děkuji za pozornost

OTÁZKY?

Pavel Minařík
CTO, AdvaICT, a.s.
pavel.minarik@advaict.com
Tel.: +420 733 713 703