biztributor
H-1112 Budapest, Kőoltár utca 4/A, Hungary
T +36 1 392 0218 • F +36 1 392 0217
info@biztributor.hu • www.biztributor.hu

FireEye™

Bevezető

A dokumentum célja összefoglalni a szükséges technikai előkészületeket a FireEye PoC előtt, hogy az sikeresen végig mehessen.

PoC kit felépítése

A FireEye PoC kit 3 appliance-t tartalmaz:

- NX series: Az NX appliance vizsgálja a hálózati (webes) forgalmat.
- EX series: Az EX appliance vizsgálja az e-mail forgalmat.
- CM series: Központi menedzsmentet biztosít és korrelál az NX és EX appliance-ek között a multi-vector támadások detektálása érdekében.

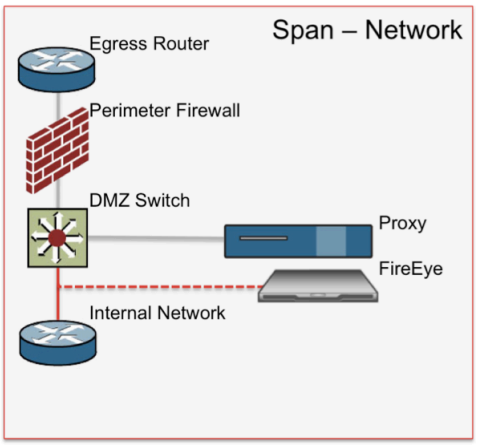
NX appliance

Tipikusan négyféle módon lehet az NX eszközt hálózatba illeszteni:

- SPAN-Network (javasolt)
- SPAN-Proxy
- Inline-Network
- Inline-Proxy

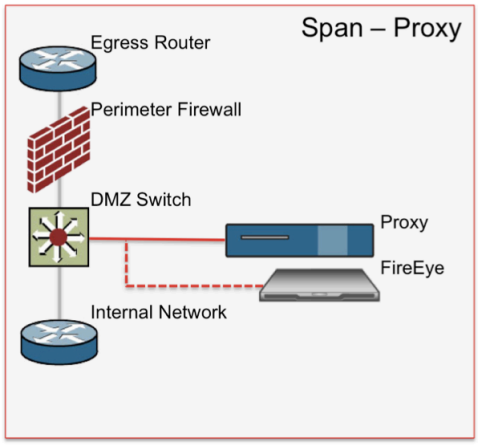
SPAN-Network (javasolt)

Rálátást biztosíthat a teljes forgalomra amellett, hogy egyáltalán nem zavarja a meglévő éles hálózat működését, az elemzés a kitükrözött forgalmon keresztül történik. Szükséges mindkét irány (Rx/Tx) tükrözése a portokon. Az NX applaince több fizikai interfésszel rendelkezik, így több SPAN portot is lehet csatlakoztatni (pl. több internet kijárat külön switcheken).



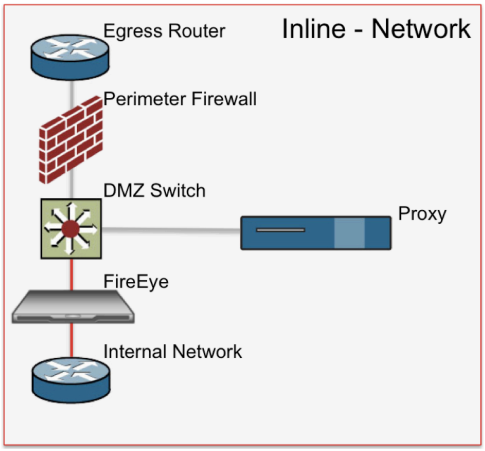
SPAN-Proxy

Hasonló a *SPAN-Network* módhoz, viszont ilyen elhelyezés esetén csak azt a forgalmat kapja meg az NX eszköz, ami a Proxy eszközön keresztül továbbítódik.



Inline-Network

Inline módban az eszköz a hálózat aktív elemeként működik. Az elemzés a forgalom másolatán történik, így késleltetést nem jelent.

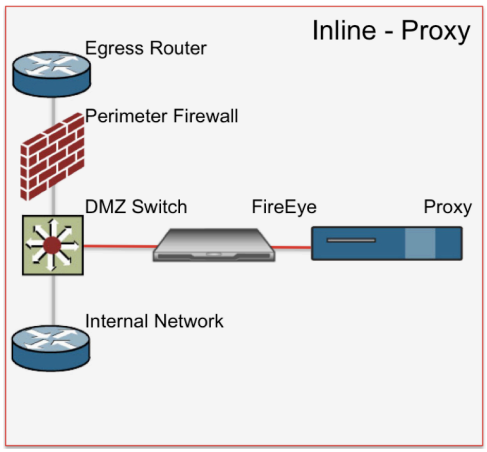


Inline-Proxy

Hasonlóan az Inline-Network módhoz, ilyenkor az eszköz a hálózat aktív elemeként működik. Hátrány lehet az előzőhöz képest, hogy csak az a forgalom megy keresztül az eszközön, ami a Proxy-n keresztül továbbítódik.

biztributor
H-1112 Budapest, Kőoltár utca 4/A, Hungary
T +36 1 392 0218 • F +36 1 392 0217
info@biztributor.hu • www.biztributor.hu

FireEye



Felmerülő kérdések az NX elhelyezéséhez és méretezéséhez

- Mekkora internetes sávszélesség áll rendelkezésre?
- Meghatározható a ténylegesen használt sávszélesség?
- Hány internet kijárat található a hálózatban?
- Hány felhasználó található a hálózatban?
- SPAN elhelyezés esetén rendelkezésre áll-e olyan eszköz, ahol a tükrözés elvégezhető?
- Hány tükrözött port csatlakoztatására van szükség (pl Load Balance-olt hálózat vagy több internet kijárat esetén), hogy a teljes hálózati forgalmat monitorozni lehessen?
- Amennyiben a Proxy előtt van csak lehetőség elhelyezni az eszközt (vagy innen tükrözni a forgalmat): a Proxy egy interfészen (single homed) vagy két interfészen (dual homed) keresztül csatlakozik a hálózathoz?
- Milyen portokon zajlik a HTTP kommunikáció (normál 80-as porton kívül pl. Proxy miatt egyéb portok)?
- Menedzsment célokra szükséges egy IP interfészt konfigurálni az eszközön (IP cím, netmask, gateway és DNS)

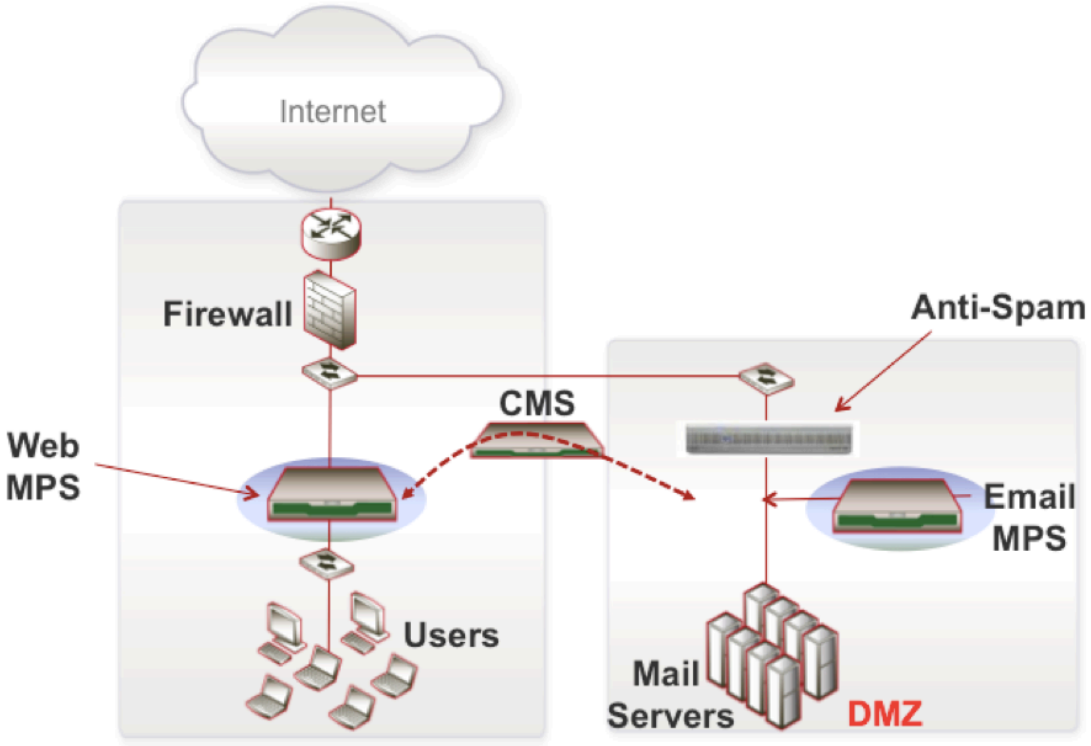
EX appliance

Háromféle módon lehet az EX appliance-t a hálózatba illeszteni:

- SPAN (Tap) mód (javasolt)
- BCC mód (javasolt)
- MTA mód

biztributor
H-1112 Budapest, Kőoltár utca 4/A, Hungary
T +36 1 392 0218 • F +36 1 392 0217
info@biztributor.hu • www.biztributor.hu

FireEye



SPAN (Tap)

SPAN mód esetén az EX appliance a tükrözött forgalmon keresztül figyeli az SMTP forgalmat. Mivel az elemzés csak a forgalom másolatán történik és aktívan nem szerepel a hálózatban az eszköz, így nincs semmilyen kihatással a hálózat működésére.

BCC

BCC mód esetén tipikusan az anti-spam gateway-en (vagy a levelező szerveren magán) szükséges módosítást végezni, miszerint a beérkező – már megszűrt – tiszta levelekről egy másolatot küldjön az EX appliance-nek. Megjegyzés: Az EX appliance-nek nem szükséges postafiókot létrehozni a tartományban, elegendő az IP címére küldeni a másolatot (amennyiben IP címet nem lehet megadni a bcc másolathoz csak e-mail címet, akkor egy tetszőleges nem használt tartományt – pl. fireeyepoc.local – szükséges ehhez használni és az SMTP szerveren felkonfigurálni, hogy ezt a tartományt az EX appliance IP címére szükséges továbbítani – e-mail címnek bármit lehet használni, pl. ex@fireeyepoc.local, mivel az eszköz minden SMTP forgalmat feldolgoz.

MTA

MTA mód használatakor az EX appliance bekerül a mail-flow-ba. Tipikusan ilyenkor az anti-spam eszköz továbbítja a megszűrt leveleket az EX appliance-nek, ahonnan továbbításra kerül a levelező szerverre (vagy a következő SMTP eszköznek). MTA esetén tud működni az eszköz Block, illetve Monitor módban is. Monitor mód esetén késleltetés nélkül továbbítja a levelet és a másolaton végzi el az ellenőrzéseket, Block mód esetén

előbb lefut az ellenőrzés és ennek az eredménye dönti el, hogy továbbításra vagy karanténozásra kerül a levél.

Felmerülő kérdések az EX elhelyezéséhez és méretezéséhez

- Mekkora a szűrt bejövő levelek száma naponta?
- Ismert ezeknek az eloszlása (pl. 80%-a munkaidőn belül érkezik)?
- SPAN mód esetén rendelkezésre áll olyan switch, amin a teljes SMTP forgalom (megszűrt) tükrözésre kerülhet?
- BCC mód esetén van lehetőség ilyen konfigurációra az anti-spam eszközön (a gateway-ek 90%-a támogatja a domain alapon eltérő IP-re történő továbbítását a másolatoknak)
- Menedzsment célokra szükséges egy IP interfészt konfigurálni az eszközön (IP cím, netmask, gateway és DNS)
- BCC vagy MTA mód esetén külön interfészen figyeli az SMTP forgalmat az eszköz, így szükséges még egy IP interfész ilyen telepítési mód esetén (lehet azonos subnet)

CM appliance

A CM eszköz nem végez közvetlen elemzést, így a hálózatba illesztéshez elegendő egy IP cím, amin keresztül tud kommunikálni az NX és EX eszközökkel és az internettel a licenszek ellenőrzése és a frissítések letöltése végett.

Szükséges tűzfalszabályok

- HTTPS (TCP 443) kommunikáció az internetre (közvetlen vagy Proxyn keresztül). Megjegyzés: amennyiben a CM központi menedzsment appliance is telepítésre kerül, úgy elegendő csak innen engedélyezni a kapcsolatot. Fontos, hogy SSL terminálás esetén fel kell venni kivételként ezt a kapcsolatot.
- SSH (TCP 22) és HTTPS (TCP 443) kapcsolat engedélyezése a CM és az NX-EX appliance-ek között (mindkét irányban). Ez szükséges a központi menedzsmenthez és a korrelációkhoz.
- Az appliance-ek menedzselése történhez GUI-n (HTTPS – TCP 443) és CLI-n (SSH – TCP 22) keresztül, így ezeket a menedzsment hálózatból engedélyezni kell. Opcionálisan az FTP (TCP 21) engedélyezése is szükséges lehet (pl. tcpdump letöltése pcap formában).
- Opcionálisan szükséges lehet a FireEye appliance-ekről a Syslog (UDP – 514) és SMTP (TCP – 25) forgalom engedélyezése is, amennyiben a riasztások (pl. E-mail alapon) vagy 3rd party (pl. SIEM) integráció használatban lesz a PoC ideje alatt
- Opcionálisan szükséges lehet az NTP (UDP – 123) protokoll engedélyezése a FireEye appliance-ekről.