Kettős tűzfalrendszer *Zorp Gateway* és *Cisco* tűzfalakkal

2022. július 28.

A *Zorp Gateway (Zorp)* alkalmazásszintű proxy tűzfal remekül alkalmazható különböző gyártók tűzfalaival együttműködésben, kettős tűzfalrendszert alkotva. Az alábbi esettanulmányban a *Cisco* eszközeivel való együttműködést szeretnénk bemutatni.

Tartalom

1. A probléma bemutatása

Vállalati hálózatok esetén fontos, hogy minél magasabb szinten tudjuk azt megvédeni az esetleges külső vagy akár belső támadásoktól. Ennek érdekében a közép- és nagyvállalatok is egyre több hálózatbiztonsági megoldást vezetnek be. Ilyen eszközök többek között a jogosultságkezelés, a tűzfalak, a behatolás detektáló (IDS) és megelőző rendszerek (IPS), illetve a demilitarizált zóna (DMZ) kialakítása. Ezek szakszerű kombinálásával növelhetjük a hálózatunk biztonsági szintjét.

Tűzfalak esetén, a hálózati struktúrát is figyelembe véve, többféle megoldást tudunk alkalmazni. A legegyszerűbb az egy tűzfalból álló, olcsóbb és könnyebb megoldás. Ebben az esetben azonban korlátozottak a lehetőségek a különböző hálózati szegmenseink szeparálására. Ennek veszélye, hogy a tűzfal esetleges sérülékenységének kihasználásával, vagy akár egy rosszul beállított szabály következtében, áttörhető az egyetlen védelmi vonalunk.

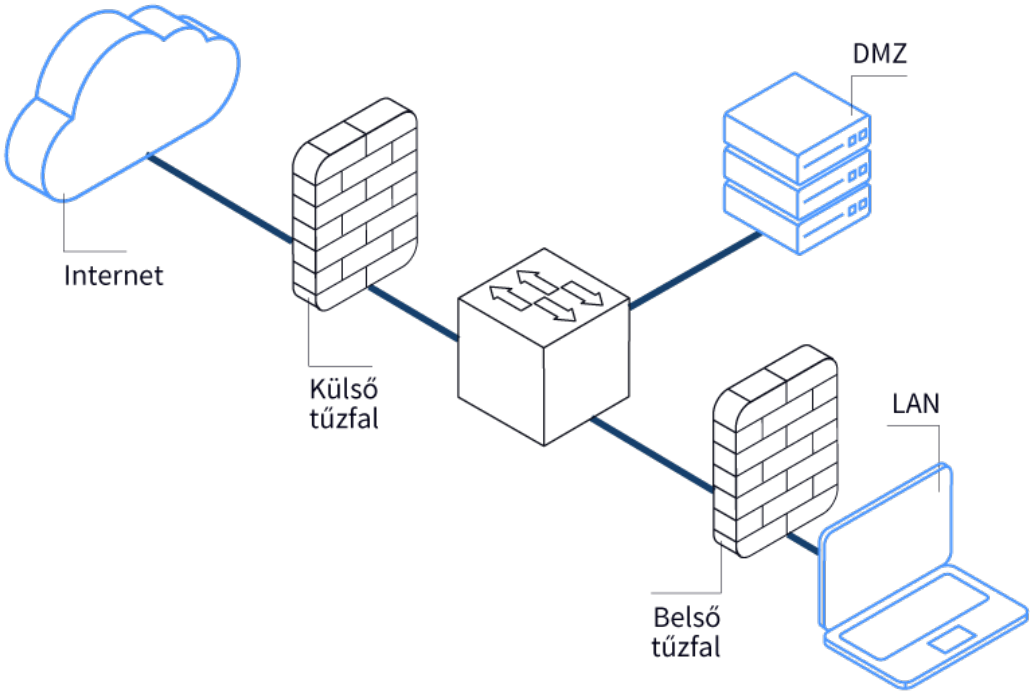
IDS: Intrusion Detection System, azaz behatolás detektáló rendszer. Olyan hardver vagy szoftver, ami a hálózatba kötve passzívan figyeli a rajta áthaladó forgalmat, erről elemzést készít, és szokatlan tevékenység esetén riasztani tud.
IPS: Intrusion Prevention System, azaz behatolás-megelőző rendszer. Olyan aktív eszköz, ami a hálózatba kötve vizsgálja és elemzi a rajta áthaladó forgalmakat, ha szükséges, meg tudja szakítani a kapcsolatot.
DMZ: Demilitarizált zóna, egy fizikai vagy logikai alhálózat, aminek a célja elválasztani a külső, nem megbízható hálózatról is elérhető eszközöket a belső hálózattól.

2. A megoldás bemutatása

A kettős tűzfalrendszer

Vállalatunk hálózati biztonságának növelése érdekében jó megoldás lehet egy kettős tűzfalrendszer kialakítása.

A megoldás alapja, hogy külön tűzfal szűri az internetről érkező külső hálózati forgalmat a két tűzfal között kialakított demilitarizált zóna (DMZ) felé. A DMZ-ben található szerverek kommunikálhatnak külső hálózatokkal, a belső hálózat felé viszont külön korlátozott kapcsolattal rendelkeznek. Forgalmuk - a teljes befelé irányuló forgalommal együtt - áthalad a belső tűzfalon, amely mögött húzódik a belső hálózat.



1. ábra - A kettős tűzfalrendszer általános felépítése

A rendszer implementációja költségesebb, mint az egy tűzfalas megoldás, hiszen több tűzfalat és hálózati eszközt igényel, illetve figyelnünk kell rá, hogy kettős tűzfal esetén két helyen kell a szabályrendszerünket felépíteni és karbantartani. Ezek mellett azonban számos előnye közé tartozik, hogy a külső tűzfal kompromittálása csak az első védelmi vonal elesését jelenti, időt ad annak detektálásához, és a szükséges lépések megtételéhez. Megakadályozza továbbá a támadó közvetlen hozzáférését a belső hálózathoz, mivel a DMZ-ből csak erősen korlátozott kommunikációt engedünk a belső hálózat irányába.

A fenti megoldást a következőképpen tehetjük még biztonságosabbá és robosztusabbá:

- a két tűzfalhoz különböző gyártó termékeit használjuk
- célszerű egy hardveres és egy szoftveres megoldást ötvözni
- praktikus különböző funkcionalitású eszközöket párosítani a skálázhatóság növelése szempontjából

A kettős tűzfal megoldás fent említett előnyei kiegészülve a különböző eszközök tudásával és tulajdonságaival egy sokkal biztonságosabb és magas szinten finomhangolható rendszert hoznak létre.

2.1. Cluster alkalmazása

Fontos szempont lehet a minél magasabb rendelkezésre állás érdekében mind a külső, mind a belső tűzfalak clusterben való alkalmazása is. Ez esetben az elsődleges eszköz esetleges meghibásodása esetén a forgalmat át tudjuk irányítani a másodlagos tűzfalra. Emellett megkönnyíti a frissítéseket is, mivel nem kell az éles rendszert tesztelés nélkül módosítani, hanem először el tudjuk végezni a másodlagos (nem aktív) tűzfalon a frissítést, ezután átterelni rá a forgalmat, majd frissíteni a cluster másik tagját, és ezután visszairányítani rá a forgalmat. Ha valamilyen probléma merülne fel a frissítést követően, könnyedén vissza tudunk állni a másik node-ra, nem okozva ezzel nagyobb fennakadást a hálózati forgalom kiszolgálásában.

2.2. A *Zorp Gateway* nyújtotta előnyök

A *Zorp Gateway* alkalmazás proxy tűzfal egy rendkívül rugalmas, jól testreszabható többfunkciós hálózatbiztonsági szoftver:

- Alkalmazás szinten képes szűrni vagy akár módosítani az adott forgalmat, megvédve ezzel a kritikus rendszereket a magas szintű külső és belső támadásoktól.
- A Deep Packet Inspection (DPI) technológiát alkalmazva, a forgalom egészét vizsgálva - beleértve a hálózati csomag tartalmát is - tudja szűrni a hálózati protokollok szabványait (standards), és az erre vonatkozó beállított szabályokat sértő kapcsolatokat.
- Rugalmas architektúrájának és programozható konfigurációjának köszönhetően bármilyen biztonsági szabályrendszert képes követni, akár a Zero Trust modellt is.
- A *Zorp Gateway* lehetővé teszi a titkosított csatornák kezelését magas szintű titkosítás támogatása mellett, illetve az azon áthaladó teljes forgalom felügyeletét és szűrését, mindezt alkalmazás szinten. Emellett segítségével titkosíthatjuk a nem titkosított vagy régi, már nem támogatott hálózati protokollokat is.
- A *Zorp Gateway* menedzsment felületén a cluster is könnyen beállítható és kezelhető. Ugyanitt a konfigurációk konzisztenciáját is könnyű megtartani, illetve követni.

2.3. *Zorp Gateway* és *Cisco* tűzfalak együttes használata

Az alábbi esettanulmányban a kettős tűzfalrendszer alkalmazásának lehetőségeit vizsgáljuk meg, a *Zorp* és a *Cisco* tűzfalak használatával.

A *Zorp Gatewayt* például egy *Cisco ASA* vagy *FirePower* tűzfallal kiegészítve egy sokrétű, megbízható és magas szinten finomhangolható tűzfalrendszert hozhatunk létre. Ahogy korábban láttuk, érdemes különböző gyártók termékeit ötvözni, emellett célszerű egy hardveres és egy szoftveres megoldást alkalmazni. Esetünkben, a *Zorp* tűzfal oldalról a szoftveres, a *Cisco* tűzfal részéről pedig a hardveres (appliance) kritérium teljesül.

A *Zorp Gateway* alkalmazás proxy tűzfal által kínált magas szintű protokollszűrési lehetőségek, illetve a *Zorp* nyújtotta, jelenleg ismert legerősebb titkosítási képességek nagyszerűen kombinálhatóak a *Cisco* vagy bármelyik másik gyártó (pl. *Checkpoint, Fortinet, Juniper, Palo, Alto,* stb.) megoldásaival.

A felépítés szempontjából két lehetőségünk van, aszerint, hogy melyik tűzfal hol helyezkedik el. Azt, hogy melyik a megfelelő megoldás, számos körülmény befolyásolhatja:

- a szükséges funkcionalitás
- a meglévő rendszer bővítési lehetőségei
- a vállalati vagy külső szabályozások

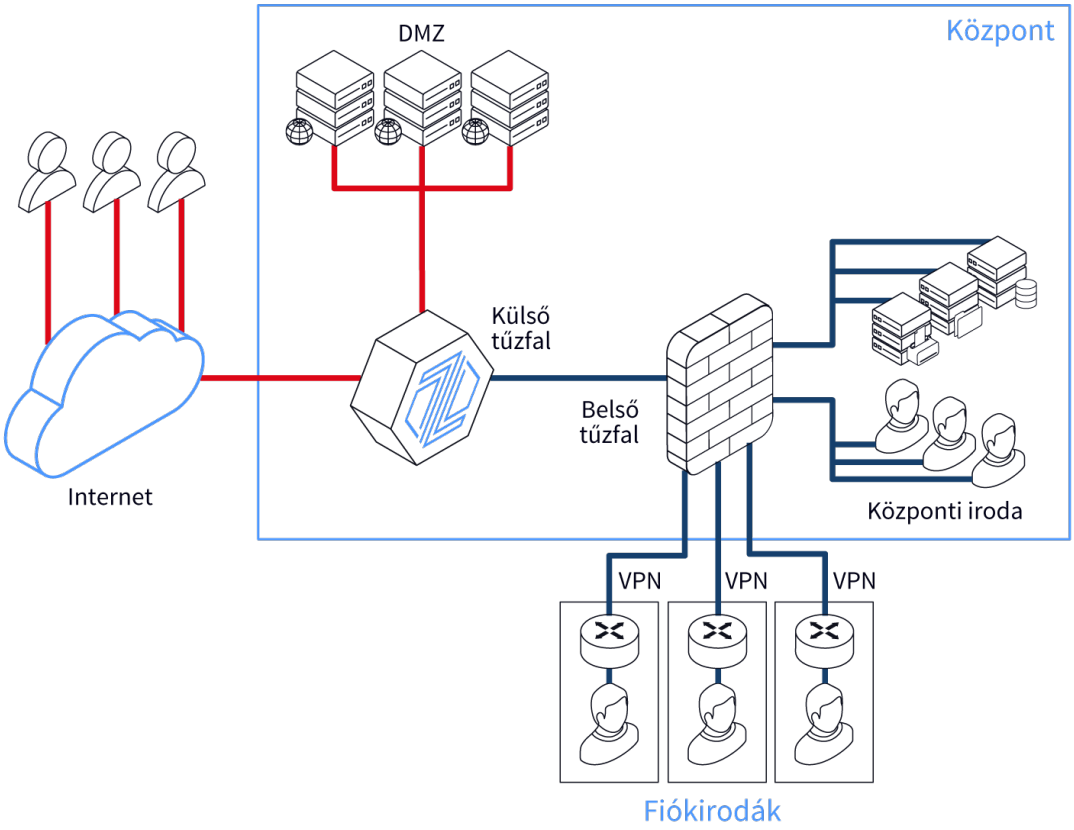
Az alábbiakban a *Cisco* tűzfal megoldásaival való együttműködésre mutatunk példákat.

2.4. Gyakorlati példa 1: *Zorp Gateway* mint külső tűzfal, *Cisco* mint belső tűzfal

Az alábbi példában egy olyan kettős tűzfalrendszert mutatunk be, ahol a *Zorp Gateway* áll a külső oldalon és egy *Cisco* tűzfal (*ASA*, *FirePower*) a belső oldalon.

Az internet felől egy *Zorp* tűzfal szűri a kintről érkező hálózati forgalmat a két tűzfal között kialakított DMZ zóna felé. A DMZ kialakítható a két tűzfal között vagy közvetlenül a *Zorp* egyik interfészén is. Az itt található szerverek az internetről, illetve a belső hálózatról is elérhetőek, a befelé irányuló forgalmuk viszont erősen korlátozott. A belső tűzfal, ami esetünkben egy *Cisco ASA* vagy egy *Firepower*, védi a belső hálózatot, és kezeli a DMZ és a belső hálózat közötti kapcsolatot.

Ez a megoldás hasznos lehet például egy sok telephellyel rendelkező vállalat esetén, amelynek több, kisebb fiókirodája is van. A telephelyeken sok esetben nincs magas szintű forgalmi szűrés, egy *Cisco* router vagy egy *Cisco ASA* biztosítja az átjárót az internetre. A működéshez szükséges belső szerverek elérését a telephelyek és a központ között kialakított site-to-site VPN kapcsolat biztosítja, amely jellemzően egy *Cisco ASA* vagy *FirePower* eszközön keresztül történik. A kettős tűzfalrendszer kialakításánál ezen eszköz funkcionál belső tűzfalként, így a site-to-site (S2S) kapcsolatokat azonos gyártójú eszközök kezelik, a belső hálózatot pedig módosítás nélkül továbbra is elérik. A *Zorp* külső tűzfalként való alkalmazása lehetővé teszi a DMZ-hez tartozó eszközök szeparálását, illetve segítségével titkosíthatjuk a nem titkosított vagy gyengébb titkosítással rendelkező kapcsolatokat is. Emellett akár a fiókirodák internetelérését is át lehet irányítani a központ felé a *Zorp* tűzfalon végzett protokoll- és tartalomszűrés céljából.



2. ábra - Példa a Zorp, mint külső tűzfal és Cisco, mint belső tűzfal kettős tűzfalrendszerben való alkalmazására

Több kisebb iroda helyett egy nagyobb (központi) iroda esetén is kiváló megoldás egy *Zorp* tűzfal alkalmazása kettős tűzfal kialakításához. A felhasználók internetre irányuló forgalmát a fenti példához hasonlóan, alkalmazás szinten leszünk képesek szűrni.

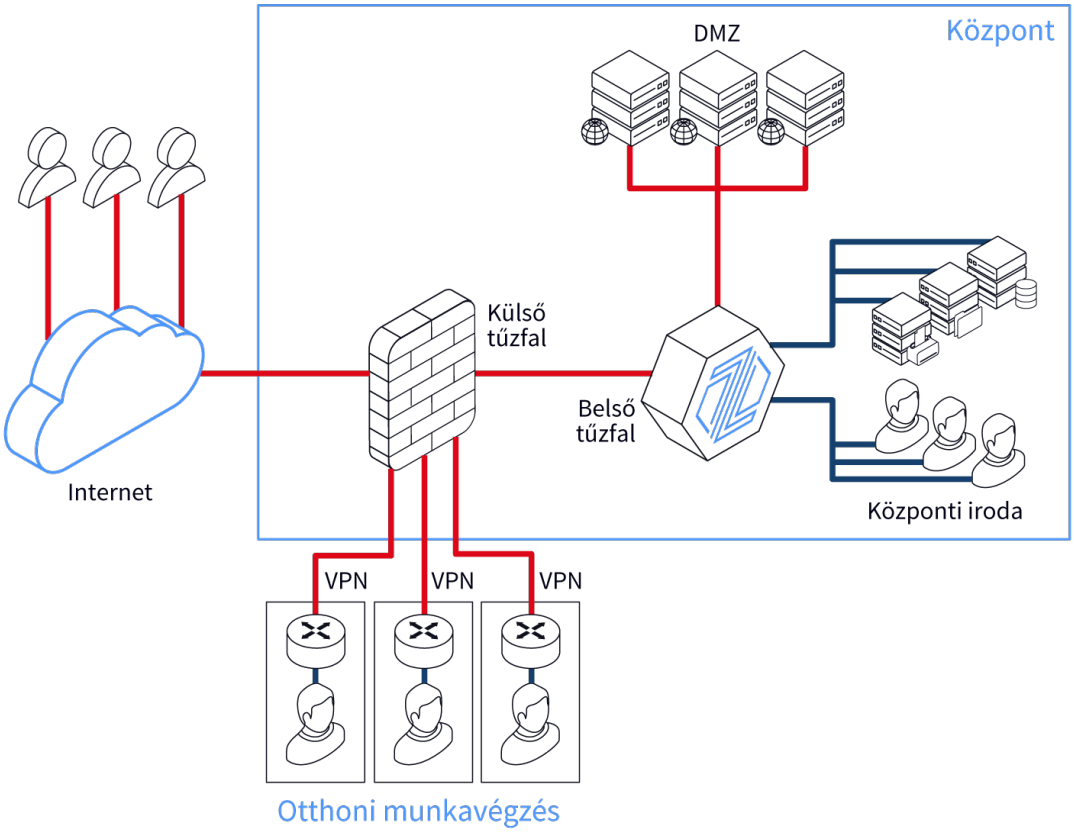
Tegyük fel például, hogy vállalatunk az internet irányába csak a TCP/80 (HTTP) és TCP/443 (HTTPS) portok használatát engedélyezi a felhasználóknak. Azon tűzfalak, amelyek nem képesek alkalmazás szinten elemezni a forgalmat, csupán protokoll, forrás és cél port, illetve forrás és cél IP cím alapján tudják szűrni a hálózati csomagokat. Ezt a fajta szűrést viszonylag egyszerűen ki lehet játszani, ha például a felhasználó egy SSH tunnelt épít ki egy külső szerverrel az engedélyezett portok valamelyikére. A *Zorp Gateway-el* azonban ez könnyedén kiszűrhető, mivel egy HTTP proxyt használva az adott tűzfalszabályon a forgalom HTTP protokoll ellenőrzésen fog átesni. Mivel a fenti példában leírt kapcsolat sérti ezt, így az blokkolásra kerül egy naplóbejegyzés kíséretében. Az egyes proxyk maximálisan testre szabhatóak, akár saját proxyt is írhatunk hozzá.

2.5. Gyakorlati példa 2: *Zorp* mint belső tűzfal, *Cisco* mint külső tűzfal

Az alábbi példában a *Zorp - Cisco* kettős tűzfalrendszer egy egyszerűbb, általánosabban használt esetét mutatjuk be, ahol a *Zorp Gateway* áll a belső oldalon, és egy *Cisco* tűzfal a külső oldalon.

Mivel a forgalom alkalmazás szinten történő elemzése és szűrése minden esetben lassabb és erőforrásigényesebb egy egyszerű csomagszűrővel történő szabályozásnál, ezért a proxy tűzfalak elé helyezett külső tűzfal jellemzően

egy egyszerűbb csomagszűrő tűzfal (pl. *Cisco ASA*). A külső tűzfal elsődleges célja tehát előszűrni a befelé irányuló forgalmat, ezáltal tehermentesíteni a belső tűzfalat, amelynek így már csak a releváns forgalmat kell alkalmazás szinten szűrnie.



3. ábra - Példa a Zorp, mint belső tűzfal és Cisco, mint külső tűzfal kettős tűzfalrendszerben való alkalmazására

Előfordulhat az is, hogy egy már meglévő *Cisco* tűzfalat szeretnénk kiegészíteni kettős tűzfalrendszerre a korábban leírt előnyök kihasználása céljából. A *Zorp* belső tűzfalként történő alkalmazásánál úgy tudjuk bővíteni a hálózatot, hogy nem kell változtatnunk az internet átjárón.

3. Konklúzió

A minél magasabb védelmi szint elérése érdekében célszerű az olcsóbb, ám alacsonyabb védelmet nyújtó, egy tűzfalas megoldásokat kettős tűzfalrendszerre bővíteni. A kettős tűzfalrendszer lehetővé teszi többek között a DMZ-ben lévő, internetről is elérhető szerverek szeparációját, ezáltal csökkenthetjük a belső rendszerünk kitettségét a kívülről érkező veszélyeknek. A kettős tűzfalrendszer hatékonyságát növeli, ha tűzfalaink két különböző gyártótól származnak, például ha meglévő hardveres tűzfalmegoldásunkat a *Zorp* szoftveres tűzfalmegoldásával ötvözzük. A *Zorp* tűzfal kiválóan kiegészíti a *Cisco ASA* és *Firepower* tűzfalakat kettős tűzfalrendszer alkalmazása esetén.

A *Zorp Gateway* által kínált kimagasló protokollszűrési képesség, illetve a jelenleg ismert legerősebb titkosítási lehetőségek nagyszerűen kombinálhatóak bármelyik másik gyártó (pl. *Cisco*, *Checkpoint*, *Fortinet*, *Juniper*, *Palo Alto*) megoldásaival is, amennyiben a cél egy magasabb szintű biztonság elérése kettős tűzfalrendszerrel.

4. További anyagok

Zorp Gateway főoldal

Próbaverzió igénylése