Zorp

Termékleírás

Előszó

A Zorp teljes ellenőrzést biztosít a normál és titkosított hálózati forgalom felett, és képes a forgalom tartalmának szűrésére és módosítására is.

A Zorp tűzfal egy határvédelmi eszköz, melyet kiterjedt informatikai hálózattal és magas biztonsági igényekkel rendelkező vállalatok számára fejlesztettek ki. A Zorp megvizsgálja és elemzi a hálózati forgalom tartalmát, és ellenőrzi, hogy megfelel-e a használt hálózati protokoll (például HTTP, IMAP, stb.) előírásainak. A Zorp központi tartalomszűrő szolgáltatást is nyújt a hálózat számára, beleértve a vírus- és spamszűrést, és a titkosított és beágyazott protokollok széles skálájának vizsgálatát, mint például a biztonságos böngészéshez használt HTTP vagy a levelezéshez használt POP3S. A termék fejlett autentikációs metódusokat is támogat, mint például a Single Sign On vagy a külső csatornán történő (out-of-band) autentikáció. A Zorp központi menedzsment felülete több tűzfal kezelésére is alkalmas, és hihetetlen rugalmasan konfigurálható, hogy az eltérő igényeket is kielégítse.

A Zorp technológia hatékony válasz a ma és a holnap biztonsági kihívásaira. A technológiára épülő termékek lehetőséget adnak az informatikai vezető számára, hogy a legmagasabb szintű biztonsági előírásokat is kompromisszumok nélkül valósítsa meg.

Tipikus felhasználók

A Zorp alkalmazásszintű határvédelmi technológia által nyújtott védelem alkalmas a legmagasabb szintű biztonsági igények kielégítésére is. A Zorp tipikus felhasználói az államigazgatási, a pénzügyi és a távközlési szektorból, illetve az iparvállalatok közül kerülnek ki.

Különösen indokolt a technológia alkalmazása a következő esetekben:

- Érzékeny információt kezelő vagy kritikus üzleti folyamatot megvalósító hálózat védelme.
- Egyedi, különleges IT biztonságtechnikai probléma megoldása.
- Titkosított csatornák (például HTTPS, POP3S, IMAPS, SMTPS, FTPS, SFTP, stb.) szűrése.
- Központi tartalomszűrés (vírus és spam) akár titkosított csatornákban is.
- Speciális protokollok (például Radius, SIP, SOAP, SOCKS, MS RPC, VNC, RDP, stb.) szűrése.
- Single Sign On (Kerberos) autentikáció megvalósítása.
- Felhasználói szintű QoS megvalósítása.

Alkalmazási területek

A széleskörű szolgáltatáspalettának és a részletes testre szabási lehetőségeknek köszönhetően a Zorp technológia több, egymástól jól elkülöníthető területen is hatékonyan alkalmazható.

Általános tűzfal

Általános célú proxy tűzfal, alkalmazásszintű védelemmel több, mint húsz hálózati protokollban, rengeteg beállítási lehetőséggel.

Tartalomszűrés

Vírus- és spamszűrés egyedülálló módon több, mint tíz normál és titkosított hálózati protokollban, akár extrém méretű terhelésre is.

Szervervédelem

Alkalmazáskiszolgáló elé telepített tűzfal protokollellenőrzésre és a szerver biztonsági hiányosságainak kiküszöbölésére. MS Exchange szerverek távoli elérésének védelmére is kiválóan alkalmazható.

VPN végpont

SSL alapú és IPsec VPN végpont távoli telephelyek integrálásához, valamint WiFi hálózatok biztonságának növeléséhez.

Terhelés megosztás

Dinamikusan változó terhelés megosztás állapotinformációk alapján.

QoS

Felhasználói csoportokra vagy egyénekre; valamint kommunikációs csatornára (protokollokra), MIME típusra és fájlméretre szabható sávszélesség menedzsment.

Különleges termék tulajdonságok

Teljes körű protokollértelmezés

A Zorp a csomagszűrő tűzfalakkal ellentétben proxy szinten kezeli a hálózati kapcsolatokat. Az egyik oldalon végződteti őket, a másikon újakat kezdeményez; így az eszközön teljes valójában jelenik meg a forgalmazott információ, lehetőséget adva a teljes körű elemzésre. A Zorp több, mint húsz különböző hálózati protokollhoz rendelkezik elemző modullal, melyek mindegyike 100%-ban értelmezi a protokoll utasításait és attribútumait. Minden proxy modul ismeri a protokoll eredeti szabályait, ami alapján képes kiszűrni a szabványokat sértő kapcsolatokat. Minden proxy képes továbbá az adott protokoll TLS- és SSL-titkosított változatának ellenőrzésére is.

Egyedülálló konfigurációs lehetőségek

Minél több tulajdonságát ismerjük egy hálózati kapcsolatnak, annál pontosabb szabályokat írhatunk elő azzal kapcsolatban. A teljes körű protokollértelmezés által nyújtott rengeteg információ birtokában a Zorp adminisztrátorok soha nem látott pontossággal valósíthatják meg a biztonsági szabályzat hálózati határpontokra vonatkozó rendelkezéseit. Az egyszerűsített szabályszerkesztő felület ellenére a termék rugalmas konfigurációs lehetőségeket nyújt, mely segít elkerülni a rossz kompromisszumokat a hatékonyan működő üzleti folyamatok és a megfelelő szintű biztonság között.

Visszahatás a hálózati forgalomra

A Zorp nem csupán kifinomult döntések meghozatalára képes a hálózati forgalomból nyert információ alapján, de képes a forgalom bizonyos elemeinek módosítására is az előírásoknak megfelelően. Mindez lehetővé teszi biztonsági kockázatot rejtő adatok elrejtését, de akár a tűzfal mögött lévő alkalmazások biztonsági hiányosságainak orvoslását is.

Titkosított csatornák ellenőrzése

A Zorp technológia teljes körű ellenőrzést kínál a titkosított csatornák felett. A beágyazott adatforgalom mélyreható vizsgálata már önmagában is olyan potenciális támadásokat képes felfedni és megállítani, mint vírusok, trójai programok és más kártékony kódok. A termék ezen képessége védelmet nyújt veszélyes tartalmú weboldalak vagy fertőzött e-mailek ellen, akkor is, ha azok titkosított (HTTPS, POP3S vagy IMAPS) csatornán érkeznek. Az SSH és az SSL forgalom ellenőrzése a protokollok olyan jellegzetes szolgáltatásainak elkülönített kezelését is lehetővé teszi, mint például a port- és x-forward. Ezen felül a technológia megengedi, hogy a tanúsítványok ellenőrzésén keresztül a tűzfal meghatározza, mely távoli szerverekhez kapcsolódhat a felhasználó. Adott esetben tehát a vállalati biztonsági szabályzat letilthat érvénytelen tanúsítványt felmutató, megbízhatatlan weboldalakat.

Központosított menedzsment

A Zorp központi, könnyen kezelhető menedzsment rendszere segítségével a Zorp eszközök több, akár egymástól teljesen különböző csoportja is adminisztrálható. Így a különböző telephelyeken, vagy akár különböző cégekhez tartozó eszközök egyetlen közös felületről menedzselhetők. A rendszer segítségével egységes felületről felügyelhetők a Zorp infrastruktúra-elemek licenszei és tanúsítványai is. A rendszer email riasztást küld az adminisztrátornak a licenszek és tanúsítványok lejáratáról. Ezen felül a Zorp könnyen integrálható külső rendszerfelügyeleti eszközökkel is, melyek igény esetén ellátják a szolgáltatás-felügyeleti funkciókat.

Tartalomszűrés a hálózati határponton

A Zorp platformot kínál a vírusellenőrző motorok számára, melyek a Zorp architektúra lehetőségeit kihasználva képessé válnak olyan adatcsatornák ellenőrzésére is, melyre önmagukban nem lennének alkalmasak. A Zorp eszközök moduláris felépítése és több, mint húsz proxy modulja lehetővé teszi a vírus– és spamszűrő termékek számára, hogy egyedülállóan sokféle protokollban és azok titkosított változataiban is megtalálják a kártékony kódokat.

Single Sign On autentikáció

Valamennyi hálózati kapcsolat egyetlen autentikációhoz kötése nagymértékben megkönnyíti a felhasználói jogosultságkezelést és a rendszerauditot. A Zorp single sign on megoldása egyszerű és felhasználóbarát megoldás Active Directory-val történő együttműködésre. A Zorp autentikációs modul tökéletesen integrálja a meglévő adatbázisokat, legyen az LDAP, PAM, AD vagy RADIUS. A jelszavas és erős autentikációs metódusokat (S/Key, SecureID, X.509, stb.) egyaránt támogatja a termék. A Zorp 3.4-gyel kezdődően az RDP és SSH proxyk a tanúsítvány alapú (X.509) autentikációt is támogatják, lehetővé téve a smartcard megoldások használatát és a nagyvállalati PKI rendszerekkel való integrációt.

Teljes körű IPv6 támogatás

A Zorp minden komponense támogatja az IPv6-alapú címeket, zónákat, alhálózatokat, hálózati interfészeket, NAT házirendeket és így tovább. A hálózati címfordítás az IPv4 és IPv6 hálózatok között szintén támogatott.

Architektúra

A Zorp komponensei

A Zorp különálló komponensekből épül fel, moduláris szerkezete nagyfokú rugalmasságot tesz lehetővé. Egy tipikus Zorp átjáró az alábbi komponensekből áll:

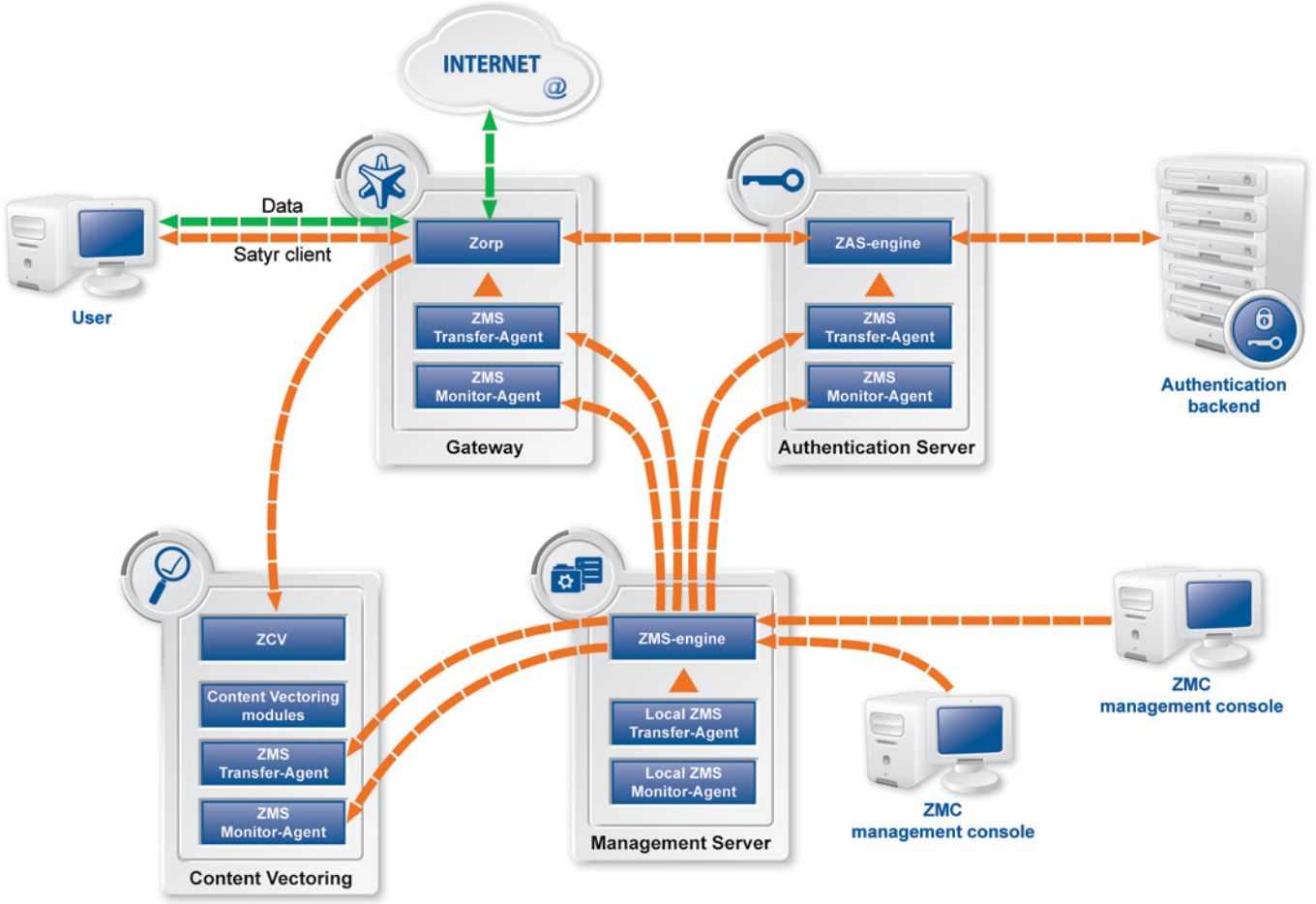
- Zorp: A Zorp maga az alkalmazásszintű proxy átjáró, mely ellenőrzi és elemzi az összes átmenő kapcsolatot.
- Zorp Management System (ZMS): A Zorp komponenseinek központi vezérlő szervere. A ZMS adatbázisban tárolja az összes komponens beállítását (a biztonsági politika implementációját), és ebből generálja le a komponensek számára szükséges konfigurációs állományokat.
- Transfer és monitoring agentek: A ZMS és a többi komponens közti kommunikációt megvalósító programok.
- Zorp Management Console (ZMC): Grafikus kezelőfelület a ZMS-hez, az adminisztrátor ennek segítségével tartja karban a rendszer elemeit.
- Zorp Authentication System (ZAS): Hálózati kapcsolatok autentikálását megvalósító komponens. A kapcsolatok autentikálásakor közvetítő szerepet tölt be a Zorp és a felhasználói adatokat tároló adatbázis (például Microsoft Active Directory) között.
- Zorp Content Vectoring System (ZCV): Tartalomszűrő keretrendszer számos különböző (például vírus- és spamszűrő) modullal. A Zorp által ellenőrzött forgalom adatrészét lehet vele ellenőrizni, akár titkosított forgalom esetén is.

A Zorp konfigurálásának és a forgalom ellenőrzésének a menete

Az adminisztrátor a grafikus ZMC felület segítségével kapcsolódik a ZMS szerverhez, ahol megvalósítja a szervezet biztonsági politikáját a komponensek megfelelő beállításával. Ezután az elkészített konfigurációs állományokat ZMS-ről áttölti a rendszer komponenseire. Az állományok elhelyezését a komponenseken a transfer agent végzi el.

A Zorp a konfigurációs beállítások alapján ellenőrzi a forgalmat

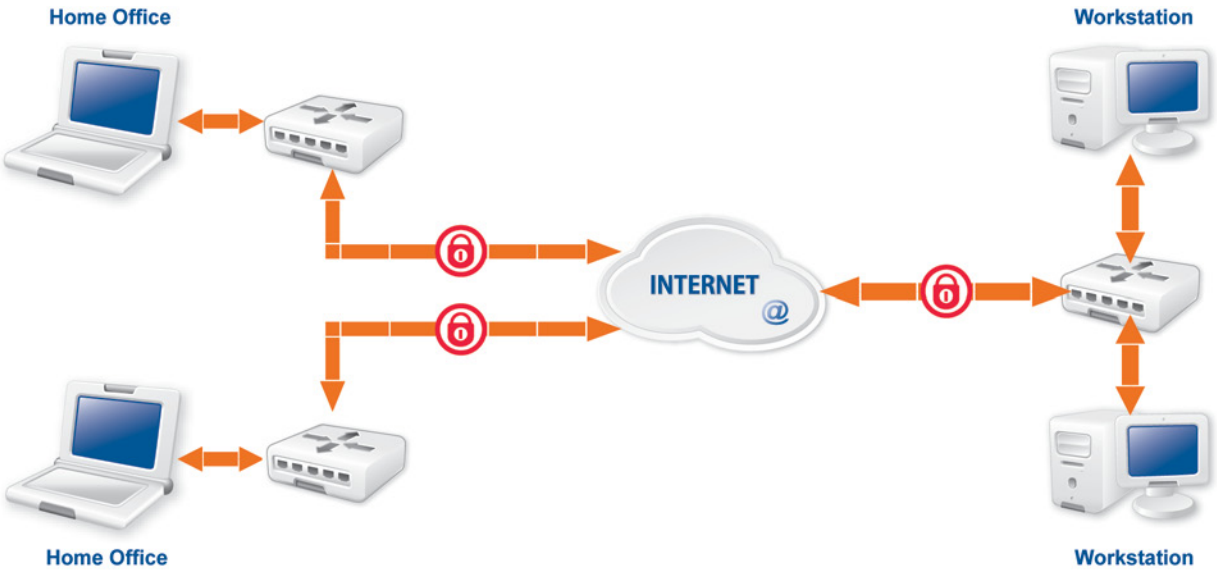
A Zorp fogadja a felhasználók által kezdeményezett kapcsolatokat. Ha a kapcsolatot autentikálni kell, bekéri a felhasználótól a szükséges adatokat (pl.: jelszó), és a ZAS közvetítésével ellenőrzi a helyességüket. Amennyiben az autentikáció sikeres, a Zorp kiépíti a kapcsolatot a szerver fele, és megkezdődhet az adatok továbbítása a szerver és a kliens között. A kommunikáció során a Zorp proxyjai ellenőrzik a kommunikációs protokollt (titkosított protokoll esetén több, egymásba ágyazott proxy révén). A Zorp a protokollban érkező adatokat átadja a ZCV-nek tartalomszűrésre, ami például elvégzi a vírus- és spamszűrést, vagy a HTTP forgalom tematikus szűrését. A kliens csak a tartalomszűrés után kapja meg az ellenőrzött adatokat.



Virtuális magánhálózatok

Gyakorta szükséges több hálózat vagy gép összekötése nem megbízható (általában nyilvános) hálózaton keresztül – például egy több telephely, vagy otthonról dolgozó munkatársak esetén. Ilyenkor fontos, hogy a kapcsolat megfelelően titkosított legyen, és ne kerülhessenek az adatok illetéktelen kezekbe. Erre a problémára nyújtanak megoldást a virtuális magánhálózatok (Virtual Private Networks, VPNs).

A VPN megőrzi a kapcsolat bizalmasságát, hitelességét, és sértetlenségét; vagyis biztosítja, hogy illetéktelenek nem tudják lehallgatni, módosítani a kommunikációt, valamint hogy a kommunikáló felek valóban azzal kommunikálnak, akivel akartak.



Támogatott VPN típusok és implementációk

A VPN-eknek több típusa, és minden típusnak több implementációja van. A Zorp az alábbiakat támogatja:

- IPSec (strongSwan — http://en.wikipedia.org/wiki/StrongSwan)
- SSL (OpenVPN)

Mind a fix IP című, mind a dinamikus IP című (RoadWarrior) kapcsolatok támogatottak, pont-pont és hálózat-hálózat topológiában egyaránt.

Testre szabható konfiguráció

A Zorp egyszerűsített szabályszerkesztő felülete ellenére magas fokú rugalmasságot biztosít a kapcsolatok paramétereinek és a protokollok elemeinek kiértékelésében, így elkerülhető a hatékony üzleti folyamat és a megfelelő szintű biztonság közötti rossz kompromisszum.

Rugalmasság és dinamikus döntések

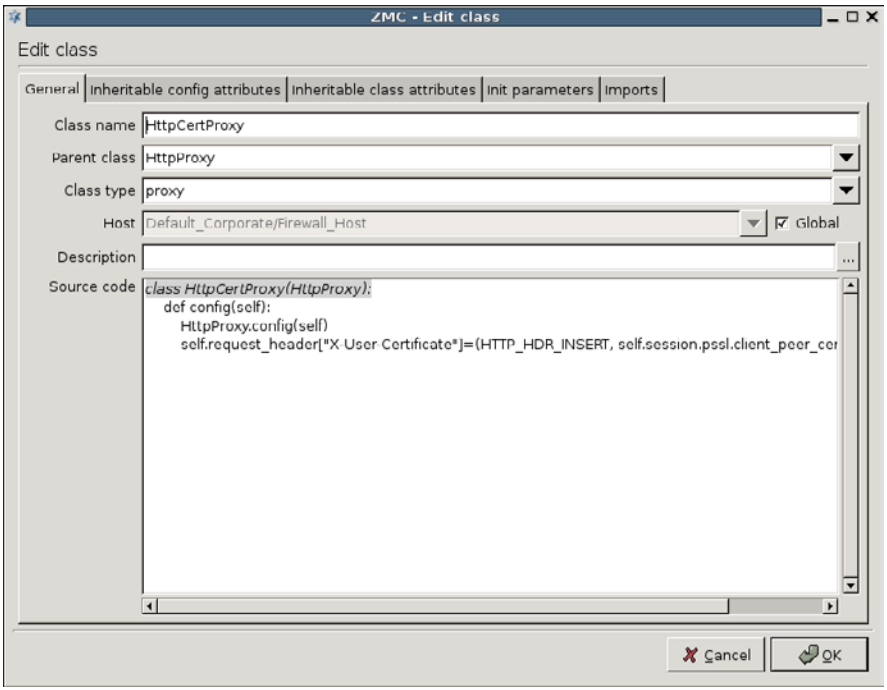
A Zorp segítségével egy adott kapcsolatról dinamikusan hozhatók akár összetett, többváltozós döntések is. A Zorp proxyk szintjén a rendelkezésre álló információ – kliens IP címe, protokoll fejlécek, stb. – teljes skálája felhasználható, és tetszőleges algoritmussal kiértékelhető. A döntés alapján szabályozni lehet a kapcsolat más paramétereit, a protokoll elemzésének mértékét, a cél szerver címét, stb. Erre a jól ismert Python programozási nyelv nyújt lehetőséget.

A Python nyelv támogatása

A Zorp döntési és konfigurációs rétege Python nyelven lett implementálva: a proxyk és egyéb osztályok teljes mértékben testre szabhatóak e nyelven. Az osztályok módosításához a Zorp grafikus felületet biztosít. Létező Python modulok is importálhatóak és a saját függvényekben, osztályokban felhasználhatóak.

Néhány egyszerűbb példa:

- HTTP forgalomban megkövetelhető, hogy a felhasználók adott típusú/verziójú böngészőt használjanak. Más böngésző esetén a Zorp megszakíthatja a kapcsolatot, vagy kisebb sávszélességet rendelhet a kapcsolathoz.
- A szervereken futó alkalmazások adatait (szerver banner), valamint a szerverek hibaüzeneteit el lehet távolítani a forgalomból, így a belső infrastruktúráról kevesebb információ érhető el illetéktelenek számára.
- Egy letöltött állományt a típusától, vagy származási helyétől függően lehetőség van szigorúbb vírusellenőrzésnek alávetni.
- Szabályozható, hogy adott helyről (címről) csak adott felhasználó férhessen hozzá egy szolgáltatáshoz (kliens cím és felhasználónév ellenőrzés).



Fürtözés

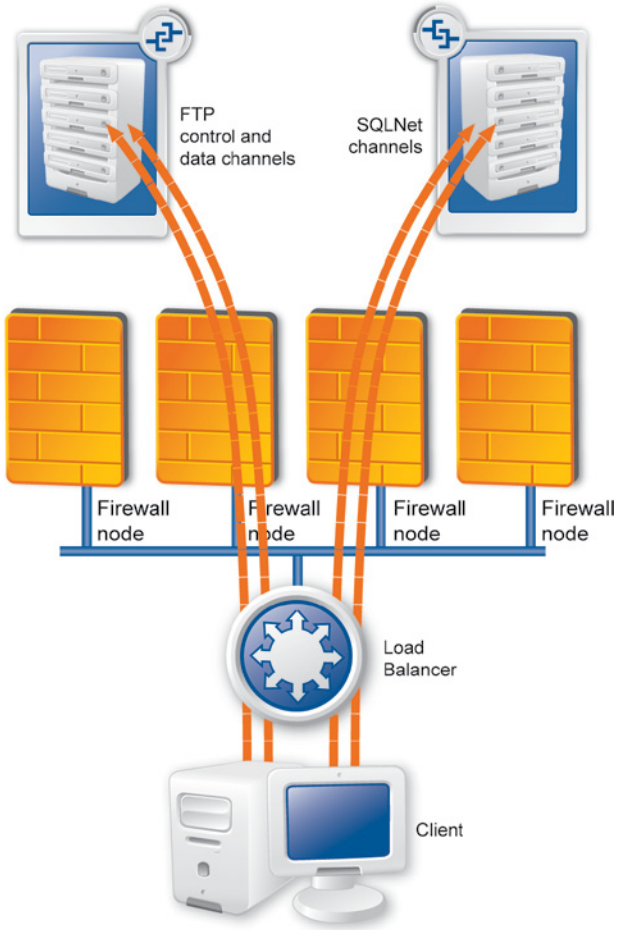
A hálózati átjáró folyamatos működése elengedhetetlen fontosságú, mivel a hálózat szegmensei (pl.: Internet – intranet, ügyfelek – szerverek, stb.) csak az átjárón keresztül kapcsolódhatnak egymáshoz. Ha hardver meghibásodás, vagy programhiba miatt az átjáró leáll, ez a kapcsolat megszűnik, és elérhetetlenné válhatnak az üzleti szempontból kritikus szolgáltatások. Az ilyen helyzetek elkerülésére alkalmazható a fürtözés, melynek lényege, hogy egy helyett több, azonosan konfigurált hardvert használunk ugyanarra a feladatra. A fürtözés alapvetően két célt szolgálhat: Magas rendelkezésre állást és terhelés megosztást.

Magas rendelkezésre állás (High Availability, HA) biztosítása

A HA fürt célja a leállási idők csökkentése, illetve a rendszer működésben tartása tervezett leállások, vagy akár a fürt egyik elemének meghibásodása esetén is. Egyszerre a fürt elemei közül csak az egyik aktív, ezeket a többi elem folyamatosan monitorozza. Amennyiben egy aktív elem leáll, a tartalék elem veszi át a szerepét.

Terhelés megosztás (Load Balance, LB)

A fürt célja nagy forgalom kezelése, amit egyetlen eszköz már nem lenne képes feldolgozni. Ennek érdekében az összes elem egyszerre működik, köztük egyenletesen kerül elosztásra a terhelés. Fontos, hogy többcsatornás protokollok (például FTP) esetén az egy kliensről érkező kapcsolatokat a fürtnek ugyanahhoz az eleméhez kell irányítani. Python szkripten keresztül állapotinformációk alapján döntő intelligens terhelésmegosztás is megvalósítható.



A Zorp elemeinek fürtözése

A Zorp összes, a folyamatos működés szempontjából lényeges eleme fürtözhető, beleértve magát a Zorpot, a tartalomszűrő rendszert (Zorp Content Vectoring, ZCV), valamint az autentikációs rendszert (Zorp Authentication System, ZAS).

A legtöbb IT biztonsági politika nem engedi meg az ellenőrizetlen tartalmak átengedését, ezért egyetlen tartalomszűrő szerver használata nem elegendő, mivel bármilyen hiba esetén a teljes forgalom leállhat. A tartalomszűrés szigorúságától (például a használt víruskereső modulok száma) és a tűzfalon átmenő forgalom mennyiségétől függően szükség lehet terhelés megosztásos fürt kialakítására is, az adatok megfelelő sebességű ellenőrzése érdekében.

Szerver fürtök kiszolgálása Zorppal

Gyakran előfordul, hogy a Zorp szerverfürtöket véd. Ilyen esetekben fontos, hogy lehetőleg már a Zorp a megfelelő, éppen aktív elemekhez irányítsa a bejövő kapcsolatokat. A Zorp lehetőséget nyújt failover típusú kapcsolódásra, vagyis ha a szerverfürt egyik eleme nem elérhető, automatikusan a következő aktív elemhez kapcsolódik. A beérkező kapcsolatok round-robin jelleggel is eloszthatóak a fürt elemei között, ilyenkor a Zorp minden új kapcsolatot a fürt soron következő, aktív eleméhez irányít.

Támogatott fürtözési megoldások

Magas rendelkezésre állás esetén

- A használt IP cím (Service IP) átvétele
- MAC cím átvétele
- RIP üzenetek alapján történő átállás

Terhelés megosztás esetén

- DNS alapú terhelés megosztás
- Terhelés megosztás külső eszköz segítségével
- Multicast MAC cím alapú terhelés megosztás

Autentikáció

A Zorp Authentication Server (ZAS) segítségével lehetővé válik a hálózati átjárón átmenő összes kapcsolat autentikálása. A hálózati autentikáció célja a felhasználók által kezdeményezett kapcsolatok autentikálása, annak érdekében, hogy csak a megfelelő személyek érhessenek el bizonyos szolgáltatásokat. Ellentétben azzal a széles körben elterjedt gyakorlattal, amely a számítógép IP címét azonosítja a felhasználóval, a Zorp nyújtotta megoldással a teljes hálózati forgalom a felhasználók szintjén azonosítható és auditálható. A protokollon belüli (inband) és a protokollon kívüli (outband) autentikáció egyaránt támogatott. Az outband autentikáció előnye, hogy tetszőleges protokollal és autentikációs metódussal kombinálható, és segítségével egyszerű, a felhasználók számára transzparens single sign on (SSO) megoldás alakítható ki.

A ZAS dióhéjban

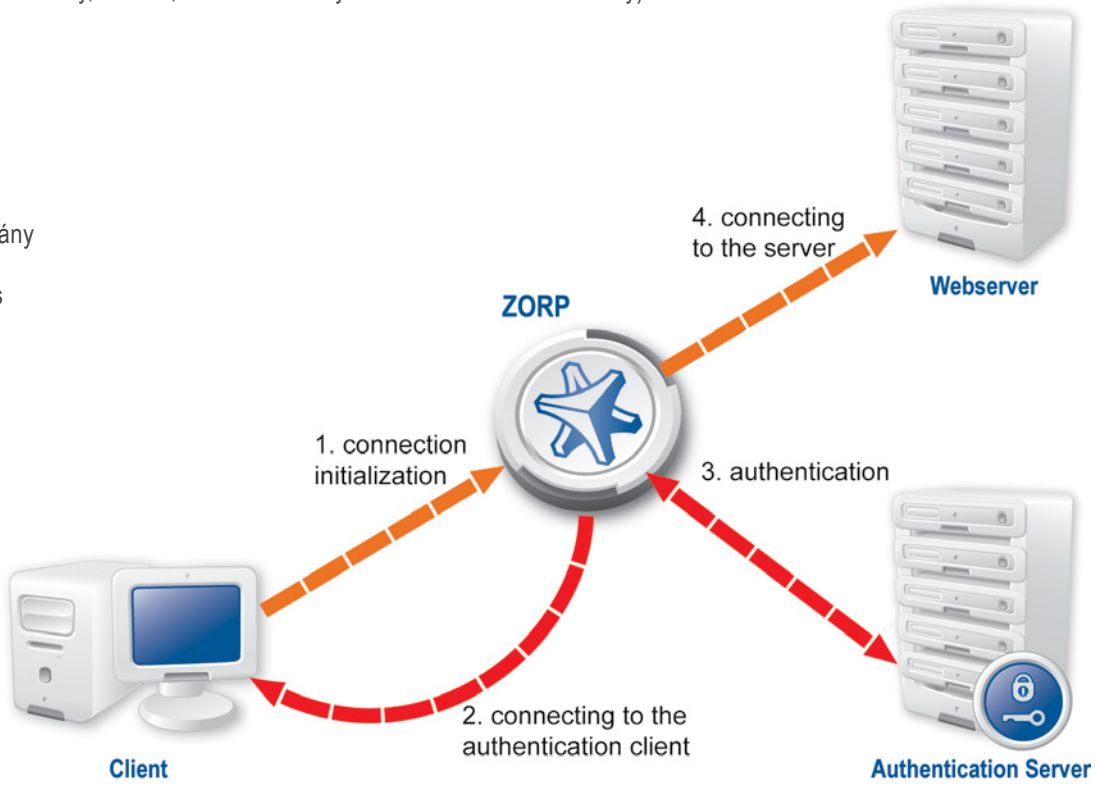
A ZAS nem egy autentikációs adatbázis, hanem egy köztes elem, ami a Zorp és a már meglévő, a felhasználók adatait tároló adatbázis között kommunikál. Így a hálózati forgalom autentikálása egyszerűen megvalósítható és könnyen beilleszthető a már kialakított infrastruktúrába. Amikor egy kliens megpróbál használni egy szolgáltatást (vagyis új kapcsolatot kezdeményez), amihez autentikáció szükséges, a Zorp az autentikáció adatait (például felhasználónév, jelszó, stb.) a ZAS szerver segítségével továbbítja a felhasználói adatbázisnak. A Zorp csak sikeres autentikáció esetén engedélyezi a kapcsolatot.

Támogatott adatbázisok

- LDAP (Microsoft Active Directory, POSIX, Novell Directory Services / Novell eDirectory)
- PAM
- RADIUS
- TACACS
- Apache htpasswd állomány
- Beépített ZAS adatbázis

Támogatott metódusok

- Felhasználónév/jelszó
- S/Key
- CryptoCard RB1
- LDAP binding
- GSSAPI/Kerberos5
- X.509 tanúsítvány



Single sign on

A Zorp Authentication Agent kliensprogram és a Kerberos protokoll segítségével olyan hatékony outband autentikáció valósítható meg, amely során a felhasználónak elég egyszer azonosítania magát, és minden további autentikációt automatikusan elvégez számára a rendszer. Az outband autentikáció további előnye, hogy a csak gyenge autentikációs metódusokat (például felhasználónév-jelszó) támogató protokollokhoz is elérhetővé teszi az erős autentikációs metódusok (például hardver token) használatát

Szolgáltatás minőségének (QoS) befolyásolása

A Zorp dinamikus döntéshozási rendszere lehetővé teszi, hogy a különböző felhasználók, csoportok eltérő minőségű kapcsolatokat vegyenek igénybe. Például a használt kliensalkalmazás, célszerver címe, stb.) alapján lehet korlátozni a kapcsolat sávszélességét és más paramétereit.

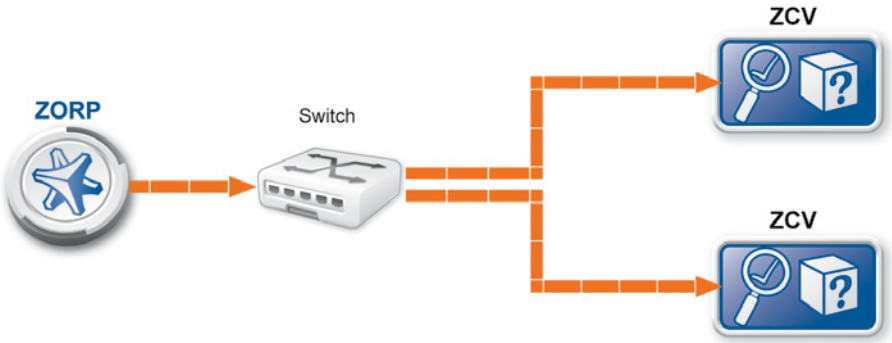
Víruskeresés és tartalomszűrés

A sok spam, a vírusok, trójaiak és egyéb káros tartalmak miatt manapság már elengedhetetlen a hálózati forgalom minél kiterjedtebb és mélyrehatóbb szűrése. Ez a feladat a hálózati határponton végezhető el a legkényelmesebben, mivel ezen a ponton az összes Internet felől jövő (és kifele menő) forgalomnak át kell haladnia. A Zorp Content Vectoring (ZCV) tartalomszűrő keretrendszer a Zorp alkalmazásszintű átjáró révén több mint tíz hagyományos és beágyazott protokollt képes elemezni, és natívan támogatja a magas rendelkezésre állást, valamint a terhelés megosztást is. Segítségével lehetővé válik a titkosított protokollok (HTTPS, POP3S, stb.) ellenőrzése is, melyeket egyre gyakrabban használnak kártékony kódok letöltésére.

A ZCV dióhéjban

A Zorp alkalmazásszintű átjáró csak a forgalom protokoll-specifikus részét vizsgálja, a tartalom ellenőrzését a ZCV-re bízza. A ZCV nem egy tartalomszűrő motor, hanem egy keretrendszer, amely egységes felületet nyújt számos tartalomszűrő modul (például vírus és spamszűrők) menedzseléséhez és konfigurálásához. A Zorp az átvizsgálandó adatokat (az adott forgalom típusának és besorolásának megfelelő paraméterekkel együtt) átküldi a ZCV-nek. A ZCV az adatokat továbbküldi a tartalomszűrést végző moduloknak, így a tartalomszűrést a Zorptól független modulok hajtják végre, amik akár külön gépen is futhatnak. Ez az architektúra lehetővé teszi tartalomszűrő fürtök kialakítását is.

A ZCV rugalmasan konfigurálható; akár a vizsgált kapcsolat, e-mail, vagy állomány tulajdonságai alapján is eldöntheti, hogy melyik modulokkal, és azok milyen beállításaival történjen az adatok ellenőrzése. Különböző szolgáltatásokhoz használható ugyanaz a modul eltérő paraméterezéssel, így például egy vírusszűrő modul ellenőrizhet minden fájlt a tűzfalon átmenő HTTP forgalomban, és – eltérő paraméterekkel – az e-mailek csatolmányait. Különböző típusú forgalomhoz, állományokhoz akár eltérő modulcsoportokat is lehet rendelni. A fenti példában a HTTP forgalmat szűrheti egy vírusszűrő és egy tartalomszűrő modul, és eltávolítható minden kliensoldali szkript, míg az e-maileket ellenőrizheti ugyanaz a vírusszűrő modul (akár eltérő paraméterezéssel is) és egy spamszűrő.



Trickling

Az időtúllépés elkerülése és a felhasználók elégedettségének növelése érdekében a ZCV támogatja az ún. „csepegtetést” (trickling). Ez annyit jelent, hogy a proxy kis adatcsomagokat küld a kliensnek, ami így azt érzékeli, hogy lassan bár, de jön az adat. A csöpögtetés már a fájl letöltése alatt elkezdődhet, következésképpen ezt az adatot nem lehet vírusszűrővel ellenőrizni, így elméletileg lehetséges, hogy vírus is átjusson. Az ilyen szituációk elkerülése érdekében a ZCV a letöltött fájl mérete alapján határozza meg a kliensnek csepegtetendő adat mennyiségét, és mivel a fájl nem teljes, elhanyagolható annak az esélye, hogy a vírus működőképes lesz.

Karanténozás

A tartalomszűrő modulok által elutasított (fertőzöttnek vagy spamnek tartott) állományok általában törlésre kerülnek. Bizonyos esetekben ez nem elfogadható, ekkor az adatok karanténozására – átmeneti és biztonságos tárolására – van szükség, amíg ki nem derül, hogy tartalmaznak-e valamilyen fontos információt. Időnként egy állomány még akkor is fontos lehet, ha vírussal fertőzött, ugyanis a vírus eltávolítása nem mindig lehetséges, és a művelet esetenként magát az állományt is károsíthatja. Azt is figyelembe kell venni, hogy a víruskeresők és a spamszűrők sem tévedhetetlenek, így néha „ártatlan” állományokat és leveleket utasítanak el.

Az összes ZCV modul egy közös karantént használ. Ennek mérete rugalmasan szabályozható az állományok mérete, száma, vagy a karanténozás időpontja alapján. Ehhez hasonló szabályok akár a karanténozott állományok különböző típusaihoz is rendelhetők az állományról tárolt metaadatok (például fertőzés típusa, a küldő e-mail címe, stb.) alapján.

Támogatott modulok

A ZCV segítségével a Zorp több mint tíz protokollban végezhet vírusszűrést, beleértve titkosított protokollokat is, mint a HTTPS és a POP3S. Jelenleg a ZCV az alábbi modulokat támogatja:

1. Vírusszűrő modulok
    a. ClamAV (www.clamav.net)
    b. NOD32 (www.nod32.com)
2. Spamszűrő modulok
    a. SpamAssassin (spamassassin.apache.org)
    b. Commtouch (www.commtouch.com)
3. URL osztályozó és szűrő modul a HTTP és HTTPS tartalmak ellenőrzéséhez, melynek révén kontrollálható, hogy a felhasználók milyen típusú tartalmakat böngészhetnek. Minden URL egy adatbázis alapján kategorizálható. Egy adott URL-hez a hozzáférést az URL kategóriája alapján tiltható vagy engedélyezhető.
4. Egy HTML szűrő modul, amely az általános tartalomszűrésen kívül JavaScript, ActiveX, Java, és Cascading stylesheet (CSS) szűrésére is képes.
5. Egy általános adatfolyam szűrő modul (sed), amely az adatfolyamban előforduló sztringek manipulálására és szűrésére képes.
6. Egy általános e-mail fejléc szűrő modul (mail-hdr), az e-mailekben előforduló fejlécek manipulálására és szűrésére.

Telepítés és támogatott platformok

Támogatott hardver platformok

A Zorp alkalmazásszintű átjáró 64 bites operációs rendszeren fut , és az x86-64 (amd64) platformot támogatja.

Támogatott szoftver platformok

A Zorp alkalmazásszintű átjáró tagjai 64 bites Linux disztribúción futnak.

A ZMC grafikus kezelőfelület az alábbi operációs rendszereken érhető el:

- Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7
- GNU/Linux (Ubuntu 10.04 (Lucid))

Telepítés

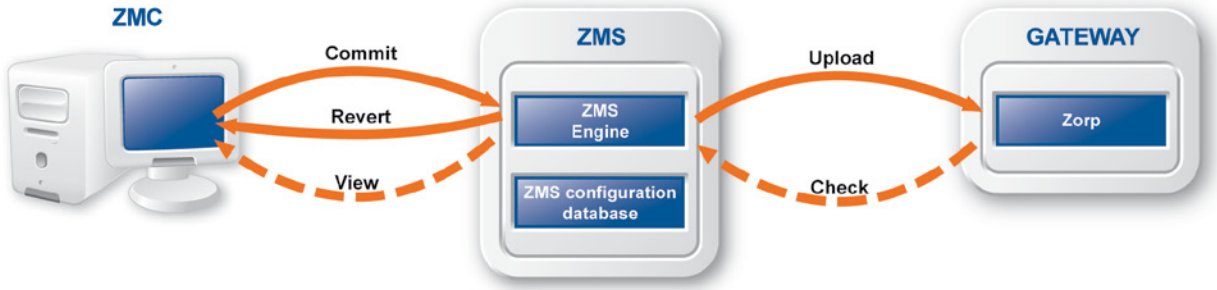
A Zorp alkalmazásszintű átjáró komponensei DVD-ROM-ról telepíthetők. A telepítendő gépnek grafikus kártyával vagy soros konzollal kell rendelkeznie.

Menedzsment rendszer és GUI

A Zorp központi, könnyen kezelhető menedzsment rendszere, a Zorp Management System (ZMS) segítségével a Zorp eszközök több, akár egymástól teljesen különböző csoportja is adminisztrálható. Így a különböző telephelyeken, vagy akár különböző cégekhez tartozó eszközök egyetlen közös felületről menedzselhetők. A rendszer segítségével egységes felületről felügyelhetők a Zorp infrastruktúra-elemek licenszei és tanúsítványai. Igény esetén a rendszer email riasztást küld az adminisztrátornak a licenszek és tanúsítványok lejárata előtt.

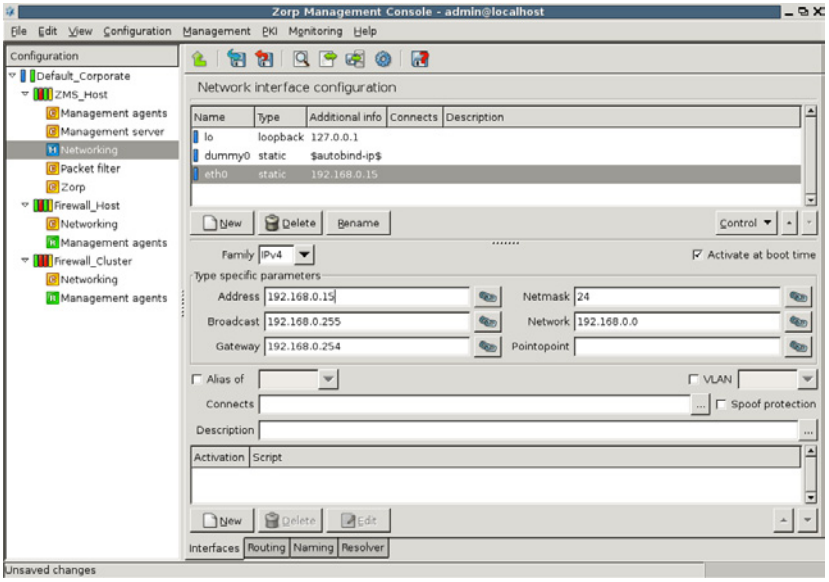
A menedzsment rendszer működése

Az adminisztrátor a grafikus kezelőfelület (Zorp Management Console, ZMC) segítségével szerkeszti a ZMS szerveren tárolt konfigurációs állományokat. A rendszerhez tartozó összes gép (Zorp, ZAS, ZCV) konfigurációját a ZMS XML adatbázisa tárolja. Az adminisztrátor a konfiguráció módosítása után elmenti a változtatásokat a ZMS-be. Az elkészített konfigurációból a ZMS generálja le az egyes eszközök számára megfelelő formátumú konfigurációs állományokat, majd ezeket letölti a megfelelő eszközre (tűzfal, tartalomszűrő, stb.). Az eszközök csak a ZMS-sel kommunikálnak, közvetlenül nem érhetőek el a kezelőfelületről.



A grafikus kezelőfelület

A Zorp Management Console (ZMC) egy grafikus kezelőfelület a ZMS és az általa menedzselt eszközök adminisztrálásához. Segítségével könnyen elvégezhető minden beállítás – még Linux tűzfalak karbantartásában járatlanok által is.



Multisite menedzsment

A rendszer segítségével a Zorp eszközök több, akár egymástól teljesen különböző csoportja is adminisztrálható. Így a különböző telephelyeken, vagy akár különböző cégekhez tartozó eszközök egyetlen közös felületről menedzselhetők.

Monitorozás

A Zorp tűzfal komponensek felügyelete könnyen megoldható külső rendszerfelügyeleti eszközök segítségével, melyek igény esetén ellátják a jelentés-készítési és szolgáltatás-felügyeleti funkciókat is.

Támogatott platformok – ZMS és ZMC

A ZMS telepíthető egy Zorpot futtató gépre is, de – különösen több eszköz használata esetén – ajánlott a szerepeket szétválasztani, és egy, a feladatra dedikált gépet használni.

A ZMC grafikus kezelőfelület az alábbi operációs rendszereken érhető el:

- Microsoft Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7
- GNU/Linux (Ubuntu 10.04 (Lucid))

Tudjon meg többet

- A Zorp honlapja: https://www.balasys.hu/hu/zorp-gateway.html
- Demóverzió igénylése: https://www.balasys.hu/hu/forms/kapcsolat.html
- Visszahívás kérése: https://www.balasys.hu/hu/forms/arajanlat.html

Tartalomjegyzék