clavister WhitePaper

Clavister DoS och DDoS skydd

Hur man skyddar sig mot DoS och DDoS attacker med hjälp av Clavister

Översikt

Denial of Service (DoS) attack är, precis som namnet antyder, en form av attack som ämnar begränsa eller helt och hållet förhindra åtkomst till en tjänst. Många känner igen förkortningen DoS eller DDoS från att tillgången till en hemsida begränsats men området är mycket bredare än så. DoS och DDoS omfattar även attacker som stör hela verksamheten och kostar stora summor pengar i förlorade inkomster och produktivitet.

Att bli utsatt för en attack riktat mot sin infrastruktur, DoS eller DDoS, kan nu anses tillhöra vardagen.

I takt med att attack-verktyg blir allt mer lättillgängliga och enkla att använda ökar antalet organisationer som blir utsatta.

Samtidigt som det blir enklare att skapa dessa attacker så har verktygen också blivit mer avancerade och kan skapa och använda sig av stora nätverk av infekterade datorer i en koordinerad attack (Distributed Denial of Services - DDoS). Infekterade system, ofta hemdatorer, används för att utfärda attacker och kontrolleras från en central punkt. Denna form av attack är oftast svårare att skydda sig mot och leder till mer kännbara konsekvenser.

I detta dokument reder vi ut begreppen kring dessa attacker och förklarar hur olika tekniker används, vilka sårbarheter som oftast utnyttjas och hur man kan skydda sig på ett effektivt sätt.

DoS och DDoS är ett problem som växer exponentiellt

För att se hur hotbilden med DoS/DDoS attacker förändras bör man titta på två viktiga faktorer, nämligen antalet attacker samt hur pass komplexa/omfattande dessa attacker är. Antal och komplexitet motsvarar sannolikheten att man drabbas samt hur pass allvarliga konsekvenserna blir av en attack. Om båda faktorer ökar så växer problemet exponentiellt.

Flertalet studier visar på en markant ökning i både frekvens och kapacitet och indikerar en ökning under kvartal 4 - 2013 motsvarande 18 % i antal attacker och en tillväxt av antal paket-per-sekund med 87 %.

Det exponentiellt växande problemet med DoS och DDoS attacker aktualiserar behovet av en genomtänkt strategi för hur man bemöter och hanterar den krissituation som uppstår om, eller när, man utsätts för en attack.

Tillfället gör tjuven - Ett uttryck som gör gällande för DoS och DDoS attacker?

DoS och DDoS attacker har existerat nästan lika länge som Internet, men varit ett begränsat fenomen eftersom det tidigare krävts specialkunskaper för att utföra en framgångsrik attack.

En bidragande orsak till den dramatiska ökningen av antalet attacker är att verktyg för att skapa Denial of Service (DoS) attacker har blivit mer tillgängliga och enkla att använda, även för de som inte besitter specialkunskaper.

Orsaken till ökat antal paket per sekund beror på flera faktorer som till exempel att internetkapaciteten hos de som skapar attackerna har ökat men också att verktygen för skapa koordinerade attacker blivit mer tillgängliga. I dag går det till och med köpa hela nätverk med redan infekterade maskiner (bot-nets) som står redo att användas i en koordinerad attack. Dessa kan hyras per timme och betalas enkelt med ett vanligt kreditkort.

Till skillnad från många andra typer av attacker som i allt större grad drivs av organiserad brottslighet och med finansiella intressen så är DoS och DDoS attacker oftare ett uttryck av missnöje och en form av vedergällning.

Organiserad brottslighet med finansiella intressen existerar dock inom området kring DoS/DDoS attacker men då oftast som den part som tillhandahåller (mot ersättning) infrastruktur som möjliggör snabbare och mer storskaliga attacker. Denna typ av infrastruktur som ofta omnämns som Bot-Nets består av ett större antal datorer som infekterats med trojaner. De maskiner som infekterats. även kallade Zombies, är ofta opåverkade och omedvetna om detta tills den dag infrastrukturen hyrts ut till en gärningsman som aktiverar dem vid attacktillfället.

Den organiserade brottsligheten har ett ekonomiskt intresse i att infektera stora mängder datorer men också att göra attackverktyg så sofistikerade och tillgängliga som möjligt eftersom fler attacker leder till mer inkomster.

Allt detta sammantaget innebär att personer som är missnöjda med en åsikt eller hur ett företag agerat mot dem kan enklare och snabbare “ge igen”. Med andra ord är det lättare att agera påverkad av stundens hetta, eller som man också skulle kunna säga: Tillfället gör tjuven.

Olika typer av DoS och DDoS attacker

För att effektivt skydda sig måste man också förstå hur en attack är uppbyggd och vilka system som oftast attackeras samt hur attackerna går till. Problematiken kring DoS och DDoS attacker gör det också nödvändigt att förstå hur infrastrukturen kan påverkas vilka nätverkskomponenter som utgör den svagaste punkten och som kommer att drabbas vid en attack.

Inom området DoS och DDoS brukar man dela in attackerna i ett antal olika grupper (se lista “Grupper av DoS och DDoS attacker” nedan).

Respektive typ av attack har olika mönster och måste bekämpas på olika sätt för att ge ett gott skydd och minska konsekvenserna.

Gruppering och klassificering av vanligt förekommande varianter av DoS och DDoS attacker

- attacker som överbelastar Internet-förbindelsen
- attacker som överbelastar svaga punkter i nätverksinfrastrukturen
- attacker som riktas mot enskilda datorer eller applikationer
- attacker som använder (tcp/ip) protokollen på ett felaktigt sätt
- överbelastningsattacker med legitim trafik
- attacker som utför ej legitima operationer i applikationer men som blandas med legitima operationer och därför är svåra att upptäcka och/eller detektera.

Överbelastning av internet-förbindelsen

Attacker där mängden data överskrider kapaciteten på offrets Internet-förbindelse eller nätverksutrustning skapar ofta förödande konsekvenser där varken kunder eller externa användare har åtkomst till organisationens olika system. Det skapar även problem för interna användare som inte kan nyttja system som ligger utanför det interna nätverket.

För att generera tillräckligt med trafik och uppnå en överbelastning av Internet-förbindelsen krävs det som regel en större mängd datorer som koordineras. Beroende på Intenet-förbindelsens kapacitet handlar det om från 500 datorer med upp till > 25,000 datorer. Denna typ av attack är väldigt enkla att utföra om den som utför attacken har tillgång till ett så kallat BOT-nät.

Även om denna typ av attack blir mindre vanlig så finns det goda skäl att se över sin strategi för att undvika ett fullständigt driftstopp i alla delar av nätet om man blir utsatt.

Attacker från större eller mindre BOT-nät har på senare tid ersatts av attacker från BOT-nät med färre anslutna men mer kraftfulla datorer. Ur en attackerares perspektiv kan det vara att föredra speciellt för attacker av mer komplicerad art.

Överbelastning av svaga punkter i nätverksinfrastrukturen

Många organisationer använder, av praktiska och säkerhetsmässiga skäl, den centrala brandväggen också som central router för det interna nätverket. I en sådan arkitektur bör man se över de potentiella svagheter och hur en överbelastningsattack kan påverka hela nätverket och alla dess användare.

I ett scenario där en felaktigt dimensionerad brandvägg överbelastas av en DDoS attack från Internet blir konsekvensen att även trafik på det interna nätverket påverkas. Några exempel på hur en sådan situation yttrar sig inkluderar bland annat följande:

- VPN-anslutningar kopplas ner
- IP baserade telefonsamtal (VoIP) får dålig kvalitet eller kopplas ned
- Interna file shares blir långsamma eller omöjliga att använda
- Interna applikationer och tjänster blir långsamma eller upphör fungera
- Externa tjänster blir långsamma eller inte tillgänglig från det interna nätverket
- Tillgång till email blir extremt långsamt eller upphör helt och hållet
- Backup och loggdata som skickas mellan olika segment i brandväggen blir långsamma eller upphör fungera.

Brandväggar har oftast dimensionerats för en legitim trafik av viss typ. Men i takt med att nya tjänster har tagits i bruk, mer funktionalitet aktiverats och nätverkets kapacitet ökat har förutsättningarna ändrats. Om det dessutom förekommer överbelastningsattacker eller felaktigt användande av applikationer så kommer man snart att erfara kapacitetsproblem.

Är UTM och NGFW brandväggar mer sårbara för DoS attacker?

Många organisationer väljer att uppgradera mjukvaran på befintlig hårdvara och komplettera med UTM och NGFW funktioner. Application Control, IPS och liknande ger ett bra skydd men uppgradering och aktivering av ny funktionalitet måste ske på ett kontrollerat och genomtänkt sätt.

När mer funktionalitet aktiveras på en brandvägg måste man säkerställa att kapaciteten fortfarande överstiger den som kan genereras vid en DDoS attack samtidigt som det interna nätverket fortsätter att fungera opåverkat.

Många UTM och NGFW produkter har utformats kring relativt gammalmodig teknik där applikationsigenkänning sker med hjälp av en IPS motor med hundratusentals applikationssignaturer. Denna teknik resulterar inte bara i hög felmarginal utan också i en kraftig prestandaförsämring. Vissa leverantörer har en prestandaförsämring med upp till 80 % när denna funktionalitet aktiverats. En prestandaförsämring med 80 % på brandväggen leder sannolikt till att hela nätverket och alla användare påverkas under en attack.

Brandväggen är oftast inte målet eller angreppspunkten men kan på grund av bristfällig dimensionering och prestanda vara den svaga länken som gör att konsekvenserna blir större än vad den som utfört attacken hade hoppats på.

Attacker som riktas mot enskilda datorer eller applikationer

I stället för att överbelasta hela Internet-förbindelsen så kan även den som vill utföra en attack utnyttja sårbarheter i utvalda system och åstadkomma en överbelastning och störa viktiga tjänster med relativt lite trafik.

Sårbarheter i system kan vara allt från en bugg i programkoden i den applikation som används för att leverera en tjänst men kan också vara så enkelt som en websida som kräver relativt mycket processorkraft för att genereras.

Den mest klassiska formen av attack som riktas mot enskilda applikationer bygger på att många (små) http förfrågningar sker till adresser på en webbserver som innehåller stora filer eller bilder. Några få megabyte i förfrågningar från klienten kommer att resultera i att webbservern svarar med flera gigabyte data och riskerar att överbelasta både server och Internet-förbindelse.

Ett klassiskt sådant exempel är att hitta en bild på en WEB-server, som är dynamisk, d.v.s. som inte kan lagras i en cache. Om en illvillig person länkar en sådan bild till ett facebook meddelande och lyckas dela den bilden eller inlägget med 25,000 personer så kommer troligen belastningen på den server som håller bilden att snabbt överbelastas. I det fallet är all trafik legitim ur en brandväggs perspektiv men ohanterlig ur ett prestandaperspektiv.

Utnyttjande av sårbarheter i applikationer

Att utnyttja sårbarheter (buggar) i applikationer kan vara potentiellt mer förödande men kräver oftast mycket högre kompetens. Om applikationerna rättas (patchas) regelbundet och skyddas av till exempel IPS system så kan det många gånger krävas att man specialskriver en attack och utnyttjar okända sårbarheter. Detta kan vara ett väldigt tidsödande arbete.

Om gärningsmannen är framgångsrik med en attack av denna kategori kan det i värsta fall ge honom/henne fullständig åtkomst till hela systemet och leda till en totalt havererad miljö, förlorad och/eller förstörd information.

Utöver kännbara konsekvenser av en sådan attack blir också arbetet med att återställa driften väldigt tidskrävande och komplicerat.

Utnyttjande av svagheter i applikationer

Ett enkelt sätt att störa driften på till exempel en webbserver eller en affärsapplikation och som dessutom inte kräver särskilt mycket trafik är att rikta attacken mot sidor och funktioner som kräver mer processor tid. Teorin är ganska enkel, för varje förfrågan som ställs mot en server vill man åstadkomma maximalt nyttjande av hårdvaruresurser för att snabbare åstadkomma en överbelastning.

Vanliga exempel på sårbara sidor eller funktioner är de som innehåller stora bilder eller använder sig av komplexa och omfattande SQL uttryck.

Om den som utför attacken kan identifiera de sidor eller funktioner som resulterar i stora datamängder i svar eller som kräver längre tid (mer processorkraft) för att genereras så kan en överbelastning genomföras med betydligt mindre insats.

I stället för att behöva få tillgång till hundratals eller tusentals med infekterade datorer (zombies) så kan samma skada åstadkommas med ett fåtal datorer som skickar rätt typ av trafik och förfrågningar.

För att skydda sig mot den typen av attacker krävs det att den som har konstruerat programmet som hanterar data har inbyggda skydd för att begränsa datamängder och/eller tiden en förfrågan får använda systemresurserna. Man kan till exempel tänka sig ett register över Sveriges samtliga telefonabonnenter. I gränssnittet för att söka bör man lägga till ett par begränsningar som till exempel:

- mängden svar som returneras för inte överstiga 100 poster
- söksträngen måste innehålla minst 5 tecken
- söksträngen måste innehålla minst en bokstav
- Captcha's skall matas in om det sker mer än 1 sökning per sekund från samma IP adress

Genom att konstruera gränssnittet och införa kontroller så nära användaren som möjligt kan överbelastningsproblem, avsiktliga eller oavsiktliga, undvikas.

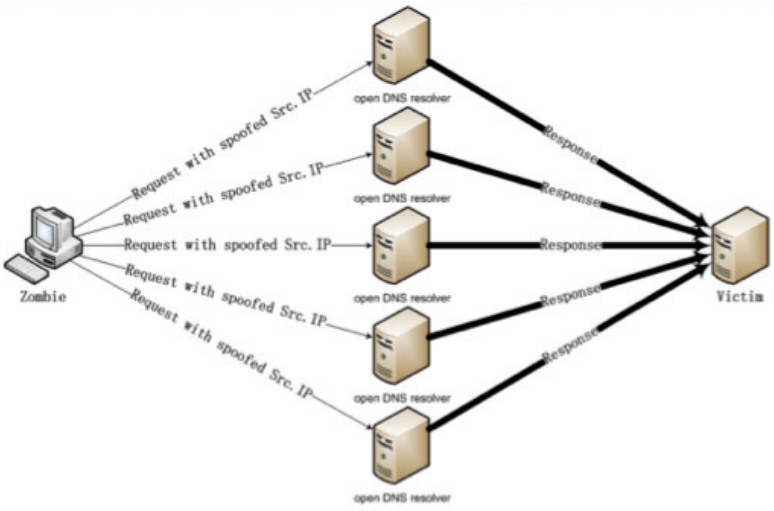
Ett annat exempel på svagheter i applikationer som kan utnyttjas är till exempel FTP applikationer där det i en session ingår flera olika typer av signaleringspaket som infrastrukturen förväntar sig i en speciell ordning. Om denna ordning bryts och paket som inte tillhör någon existerande session dyker upp så kan den enhet som får paketet hantera det på olika sätt, beroende på implementation. Det korrekta sättet att hantera detta på, ur ett DDoS perspektiv är att kasta paketet. Men ur ett applikationsperspektiv kan det vara mer rätt att försöka återupprätta sessionen eller att skicka ett felmeddelande till avsändaren. Den typen av operation förbrukar resurser och tid vilket snabbare leder till en överbelastning.

Reflektionsattacker

Reflektionsattacker använder en teknik som innebär att gärningsmannen attackerar offret genom att nyttja en mellanhand. Principen bakom reflektionsattacker bygger på att gärningsmannen skickar en falsk förfrågan till mellanhanden där frågan ser ut att komma från det egentliga offret. Svarsmeddelanden från mellanhanden som därmed riktas till det verkliga offret är den trafik som utgör själva attacken.

Denna teknik försvårar avsevärt arbetet med att spåra gärningsmannen och häva attacken.

Ett klassiskt exempel på en reflektionsattack är att gärningsmannen skickar en mängd A record förfrågningar till legitima DNS (Doman Name Server) system. Förfrågningarna är förfalskade för att se ut att komma från det primära offret. När de legitima DNS servrarna svarar på förfrågningarna så adresseras denna trafik till offret (denna trafik omnämns ofta som åter-spridning - eng. backscatter).



Figur 1: Reflektionsattack

Reflektionsattacker är mest framgångsrika om de kombineras med olika tekniker där svarsmeddelandet är större än förfrågan vilket ofta är fallet gällande DNS förfrågningar till poster av typen TXT. Med andra ord kan en enkel förfrågan till en mellanhand resultera i ett större svarsmeddelande till det verkliga målet samtidigt som det är svårt att spåra vem som verkligen ligger bakom själva attacken.

Hur man bygger ett robust nätverk och skyddar sig mot DoS och DDoS attacker

Det finns ingen mirakellösning för att skydda sig mot DoS och DDoS attack. Eftersom det finns flera olika typer av attacker så finns det också flera olika sätt att skydda sig mot dessa. Med en väl genomarbetad plan, korrekt dimensionerat nätverk och brandväggar och med särskild funktionalitet för området kan man uppnå ett gott skydd.

Eftersom DoS och DDoS attacker kan se väldigt olika ut så krävs en kombination av olika funktioner för att ge ett bra skydd. Tabellen nedan ger en översikt av vilka tekniker som lämpar sig väl för respektive kategori av attack.

	IPS	AC	Rate Limiting	Traffic Shapin	SLB	RLB	Cloud och CDN	Capacity Planning	Multi Layer FW
Överbelastning av Internetlänk						X	X		
Blockerad/Begränsad tillgänglighet till interna system för externa användare/kunder				X					
Blockering/begränsning av både inkommande och utgående trafik för anställda/ användare				X		X			
Överbelastning av nätverksutrustning									
orsakat av hög volym paket			X	X				X	X
orsakat av hög volym sessioner			X		X			X	X
Tjänstespecifika attacker									
Överbelastning orsakat genom:									
...nedladdning av stora filer		X	X	X	X		X		
...utnyttjande av CPU- intensiva resurser/funktioner		X	X	X	X		X		
...hög volym korrekt trafik			X	X	X		X		
...högt antal inloggningar via SSL-krypterade förbindelser		X	X		X				
Havererad tjänst genom utnyttjande av sårbarheter i applikationer (hacked/crashed)	X	X							
Reflektionsattacker (DNS)		X	X	X	X		X		

Nätverksdesign

Korrekt dimensionerad central brandvägg

Det är av yttersta vikt att man har en korrekt dimensionerad brandvägg i de fall man avser använda samma enhet för att hantera såväl publika som interna tjänster. En korrekt dimensionering av brandväggar och övrig utrustning måste utgå i från den totala kapaciteten man förväntas exponera brandväggen för. Detta innebär att man måste studera den aggregerade kapaciteten för trafik i båda riktningar för samtliga nät som kopplas mot brandväggen och göra en bedömning av hur trafik i såväl normal-scenario som worst-case scenario ser ut.

Vidare så måste samtliga funktioner som har slagits på i brandväggen ha tillräckligt med systemresurser för att kunna användas i den planerade omfattningen. Funktioner som ofta kräver mycket CPU-kapacitet är de som kräver en mer ingående analys eller kryptering/dekryptering. Exempel på sådan funktionalitet inkluderar:

- Etablering av SSL-sessioner med långa krypteringsnycklar
- Inspektion av SSL-trafik som innefattar både dekryptering och återkryptering
- Application Control
- AntiVirus
- IPS

Även strukturen i routing kan orsaka problem. I det fall man till exempel har 1-Gbps interface och har trafiken styrd på ett sätt att all trafik måste passera brandväggen flera gånger så måste också brandväggen vara dimensionera för att kunna hantera den aggregerade trafiken. Det är inte ovanligt att trafiken behöver passera brandväggen upp till 6 gånger innan paketen har returnerats till avsändaren.

Då många tillverkare av nätverksutrustning enbart tillhandahåller kapacitetssiffror för så kallad plaintext trafik och med endast enklare brandväggsfunktionalitet aktiverat är det viktigt att man studerar hur enheten påverkas om man avser använda tjänster som till exempel UTM och NGFW funktionalitet. Vissa produkter får en prestandaförsämring motsvarande 80 % vilket innebär att även relativt lite trafik vid en DoS eller DDoS attack kan överbelasta nätverksenheterna. Överbelastning av en sådan centralt placerad enhet leder till generellt dåliga svarstider i hela nätverket och därmed samtliga tjänster där trafiken passerar genom brandväggen.

Utöver kapacitet i form av bandbredd är det även viktigt att säkerställa att brandväggar och andra enheter kan hantera tillräckligt många nya förbindelser per sekund, antal paket per sekund samt totalt antal samtidiga förbindelser.

Till skillnad från Clavister så är de flesta brandväggar designade på ett sätt som innebär att när maximalt antal förbindelser uppnåtts så blockeras all ny trafik tills dess att gamla förbindelser nått dess time-out värde. Denna svaghet finns i de flesta brandväggar på marknaden och resulterar i att det tar flera minuter, eller i värsta fall timmar, innan riktig trafik får möjlighet att passera genom brandväggen.

Segmenterat nätverk med olika brandväggar för publika och interna tjänster

Genom att segmentera nätverket och isolera system och funktioner som är publikt tillgängliga och exponerade för attacker från interna och semi-publika system begränsas konsekvenserna vid en DoS/DDoS attack.

I stället för att både det interna nätet och de publika tjänsterna påverkas vid en attack kan man separera dessa och bibehålla service från de interna funktionerna i full eller begränsad skala trots att det pågår en attack mot publika system.

Speciellt i konfigurationer där tcp/ip-baserade protokoll för lagringshantering används (till exempel NFS) är det viktigt att göra en segmentering av trafiken så att en DDoS attack inte dessutom slår ut lagringssystemen.

Med denna design av nätverket blir också kapacitetsplanering av brandväggar och andra nätverksenheter enklare.

Denna metod är att rekommendera för större och mer komplexa nätverk där många faktorer kan spela in och det är svårare att förutse konsekvenser vid en attack.

Kostnad och administrativ komplexitet är nackdelar eftersom det krävs dubbla lager av brandväggar och övrig nätverksutrustning. Dessa nackdelar kan dock begränsas eftersom kapacitet för Internet-förbindelser och publika system oftast är relativt låga och därmed inte kräver lika kostsam utrustning som till de interna systemen.

Med andra ord kan man dimensionera respektive nätverk mer noggrant med något mindre över-kapacitet än vad man bör beräkna om endast ett lager av brandväggar används. Beroende på nätverkets storlek kan denna metod faktiskt bli billigare eftersom kostnad för high-end utrustning med extrem kapacitet är dyr relativt till kostnad/megabit.

Segmenterat nätverk och molntjänster

Molntjänster och så kallade Content-Delivery-Networks (CDN) kan med fördel användas för att sprida olika affärskritiska system över flera segment och därmed undvika att en attack kan riktas mot en enskild punkt och därmed förlama hela verksamheten.

Molntjänster har också fördelen att de oftast är väldigt skalbara och gör det möjligt att temporärt öka kapacitet för kritiska tjänster och därmed kompensera för det ökade kapacitetsbehovet som uppstår vid en DoS/DDoS attack.

Clavister tillhandahåller virtuella brandväggar vilket gör det möjligt att applicera samma typ av brandväggsteknik oavsett om miljön som skall skyddas finns i det egna fysiska nätverket, det interna virtualiserade datacentret eller t.o.m. i molnet. Då Clavisters samtliga plattformar (fysiska som virtuella) använder samma grundkärna och kan administreras med samma centrala administrationsverktyg blir det enkelt att dra nytta av redan existerande kompetens.

Funktioner som motverkar eller hjälper vid DoS och DDoS attacker

Begränsning av antal förbindelser

Threshold Rules - Rate Limiting är en funktion i Clavisters produkter som gör det möjligt att sätta gränsvärden för vad som är ett normal och icke normalt beteende gällande hur förbindelser skapas mot bakomliggande system, totalt eller under en viss tidsperiod. Genom att aktivera Rate Limiting begränsas möjligheten för enskilda användare att skapa en överbelastning av de system som skyddas av en Clavister brandvägg.

Detta är ett av de mest effektiva sätten att undvika och försvåra attacker som bygger på att många förbindelser skapas på kort tid och utnyttjar eventuella svagheter där etablering av nya förbindelser är den svaga länken.

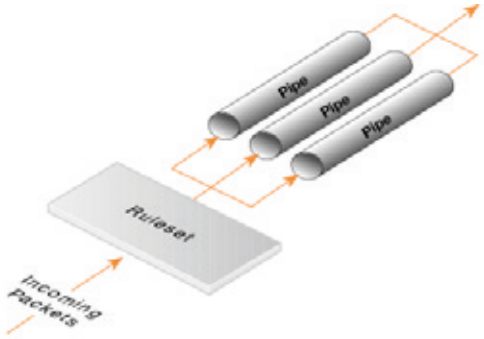
Intrångsskydd (IPS)

Intrusion Prevention Systemet i Clavisters produkter kan identifiera både kända och okända attacker genom att kombinera flera olika tekniker, däribland signaturer som ämnar skydda sårbarheter oavsett hur en attack designats för att utnyttja dem. När en attack eller försök att utnyttja en sårbarhet i bakomliggande system så kan man välja att endera stoppa förbindelsen, enbart logga den eller att till och med begränsa framtida förbindelser från den som försöker skapa intrånget i bakomliggande system.

Bandbreddskontroll

Traffic Shaping, eller bandbreddsbegränsning, är ett av de mest effektiva sätten att begränsa överbelastnings attacker. Genom att konfigurera denna funktion i Clavisters produkter kan man säkerställa att ingen enskild användare får obegränsad kapacitet till bakomliggande system. Genom att aktivera regler som fördelar kapaciteten på ett förbestämt och hälsosamt sätt försvårar man en attack.

Med Clavisters produkter går det även att kombinera Traffic Shaping med Intrångsskyddet (IPS) vilket gör det möjligt att begränsa specifika användare som har ett beteende som avviker från det normala. På så vis är det lättare att tillhandahålla en bra service till riktiga kunder och begränsa tillgängligheten för skadlig trafik. Många gånger är det bättre att "lura" gärningsmannen att attacken fungerar genom att enbart begränsa tillgängligheten i stället för att helt blockera den.



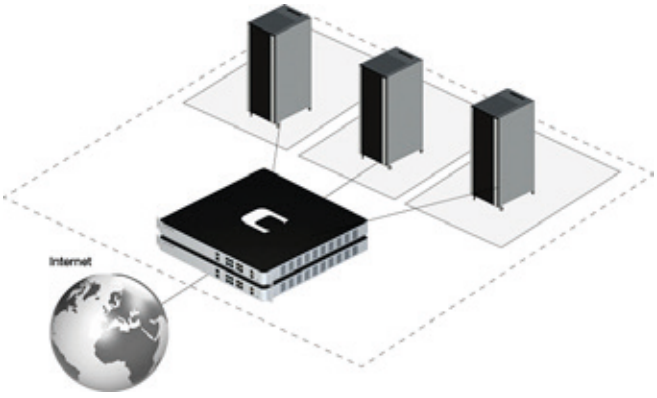
Figur 2: Bandbreddskontroll

Lastbalansering av servertjänster (SLB)

Som namnet antyder används denna funktion för att sprida last eller trafik över flera servrar. Genom att använda denna funktion ökas kapaciteten för tjänsten och de känsliga och affärskritiska systemen på ett mycket skalbart sätt.

I stället för en begränsning motsvarande den kapacitet som en enskild server tillhandahåller kan man med hjälp av SLB sprida trafiken över flera servrar med identiskt innehåll, en så kallad serverfarm.

Clavisters produkter övervakar kontinuerlig tillgängligheten och svarstider för alla maskiner som ingår i server-farmen och kan automatiskt omfördela spridningen till de servrar som är tillgängliga för tillfället. Denna funktionalitet ger en rad administrativa fördelar även i normalläget då enskilda servrar kan genomgå underhåll och tas ur drift utan att tjänsterna slutar att vara tillgängliga.



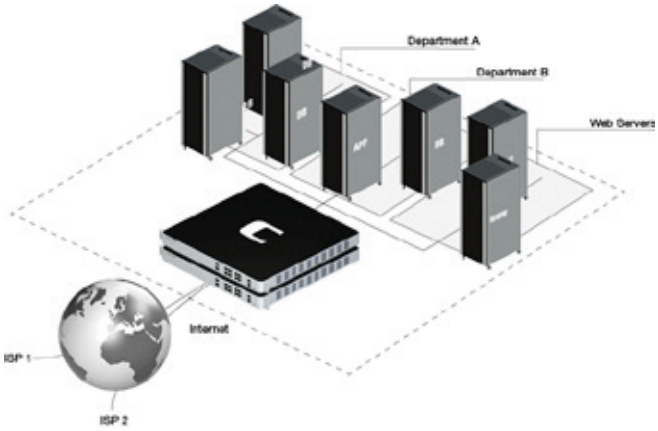
Figur 3: Lastbalansering av servertjänster

Lastbalansering - Redundanta Internetanslutningar

Genom att samtidigt använda flera Internet-förbindelser i kombination med Clavisters Route Load Balancing funktion an man säkerställa att interna användare får tillgång till Internet och de tjänster som finns utanför organisationen även under en period när den som utför attacken fyller kapaciteten på den primära Internet-förbindelsen.

I stället för en helt paralyserad organisation så kan kritiska tjänster fortfarande vara tillgängliga för användarna medans administratörer i lugn och ro kan hantera den pågående attacken på ett genomtänkt och effektivt sätt.

Clavisters funktionalitet för att distribuera trafik över flera parallella länkar kan konfigureras på flera olika sätt för att passa den aktuella situationen bäst. Trafik kan distribueras över de sekundära länkarna enligt en definerad fördelning även under normaldrift alternativt bara vid avbrott eller dålig svarstid på den primära länken.



Figur 4: Lastbalansering - Redundanta Internetanslutningar

Aktiv redundans - Lastbalansering

Denna metod innebär att trafik fördelas över samtliga Internet-förbindelser även vid normaldrift och resulterar därmed i ökad kapacitet och förbättrade svarstider. Detta är bra lösning när de sekundära länkarna har obegränsad datamängd och relativt bra kapacitet i förhållande till den primära länken.

Passiv redundans - Failover

Denna metod innebär att trafik bara skickas över de sekundära länkarna om det uppstår ett problem med den primära uppkopplingen. Detta är en önskvärd lösning när de sekundära länkarna har en begränsning i total datamängd per månad (Till exempel 3G/4G-LTE abonnemang).

Länkövervakning

Utöver själva funktionen för att distribuera kapacitet över flera länkar har Clavister även funktioner för att övervaka respektive länk och rapportera status till det system som sköter själva policy-besluten för hur trafiken skall fördelas. Med Clavisters länkövervakning (Route Monitor) kan både pingsvar, fördröjning (latency) och resultat från applikationsförfrågningar utvärderas och användas för policy beslut som avgör hur trafiken fördelas.

Utöver det skydd som Clavisters funktionalitet för trafkfördelning över multipla Internet-förbindelser ger så det även erbjuda organisationen en rad fördelar under normal drift vilket skapar nöjdare användare och rent generellt ett mer robust nätverk.

Applikationskontroll

Applikationskontroll är en funktionalitet i Clavisters produkter som identifierar och kontrollerar trafik baserat på vilken typ av applikation som används oavsett vilken port eller nätverksprotokoll som används.

Med hjälp av Application Control kan man undvika att den som utför attacken skickar skadlig trafik till de interna systemen och försöker lura säkerhetssystemen genom att härma normal trafik.

Application Control kan även användas för att till exempel ställa krav på vilken webbläsare och version som används vid anslutning mot vissa tjänster och försvårar därmed för användandet av DoS-verktyg. Givetvis kan verktyg anpassas för att skapa korrekt trafik men det är oftast en komplicerad övning och något som kräver specialistkompetens.

Figur 5: Clavister Web Management

Protokollvalidering

Protokollvalidering används för att säkerställa att trafik som tillåts genom brandväggen verkligen följer de definierade standarder som gäller för respektive protokoll. Typiska kontroller som sker genom protokollvalidering inkluderar att rätt sekvensnummer används på paket, att rätt flaggor satts och att sessioner etableras på ett korrekt sätt. Eftersom många attack-verktyg bygger på inspelad trafik där sekvensnummer inte är giltiga eller innehåller information som försöker nyttja svagheter i IP protokoll så är denna funktionalitet mycket användbar mot enklare attacker.

Protokollvalidering tvingar varje maskin som används för att attackera nätverket att etablera samtliga förbindelser på ett korrekt sätt. Därmed minskar kapaciteten som kan skickas från respektive maskin i en koordinerad attack vilket innebär att en attack inte får samma grad av påverkan på tillgänglighet alternativt att det krävs många fler maskiner i den koordinerade attacken.

Övervakning

En grundläggande princip är att man ska övervaka all utrustning och alla tjänster i nätverket. En av orsakerna till en så grundläggande övervakning är att man skall få en bra och övergripande kunskap om normalläget för att därmed göra det lättare att upptäcka avvikelser. Olika verktyg kan sedan användas för att visualisera avvikelser eller för att skicka larm om avvikelser. Vissa saker kan automatiseras medan andra mer effektivt hanteras manuellt. Det finns många olika verktyg för att övervaka nätverksutrustning. För övervakning och larmhantering av Clavisters produkter rekommenderar vi följande system:

- **Clavister InControl**
  Centralt administrationssystem för Clavisters produkter. Innehåller funktioner för både administration, övervakning och logganalys. Clavister InControl som hanterar hundratals brandväggar och samtidiga administratörer är Inkluderat i underhållsavtalet till brandväggsprodukterna och kräver ingen ytterligare licensavgift.
- **Multi Router Traffic Grapher - MRTG**
  Ett välkänt gratisverktyg för att via SNMP övervaka trafiklast på många routrar, brandväggar och dylikt. MRTG är ett verktyg som ger en bra översikt över trafiksituationen i hela nätverket och därmed gör det enklare att upptäcka om det finns ett problem och vart i nätverket det i så fall befinner sig.
- **OSsec**
  Ett välkänt gratisverktyg som kan användas för att analysera logdata från många olika källor, bland annat brandväggar, VPN utrustning, operativsystem och liknande. OSsec kan med fördel användas för att identifiera potentiella intrång genom att korrelera loggdata från olika system och skapa alarm när ett visst mönster identifierats.

Mängden av nätverksmonitoreringsverktyg på marknaden är stort. Nagios, OP5, HP Openview, IBM Tivoli, Solarwind, PRTG, Splunk, Cacti och Spiceworks är några.

Vid attacker mot nätverksinfrastrukturen är det ofta flera olika komponenter som blir drabbade. Det kan vara svårt att se sammanhangen om det uppstår ett larm på en enskild komponent. För att lättare finna nålen i en gigantisk höstack kan man använda sig av logkorrelering vilket är en nyckelkomponent för effektiv övervakning och felavhjälpning.

Beredskapsplan och Övning

Ingen säkerhetslösning är 100% perfekt och även om det fanns en sådan lösning kan fortfarande Internet-förbindelsen överbelastas.

För att man snabbt och effektivt ska kunna häva en attack och begränsa skadan bör man utforma en beredskapsplan. En bra beredskapsplan bör inkludera vem som ansvarar för arbetet, hur man identifierar vilken typ av attack man utsätts för, beskrivning på hur attacken påverkar organisationen samt hur man agerar på kort, mellan och lång sikt för att häva attacken.

En effektiv plan bör innehålla detaljerade beskrivningar för hur man agerar och bör därför uppdateras minst var tredje månad för att motsvara den aktuella miljön.

Många administratörer undviker att öva i produktionsmiljö vilket är fullt förståeligt med tanke på de potentiella störningar det kan ha på verksamheten. Faktum är dock att en begränsad övning i produktionsnätet som innebär någon eller ett fåtal timmars störning kan undvika katastrofer i framtiden.

Vissa typer av attacker är svåra att simulera utan specialverktyg som till exempel trafik-generatorer.

Det är dock möjligt att simulera dessa situationer i begränsad omfattning genom att analysera beteendet vid lägre last. Exempelvis kan man validera att Traffic Shaping regler fungerar som de skall genom att sänka tröskelvärden till den nivå man klarar av att simulera utan kostsamma specialprodukter.

Känner man sig tveksam över hur gott skydd man har bör man kontakta specialister som kan genomföra ett penetrationstest med särskild inriktning på överbelastningsattacker.

Rekommendationer

Eftersom DoS och DDoS attacker är ett brett begrepp är det svårt att göra korta och enkla rekommendationer utan att vara allt för generell. Ett bra skydd mot DoS och DDoS attacker måste skräddarsys för att passa varje enskild organisation och nätverk på ett optimalt sätt men det finns ändå några övergripande principer att ta fasta på som hjälper oavsett vilken miljö och situation det gäller.

- **Analys & kartläggning**

  Analysera din miljö och kartlägg vilka tjänster som exponeras publikt och internt och hur de påverkar varandra. Sitter båda nätverken kopplade mot samma infrastrukturutrustning som till exempel brandväggar, mm.
- **Handlingsplan**

  Upprätta en tydlig handlingsplan där det framgår vem som ansvarar för vad och vem som fattar beslut vid en krissituation.
- **Dokumentera**

  Beskriv var systemdokumentation förvaras, var säkerhetsbackuper finns samt hur återställning av drabbade komponenter görs.
- **Övervakning**

  Övervaka samtliga tjänster och lägg extra stor vikt vid att övervaka alla tjänster som är publika och kan uppfattas som måltavla för upprörda användare, kunder eller andra målgrupper som utgör hotbilden
- **Redundans**

  Ett robust nätverk med redundans hjälper vid en attack men bidrar också till ett mer effektivt nätverk under normaldrift. Detta gäller såväl Internetuppkopplingar, server-farmar och nätverksprodukter.
- **Virtualisering och virtuella brandväggar**

  Avlasta den centrala brandväggen genom att använda en virtuell brandvägg för de mer komplexa och resurskrävande funktioner (UTM/NGFW) som används för att säkra den virtuella miljön. Var observant med hur den dynamiska resursallokeringen fungerar för dina virtuella maskiner. Konfigurera alltid min och max resurskapacitet för den virtuella maskin som den virtuella brandväggen används på.
- **Kapacitetsplanering**

  En bra grundprincip är att planera med mer överkapacitet desto mer centraliserade tjänster och komponenter blir. Om du använder ett lager av brandväggar för att hantera både interna och publika nät bör man se över vilken kapacitet dessa har när samtliga funktioner är aktiverade och jämföra det med den aggregerade kapaciteten från samtliga nät under ett worst-case scenario. Har man redan gjort en investering i central brandvägg(ar) och vill utöka sin säkerhet med UTM och NGFW funktionalitet bör man vara extra försiktig och överväga att uppgradera till en större hårdvara alternativt komplettera med ytterligare ett lager brandväggar för det publika alternativt interna nätverket.
- **Rapport & Analys**

  Använd så kallade SIEM - Security Information Event Management verktyg för att analysera information från flera olika applikationer och produkter. Genom att korrelera information från flera olika system kan en attack identifieras i ett tidigare skede. SIEM verktyg hjälper även för att i efterhand återskapa och förstå hur en attack gått till och vad som skett vilket är av stor vikt för att undvika samma problem i framtiden.
- **Prioritera rätt system och tjänster**

  Undvik att sila mygg och svälja elefanter och bestäm i ett tidigt skede vad som har prioritet och vad man bör lägga extra kraft på att säkerställa kontinuerlig drift av. Kanske är det acceptabelt att hemsidan har dålig svarstid under en period medans det är en katastrof om personalen inte kommer åt diverse produktionssystem. För andra kunder är det omvänd situation.

Summering

I takt med att antalet DoS och DDoS attacker ökar så aktualiseras behovet av ett förstärkt skydd och handlingsplan.

Konsekvenserna av bristfälligt skydd, uppföljning och handlingsplan omfattar bland annat produktionsbortfall, missnöjda medarbetare, förlorade inkomster med potentiellt förlorade kunder.

Det finns inget hundraprocentigt skydd men med enkla medel som en korrekt dimensionerad och konfigurerad brandvägg kan man avvärja de flesta attacker, särskilt attacker från de som sker av personer utan specialkompetens och enbart agerar i stundens hetta.

Clavister's produkter har ett omfattande skydd mot DoS och DDoS och kan nyttjas på befintlig brandvägg eller med ett ytterligare lager av brandväggar för publika alternativt interna tjänster. I stället för kostsamma specialprodukter för området uppnås ett gott skydd utan avsevärt ökad administration och kostnad.

Molntjänster, Content Delivery Networks och virtualisering är effektiva sätt att sprida riskerna och skapa en mer robust och tolerant miljö. Säkerheten i dessa miljöer får dock inte åsidosättas och skydd motsvarande det i fysiska nätverk bör appliceras utan kompromisser. Clavister Virtual Series är en virtuell brandvägg med samma funktionalitet som de hårdvarubaserade och kan nyttjas både i molnet och det virtuella nätverket för att skydda dessa miljöer mot DoS/DDoS attacker och andra säkerhetsproblem.

En god rekommendation är att börja enkelt och förbättra säkerhetslösningen i små steg. Saknas kompetens och erfarenhet av just området skydd mot DoS och DDoS attacker bör man ta hjälp av specialister för att bistå med råd eller t.o.m. att leverera detta skydd som en tjänst.

Kontakta Clavister

Besök Clavisters hemsida www.clavister.com för mer information, kontakta oss eller någon av våra certifierade partners för rådgivning.

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com