Project DDoS

SURFnet
1 april 2016

Document Version

Document Revisions	
Project DDoS ■ SURFnet (Draft)	0.1α (2015/12/2 JS) *(obsolete)*
Project DDoS ■ SURFnet (Draft)	0.2β (2016/2/8 JS) *(obsolete)*
Project DDoS ■ SURFnet (Draft)	0.4β (2016/2/29 JS) *(obsolete)*
Project DDoS ■ SURFnet (Draft)	0.8β (2016/3/22 JS)

Distribution List			
Name	Organisation	Function	Action Approve | Review | Read
DDoS Solutions List	SURFnet	Project Manager	Read
DDoS Solutions List	SURFnet	Project Participants	Review
DDoS Solutions List	Groningen University	Project Participants	Review
DDoS Solutions List	Universiteit Twente	Project Participants	Review

Samenvatting

Voorstel tot en beschrijving van een project om DDoS-thematiek nader te preciseren, en aan de tand te voelen binnen de context van de SURFnet-dienstverlening.

Inhoudsopgave

1 Inleiding

Netwerkdiensten spelen sinds een belangrijke rol in onderwijs en onderzoek. Gebruik en capaciteit nemen toe.

Beschikbaarheid van netwerkdiensten kan echter onder druk staan. Ook zonder functionele storingen en beheersincidenten is die beschikbaarheid echter niet in absolute zin gegarandeerd; de capaciteit van het netwerkzelf, van een specifieke koppeling daarin, of van over het netwerk benaderde diensten kan uitgeput raken.

Een DDoS-aanval maakt gebruik van de beperkte capaciteit van middelen om netwerkverkeer, of specifieke netwerkdiensten, negatief te beïnvloeden of zelfs volledig buiten werking te stellen. De behoefte om bescherming te bieden tegen dergelijke DDoS-aanvallen ontstaat daarmee.

We onderscheiden in grote lijnen twee soorten DDoS-aanvallen: volumetrische aanvallen en applicatiespecifieke.

1.1 Volumetrische DDoS

Van een volumetrische aanval is sprake als de netwerkcapaciteit zelf verzadigd wordt. Een instelling met 40Gbit SURFnet-connectiviteit heeft feitelijk geen werkende verbinding meer als een DDoS-aanval er succesvol in slaagt deze capaciteit uit te putten. Het biedt ook weinig soelaas om in te grijpen in het inkomende netwerkverkeer; ook als dat allemaal tegengehouden wordt, is de connectiviteit nog steeds uitgeput.

Capaciteit is geen ééndimensionale grootheid. De link capaciteit speelt een rol en is een plafond, maar volume ontstaat uit hoeveelheden packets. Hetzelfde volume kan zowel voortkomen uit een relatief klein aantal grotere packets, alsook uit een relatief grote hoeveelheid kleine packets. De belasting voor netwerkcomponenten kan in beide gevallen sterk verschillen, en daarmee is de ‘packet rate’ naast het ‘lump sum’ volume is ook een significante factor in het perspectief van DDoS.

1.2 Applicatiespecifieke DDoS

De capaciteit van aangesproken services is doorgaans wezenlijk lager dan die van het transporterende netwerk. Al is er relatief weinig voor nodig om extreme hoeveelheden connecties naar een server op te zetten, het afhandelen van die connecties is echter een veel zwaardere taak. Sommige ‘requests’ kunnen zelfs (relatief) zeer zwaar zijn, zodat een (relatief) beperkt aantal ervan de middelen van een server al kan uitputten. Kwetsbaarheden en overige programmeer- of ontwerpfouten in server-software kunnen hier sterk aan bijdragen.

Een netwerkdienst uitschakelen kan hierdoor plaatsvinden zonder serieus beslag te leggen op de capaciteit van het netwerk. De klasse van DDoS-aanvallen met dit karakter noemen we applicatiespecifiek.

2 Aanpakken

Het zou vanzelf moeten spreken, maar toch herhalen we het hier: een maatregel nemen heeft alleen zin als de maatregel effectief is, én als de voordelige effecten opwegen tegen de nadelige. Tot de nadelige effecten van maatregelen (in het algemeen) horen kosten in brede zin; geld speelt een rol, maar is lang niet de enige factor. De zwaarte van een maatregel dient in beide aspecten proportioneel te zijn aan de onderliggende kwestie.

DDoS kunnen we een klip en klaar risico noemen, maar dat is geen vrijbrief voor arbitrair ingrijpen. Een risico vraagt niet om een ingreep, het vraagt om een duiding, en daarmee een oordeel. Of er een, en zo ja welke, aanpak er gevolgd wordt wordt hierdoor bepaald. We vereenvoudigen het hele spectrum van mogelijke DDoS-aanpakken tot de volgende drie, een moedwillige oversimplificatie ten behoeve van de helderheid.

Niets doen is een legitieme aanpak waar onvoldoende noodzaak tot ingrijpen is.
Dat kan zo zijn als de frequentie van (verwachte) DDoS aanvallen zeer laag is, en de incidentele uitval van netwerkdiensten (of het gehele netwerk) onvoldoende zwaarwegend is om de kosten, eenmalige en structurele inspanningen en eventuele overige nadelige effecten van het nemen van DDoS-maatregelen te billijken.
In het bijzonder kan het acceptabel zijn om *reactief* te opereren, dat wil zeggen te aanvaarden dat er degeneratie of uitval van functionaliteit optreedt tussen het moment dat een DDoS-aanval begint en het moment dat er in overleg met SURFnet (tijdelijke) noodmaatregelen getroffen worden (die dan hopelijk goeddeels tot herstel leiden).

Generieke doorvoerbeperkingen in de netwerkstroom kunnen aangebracht worden aan de zijde van SURFnet, die als doel hebben om onder normale omstandigheden niet op te treden, maar DDoS-aanvallen wel sterk kunnen dempen.

Specifieke DDoS-technologie kan specifiek op de verkeersstroom van een aangesloten instituut toegepast worden. Daarmee kan organisatiespecifieke kennis van het eigen netwerk toegevoegd worden, die de DDoS-analyse (en eventuele mitigatie) wezenlijk verrijkt.
Dergelijke technologie kan in het eigen netwerk geplaatst worden, of aan de zijde van SURFnet (uitgaande van de bereidheid tot samenwerken). Bijzonder vermeldenswaardig is een *hybride* inrichting; maatregelen aan de kant van de aanbieder (SURFnet) kunnen direct voorkomen uit de analyse van verkeersstromen bij (door) een instelling zelf.

De verschillende aanpakken vergen zeker een verschillend 'commitment'. Los daarvan heeft het ook zin ze op hun merites te beoordelen. Om dit te kunnen doen stellen we een experimentele aanpak voor, waarin we verschillende DDoS-scenarios beschrijven en de effecten van de verschillende aanpakken erop bekijken en beoordelen.

3 Scenarios

Er zijn vele, vele vormen en smaken van DDoS-aanvallen. Zonder afbreuk te willen doen aan die diversiteit stellen we de volgende scenarios voor om kenmerkende aspecten uit te lichten.

3.1 Scenariocategorieën

Norm Zonder ijkpunt in de praktijk van het normale valt er niets zinnigs te zeggen over de gedragingen van netwerk en diensten onder abnormale omstandigheden. We dienen dus kenmerken van de normaalsituatie te bepalen en vast te leggen.

Applicaties Zuivere applicatie-aanvallen richten zich op het 'plat' leggen van een specifieke dienst. In dit geval richten we ons op de klassieke TCP-diensten HTTP en HTTPS, de versleutelde vorm ervan, en op de UDP-dienst DNS.

Spoofing Specifiek lastig is het geval waarbij een aanval van binnenuit het netwerk plaatsvindt, typisch met gefingeerde ('spoofed') netwerkadressen die in principe wel eigen zijn aan het netwerk - en daarmee niet categorisch geblokkeerd kunnen worden. We genereren dergelijke 'spoofed' aanvallen en bezien de mogelijkheden om aanvalsverkeer te onderscheiden van regulier verkeer.

Flooding Netwerkapparatuur en programmatuur in het algemeen is potentieel kwetsbaar voor diverse protocolspecifieke aanvallen. We genereren passend TCP-, UDP-, ICMP-verkeer.

Saturatie Het verzadigen van de beschikbare netwerkcapaciteit is de zuivere volumetrische aanval. We voeren deze uit met een mengsel van min of meer regulier (gesimuleerd) netwerkverkeer - kleine en grote pakketen, vele source- en destination adressen, verschillende netwerktypen en protocollen.

3.2 Concreet

Alle onderstaande scenarios worden volgens de volgende methodiek onderzocht:

1. Eerst wordt een 'baseline' meting gedaan;
   - overall/high level;
   - breakdown per component op 't netwerkpad.
2. Vervolgens wordt een speficieke aanval uitgevoerd en de degradatie van geboden diensten bepaald (real-world impact) volgens een van tevoren gedefiniëerde meetmethode;
3. Vervolgens wordt een aantal mitigatiestrategieën bezien en ingeregeld (voor zover van toepassing en haalbaar):
   - rate-limiting op netwerkniveau,
   - DDoS-maatregelen in generieke network security appliances,
   - inzet van speficieke on-premise anti-DDoS technologie, en
   - 'upstream' orkestratie via mechanismen als BGP flowspec en productspecifieke APIs (mogelijk ook inter-vendor).
4. Na inzet van elke mitigatie wordt de speficieke aanval herhaald en de degradatie van geboden diensten opnieuw bepaald.
   - overall/high level;
   - breakdown per component op 't netwerkpad.

SURFnet heeft een netwerk, ***Onweer***, beschikbaar gesteld dat een aantal locaties met 10Gbps onderling verbindt en gerouteerd met het Internet is. Er zijn VMware ESX servers beschikbaar om 'attackers' (traffic gene-

rators) en ‘victims’ op te draaien.

De volgende scenarios worden uitgevoerd.

3.2.1 Volumetrische aanval

Primaire eigenaar Xander Jansen (SURFnet)

Ingrediënten

- Een gerouteerd 10Gbps netwerk
- Systemen (aantal: …) om als doelwit te dienen
- Systemen (aantal: …) om als aanvaller te dienen
- Systemen (aantal: …) om legitiem gebruik te genereren/meten
- …

Doelwit is een tweetal relatief *(nader te bepalen)* eenvoudige diensten: TCP en UDP. Bijvoorbeeld: HTTP en DNS.

Beschrijving Een volumetrische aanval *onder* de beschikbare linespeed wordt uitgevoerd door:

1. hoge packet rates (i.e. met 'small packets'/fragmentatie);
2. grote hoeveelheden concurrente sessies;
3. hoge session rates (i.e. met kleine/korte c.q. onvolledige sessies).

3.2.2 SYN floods

Primaire eigenaar Arjan Broos, Jeffeny Hoogervorst (Universiteit van Tilburg)

Ingrediënten

- Een gerouteerd 10Gbps netwerk
- Systemen (aantal: …) om als doelwit te dienen
- Systemen (aantal: …) om als aanvaller te dienen
- Systemen (aantal: …) om legitiem gebruik te genereren/meten
- …

Doelwit is een relatief *(nader te bepalen)* eenvoudige TCP dienst, bijvoorbeeld 'echo'.

Beschrijving Er worden SYN floods met hoge packet rates gegenereerd.

1. hoge SYN packet rates (met allerlei variaties in packet size, andere flags, …).

3.2.3 Interne spoofing

Primaire eigenaar Peter Peters, Leon Haverkotte (TU Twente, onder voorbehoud)

Ingrediënten

- Een gerouteerd 10Gbps netwerk
- Systemen (aantal: …) om als doelwit te dienen
- Systemen (aantal: …) om als aanvaller te dienen
- Systemen (aantal: …) om legitiem gebruik te genereren/meten
- …

Doelwit is een in principe breed spectrum van *(nader te bepalen)* diensten.

Beschrijving

3.2.4 DDoS en stateful componenten

Primaire eigenaar Arjan Nolle (Rijksuniversiteit Groningen)

Ingrediënten

- Een gerouteerd 10Gbps netwerk
- Systemen (aantal: …) om als doelwit te dienen
- Systemen (aantal: …) om als aanvaller te dienen
- Systemen (aantal: …) om legitiem gebruik te genereren/meten
- 'Stateful' netwerkcomponent: een Palo Alto PA-5060 firewall
- 'Stateful' netwerkcomponent: load balancer (?)
- 'Stateful' netwerkcomponent: …

Doelwit is een in principe breed spectrum van *(nader te bepalen)* diensten.

Beschrijving 'Stateful' componenten kunnen gevoelig zijn voor 'state exhaustion' attacks. Relevant zijn:

1. grote hoeveelheden concurrente sessies;
2. hoge session rates (i.e. met kleine/korte c.q. onvolledige sessies).

3.3 Benodigdheden

Om de nodige tests uit te voeren is met name benodigd:

- Een representatief testnetwerk van voldoende capaciteit (≥10Gbps);
- Reguliere clients op dit netwerk;
- 'Aanvallers' die applicatie- en volumetrische aanvallen kunnen uitvoeren door het relevante netwerkverkeer te genereren;
- Doelwitten (servers/services) die zonder consequentie aangevallen mogen worden;
- Generieke 'rate limiting' faciliteiten ten behoeve van de toepassing van generieke doorvoerbeperkingen binnen het testnetwerk;
- Specifieke anti-DDoS technologie/appliances.

SURFnet en de participerende universiteiten zullen naar verwachting in staat zijn om de nodige testfaciliteiten in te richten en vorm te geven, voor zover al niet aanwezig. Voor de specifieke DDoS-netwerktechnologie probeert ON2IT in de nodige zaken te voorzien, in overeenstemming met specialistische toeleveranciers.

3.4 Tools

Het volgende is ongetwijfeld geen extensief volledige lijst; aanvullingen welkom.

- (Unix) ping is een standaard tool om ping traffic – potentieel zeer veel daarvan – te genereren.
- fping[1] is een open source tool om (veel) ping verkeer naar meerdere bestemmingen te genereren en respons te meten.
- hping[2] is een open source TCP/IP packet assembler/analyzer, onder andere goed bruikbaar om TCP- en UDP-floods te genereren.
- ab - Apache HTTP server benchmarking tool[3] is een open source benchmark tool voor HTTP servers.
- curl-loader[4] is een open source benchmark tool voor HTTP en FTP servers.
- httperf[5] is een open source benchmark tool voor HTTP servers.
- siege[6] is een open source benchmark tool voor HTTP servers.
- Slow loris and SlowHTTPTest are 'slow and low' DoS attack tools.
- BoNeSi[7] is een open source botnet traffic simulator.
- ostinato[8] is een open-source, cross-platform network packet crafter/traffic generator en analyzer.
- Ixia IxNetwork[9] is een (commerciële) tool om high-level network flows te genereren, met real-time analyse and statistiek.
- Spirent Avalanche Next[10] is een (commerciële) enterprise-level/carrier grade network load generator en functionele testtool.

[1] Zie http://fping.org.
[2] Zie http://hping.org.
[3] Zie https://httpd.apache.org/docs/2.4/programs/ab.html.
[4] Zie http://curl-loader.sourceforge.net.
[5] Zie https://github.com/httperf/httperf.
[6] Zie https://www.joedog.org/siege-home/.
[7] Zie https://github.com/markus-go/bonesi.
[8] Zie http://ostinato.org.
[9] Zie http://www.ixiacom.com/products/ixnetwork.
[10] Zie http://www.spirent.com/Products/AvalancheNext.

- tcpreplay[11] is een open source tool om packet captures te herinjecteren.
- FortiDDoS[12] is commerciele on-premise DDoS-mitigatie (gaat gebruikt worden bij een participerende partij).
- Arbor Networks[13] biedt commerciele on-premise- en upstream DDoS-mitigatietechnologie (wordt reeds gebruikt bij participerende partijen).

[11]Zie http://tcpreplay.synfin.net.
[12]Zie http://www.fortinet.com/products/fortiddos/.
[13]Zie http://www.arbornetworks.com/products/ddos-protection-products.

4 Criteria

Testscenarios opzetten is één ding, ze uitvoeren en de resultaten beoordelen is het volgende. Om testresultaten te kunnen beoordelen zijn evaluatiecriteria nodig.

Bij het beoordelen van testresultaten speelt de waarneembare impact van de aanval een rol. We onderscheiden de volgende.

Geen invloed De waarnemingen komen overeen met de normaalsituatie.

Gracieuze degradatie Er is in functioneel opzicht sprake van een werkende situatie, zij het met verminderde responsiviteit en/of benutbare capaciteit.

Functionele storing Er zijn functionele storingen, maar niet volledig.

Uitval Het betreffende netwerk of de betreffende dienst is feitelijk niet beschikbaar.

Voor elk van de aangegeven scenarios wordt bepaald wanneer er sprake is van welke impact, en daarvan wordt een overzicht als volgt gegeven.

5 Resultaten

Aanval	***Invloed van Aanpak***		
	Niets doen	**Generieke beperkingen**	**Specifieke DDoS-tech**
Norm	Geen invloed	Geen invloed?	Geen invloed?
Applicaties	?	?	?
Spoofing	?	?	?
Flooding	?	?	?
Saturatie	?	?	?

Tabel 3: Effectiviteit van Aanpakken

6 Oplevering

Doel in eerste instantie is een document van bevindingen en aanbevelingen op te leveren op basis van de opgedane ervaringen. Dit document dient ter informatie en als aanbeveling aan de SURFnet doelgroep.

Lijst van tabellen

OVER ONS

ON2IT is specialist op het gebied van IT-security & Webscale datacenter services en oplossingen. Met onze kennis en expertise helpen wij organisaties met oplossingen in een complexe wereld. Specifieke IT-security die aansluit op de IT infrastructuur, de groei en de IT-wensen van een organisatie. Door middel van publicaties, whitepapers, onderzoek, hoogwaardige events en trainingen delen wij onze kennis en geven wij organisaties handvatten voor slimmere IT-security.