Nieuwsberichten

Meten van internetverkeer voorkomt veel virusleed

Het meten van internetverkeer is van het allergrootste belang om te voorkomen dat computers worden gekraakt. Men kan in een zeer vroeg stadium alarm slaan. Bovendien kunnen providers het gedrag van eindgebruikers goed controleren en in rekening brengen. Aiko Pras en Remco van de Meent analyseren de voordelen van het controleren van netwerkverkeer.

Voetbal is oorlog, ook op het internet. Het EK in Portugal was nog maar net begonnen toen een Duitse internetgoksite een e-mail ontving met de melding dat een DDoS-(Distributed Denial of Service)aanval op hun website zou worden ondernomen. De aanval kon worden afgekocht als 15.000 dollar zou worden betaald. De goksite weigerde, waarna de aanval begon en de site 16 uur onbereikbaar was. Voor de goksiteondernemers was dit een ramp, omdat de dagelijkse omzet tijdens belangrijke toernooien zoals de EK een veelvoud bedraagt van 15.000 dollar. Toch hadden de ondernemers een dergelijke aanval kunnen verwachten, aangezien ook andere sites het afgelopen jaar uit de lucht zijn gehaald door DDoS-aanvallen.
Een DDoS-aanval wordt gewoonlijk uitgevoerd vanaf tientallen tot duizenden gehackte computers. In de meeste gevallen hebben de bezitters van deze computers nauwelijks weet van het feit dat hun computer is geïnfecteerd en voor dergelijke aanvallen wordt misbruikt. Zelfs bij regelmatige installatie van security patches kan het gebeuren dat systemen worden gekraakt. Er bestaat dus geen garantie dat kwaadwilligen buiten de deur worden gehouden. Omdat computers gekraakt kunnen worden, is het van het allergrootste belang het in- en uitgaande verkeer te monitoren en bij abnormaal gedrag alarm te slaan. Monitoring kan op de computers zelf plaatsvinden, maar ook op speciale meetsystemen die op strategische lokaties met het netwerk zijn verbonden.
Internetproviders hebben al jaren systemen die het verkeer monitoren. De meeste netwerkapparaten bevatten tellers die bijhouden hoeveel pakketjes en bytes zijn uitgewisseld, hoe groot de pakketjes zijn, hoeveel fouten er zijn opgetreden et cetera. Deze tellers kunnen worden uitgelezen via het ‘Command Line Interface’ (CLI) en met behulp van het ‘Simple Network Management Protocol’ (SNMP). Naast het bijhouden van tellers kan het nodig zijn complete verkeersstromen te analyseren. Alhoewel voor dit doel soms routers gebruikt kunnen worden, is het vaak toch handig hiertoe speciale meetapparatuur (zogenaamde ‘probes’) te installeren.

Interessant
Het meten van internetverkeer is om meerdere redenen zeer interessant. Providers, maar ook klanten, kunnen bijvoorbeeld nagaan of de afspraken die in de ‘Service Level Agreements’ (SLA’s) zijn overeengekomen wel worden nageleefd. Internetproviders kunnen detecteren of klanten binnen hun ADSL-datalimiet blijven, of dat andere providers niet te veel verkeer genereren. Het meten van internetverkeer is daarom ook voor accounting van belang. Afhankelijk van het abonnement baseren providers de rekening voor eindgebruikers op de hoeveelheid verkeer dat is uitgewisseld. In bedrijfsomgevingen kan het meten van internetverkeer nodig zijn om de rekening van de provider te valideren en de kosten naar individuele gebruikers intern door te berekenen.
Als er fouten optreden moet eveneens gemeten worden. In principe is het aantal mogelijke foutbronnen welhaast onbeperkt. Zo kunnen de routeringstabellen inconsistent zijn, waardoor pakketten tussen routers heen en terug worden gestuurd. Als gevolg hiervan worden pakketten niet meer bij de bestemming afgeleverd. Ook kan het voorkomen dat systemen verkeerde IP-adressen toegewezen krijgen omdat iemand tijdens het installeren van een pc per ongeluk een DHCP (Dynamic Host Configuration Protocol) server heeft geïnstalleerd. Toegang tot centrale servers of zelfs het hele internet kan plotseling onmogelijk worden, omdat ergens verkeerde opties zijn geselecteerd. In al deze gevallen geven normale foutmeldingen vaak onvoldoende informatie om de foutoorzaak te detecteren. De netwerkbeheerder ontkomt dan niet aan het opslaan van netwerkpakketjes in speciale bestanden (‘traces’), die vervolgens geanalyseerd worden.

Zelfs als er geen fouten optreden kan het verstandig zijn traces van het normale verkeer te maken. De kennis die verkregen wordt door normale verkeersstromen te bestuderen, kan later worden gebruikt om abnormale patronen, zoals bijvoorbeeld veroorzaakt door virussen, sneller te herkennen. Ook als de performance daalt moet onderzocht worden wat de oorzaken zijn. Het kan zijn dat bepaalde toepassingen, zoals internetradio, peer-to-peer-(P2P)-ruilbeurzen of internetgames een te groot beslag op de capaciteit leggen. Om de performance van de normale toepassingen weer op pijl te brengen, kan de netwerkbeheerder besluiten de poorten die voor P2P-toepassingen gebruikt worden op de access routers te blokkeren.

Gratis

Voor het meten van internetverkeer zijn een groot aantal gereedschappen beschikbaar. Vaak maken deze gereedschappen zelf weer gebruik van de libpcap- of winpcap-software. Deze software, die gratis verkrijgbaar is en op iedere pc kan worden geïnstalleerd, ontvangt internetpakketjes via bestaande Ethernet- of WLAN-interfaces, en kan deze opslaan op disk. Aanvullende software kan gebruik maken van de resulterende traces om het verkeer te analyseren.

Niet alleen het verkeer van en naar de betreffende pc kan worden ontvangen, maar in de zogeheten ‘promiscuous mode’ ook het verkeer tussen andere systemen. Zeker in draadloze omgevingen kan deze software makkelijk misbruikt worden voor het afluisteren van derden. Het is overigens opmerkelijk hoe weinig aandacht men heeft voor dit soort mogelijkheden en dat gebruikers nauwelijks maatregelen nemen om afluisteren te voorkomen. Vaak redeneert men dat geen vertrouwelijke informatie wordt uitgewisseld, maar men vergeet dat er ook nog systeeminformatie wordt uitgewisseld die door potentiële inbrekers misbruikt kan worden om systemen te infecteren.

Voor het analyseren van traces wordt vaak ‘tcpdump’ gebruikt. De naam van dit programma is wat misleidend, omdat het niet alleen TCP maar ook ander verkeer kan verwerken. Voor de analyse van verkeer is, afhankelijk van het doel, veel software beschikbaar. Erg populair zijn Ntop en Ethereal; ook deze programma’s kunnen gratis worden gedownload en op diverse platformen geïnstalleerd.

Vijf minuten

Om de benodigde netwerkcapaciteit te plannen moet eveneens gemeten worden. Veel netwerkbeheerders gebruiken hiertoe ‘Multi Router Traffic Grapher’-(MRTG)-software. Deze software leest periodiek, bijvoorbeeld iedere vijf minuten, een aantal SNMP-tellers en toont de resultaten in een grafiek (zie kader). Door de maxima in de grafiek te bepalen, en daar een zekere marge bij op te tellen (bijvoorbeeld 20 procent), bepaalt men of de capaciteit moet worden verhoogd. Alhoewel deze methode eenvoudig is, heeft onderzoek aangetoond dat de resultaten tegenvallen als er toepassingen worden gebruikt met een real-timekarakter, zoals Voice over IP (VoIP) en videoconferencing. Voor dit soort toepassingen is het namelijk weinig relevant of de gemiddelde capaciteit over een periode van vijf minuten voldoende is; het real-time karakter vereist immers dat iedere seconde of zelfs binnen delen daarvan de beschikbare capaciteit voldoende is.

Een aantal jaar geleden werd nog gedacht dat voor tijd-kritische toepassingen speciale prioriteitsmechanismen, zoals Integrated Services (IntServ) en Differentiated Services (DiffServ), in het internet zouden worden ingebouwd. Alhoewel dergelijke mechanismen op kleine schaal wel worden toegepast, hebben problemen met het configureren van deze mechanismen ervoor gezorgd dat er geen grootschalig gebruik van wordt gemaakt. Om kwaliteit te garanderen hebben netwerkbeheerders momenteel dan ook geen andere keuze dan het netwerk te overdimensioneren. Omdat capaciteit geld kost, moet overdimensionering wel op een intelligente manier worden uitgevoerd. Onderzocht wordt daarom of er een relatie te vinden is tussen de 5-minuten-verkeersgemiddelden, zoals die bepaald kunnen worden met behulp van MRTG, en verkeerspieken die op de seconde- tot milliseconde-schaal optreden. De eerste resultaten van dit onderzoek zijn positief; het lijkt inderdaad mogelijk om met eenvoudige middelen te voorspellen welke capaciteit nodig is voor het intelligent dimensioneren van netwerken.

AUTEUR: Aiko Pras en Remco van de Meent

Aiko Pras (pras@cs.utwente.nl) en Remco van de Meent (r.vandemeent@utwente.nl) zijn medewerkers van de Universiteit Twente. Ze verrichten onderzoek binnen het Centrum voor Telematics en Informatie Technologie (CTIT), en participeren in projecten (M2C, Mobile en Wireless) van het Telematica Instituut (TI). Tevens wordt samengewerkt met SURFnet voor het meten van netwerkverkeer.

Quarantaine
De traces van netwerkverkeer die door middel van bijvoorbeeld libpcap gemaakt kunnen worden, kunnen door andere applicaties onderzocht worden om specifieke problemen aan te pakken. Een voorbeeld van zo'n probleem is het vroegtijdig ontdekken van het rondzwerven van virussen op lokale netwerken, om verdere besmetting van honderden of duizenden computers te voorkomen. Een project op de UT heeft geleid tot de ontwikkeling van een systeem dat, door analyse van netwerkverkeer, automatisch besmette computers 'in quarantaine' plaatst. Hierdoor wordt voorkomen dat zij nog andere systemen infecteren. De gebruiker van het besmette systeem krijgt bij het internetten automatisch een webpagina op het scherm waarop aangegeven wordt waarom de computer in quarantaine is geplaatst. Er kan enkel nog verbinding gemaakt worden met sites als Windows Update en de websites van de bekende antivirusfabrikanten, zodat het besmette systeem gerepareerd kan worden. Tenslotte kan het systeem uiteraard weer uit quarantaine worden gehaald. Meer informatie over dit project is te vinden op http://quarantaine.utwente.nl.

Principe MRTG is eenvoudig
Een van de bekendste pakketten voor het beheren van netwerken is het programma Multi Router Traffic Grapher (MRTG). Dit programma wordt gebruikt door commerciële netwerk operators, bedrijven, universiteiten en zelfs privé-personen thuis. Het programma is aan de ETH Zurich ontwikkeld door Tobias Oetiker, en wordt op vrijwillige basis door een groot aantal enthousiastelingen verder ontwikkeld. Het programma is vrij verkrijgbaar met een open-source-(GNU-GPL)-licentie. Het principe van MRTG is eenvoudig: periodiek worden tellers uitgelezen, de gevonden waarden worden in een database gezet, waarna plaatjes gegenereerd worden die via het web bekeken kunnen worden.
Voor het uitlezen van tellers wordt gewoonlijk het Simple Network Management Protocol (SNMP) gebruikt. Als basisinstelling worden tellers iedere vijf minuten uitgelezen; het is echter ook mogelijk een andere tijdbasis te kiezen. Netwerkbeheerders zijn meestal geïnteresseerd in tellers die de hoeveelheid in- en uitgaand verkeer bijhouden; MRTG staat echter ook toe andere tellers te kiezen, zoals de CPU-belasting van een server, de temperatuur van een router, of het aantal ontvangen e-mailberichten. Er zijn ook voorbeelden waarin MRTG wordt gebruikt voor heel andere toepassingen; op http://stats.kijk.info/ wordt bijvoorbeeld met behulp van MRTG de lengte van de files op de Nederlandse autosnelwegen bijgehouden.
De waarden die met SNMP zijn opgehaald, worden opgeslagen in een database. Omdat de prestaties van de oorspronkelijke MRTG-database wel eens problemen gaf, is in een later stadium door de makers van MRTG de zogeheten 'Round Robin Database' (RRD) ontwikkeld. Deze database kan in combinatie met MRTG, maar ook afzonderlijk worden gebruikt. Periodiek, bijvoorbeeld iedere vijf minuten, worden de waarden in de database gebruikt voor het genereren van plaatjes. Afhankelijk van de gekozen instellingen geven deze plaatjes een overzicht van het verloop van de tellerwaarden per dag, week, maand of per jaar.
De figuur (zie boven) toont een MRTG-plaatje met daarin het in- en uitgaande verkeer van de UT. Het plaatje is gemaakt op 21 juli. De bovenste lijn toont hoeveel verkeer vanaf de universiteit het internet is opgestuurd, de onderste lijn toont de hoeveelheid verkeer die vanaf het internet is binnengehaald. In een oogopslag is duidelijk dat de UT meer informatie produceert dan consumeert. Het plaatje laat eveneens zien dat het maximum (over een periode van vijf minuten) ruim 500 Mbps bedraagt, en ongeveer twee keer hoger is dan de gemiddelde waarde (277 Mbps). Verder blijkt dat de hoogste belasting 's avonds optreedt; dit kan een indicatie zijn voor het feit dat veel aanvragen vanuit de VS komen. Meer informatie over MRTG is te vinden op http://people.ee.ethz.ch/~oetiker/webtools/mrtg. (Aiko Pras en Remco van de Meent)

Weekblad 2004, week 37
