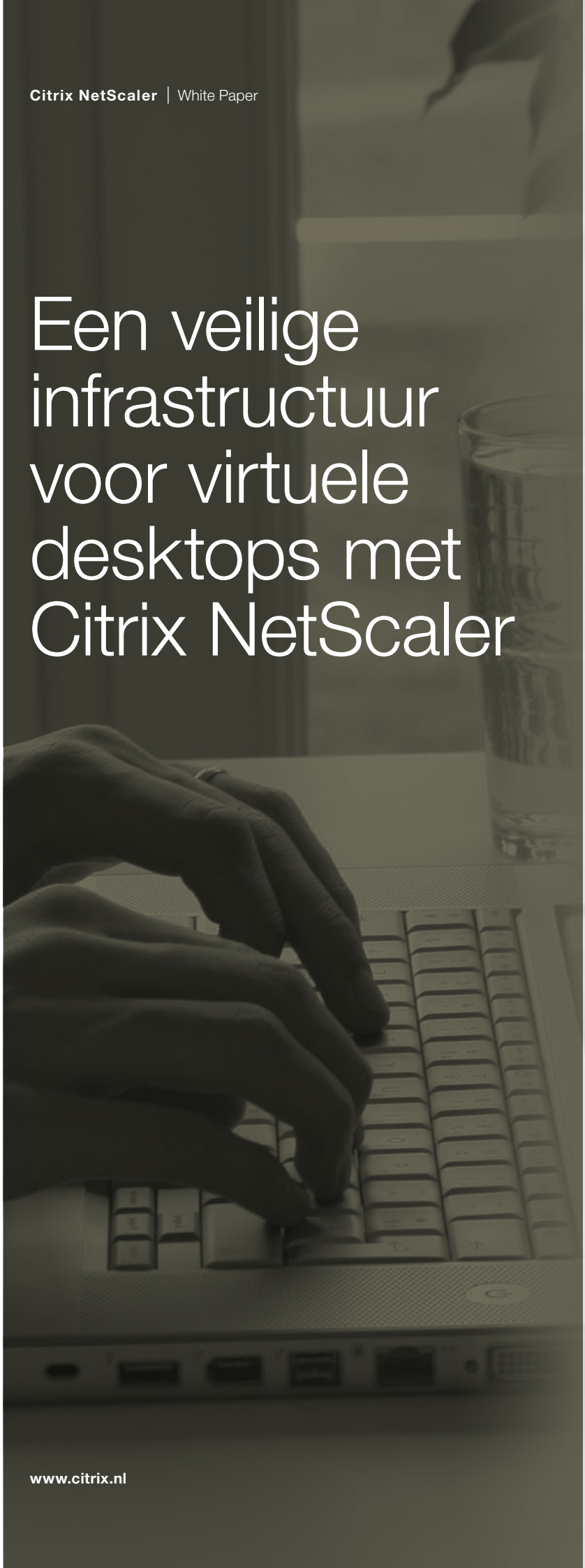
Citrix NetScaler | White Paper

Een veilige infrastructuur voor virtuele desktops met Citrix NetScaler



CITRIX®

www.citrix.nl

Moderne organisaties kiezen massaal voor desktopvirtualisatie. Ze willen daarmee hun bedrijfskosten verlagen, flexibele werkplekken creëren, de wendbaarheid van de organisatie verhogen en iets doen aan hun gegevensbeveiliging en compliance. Deze voordelen zijn echter pas haalbaar wanneer de virtuele desktopinfrastructuur een optimale beveiliging en beschikbaarheid biedt. In deze tekst leggen we uit hoe Citrix® NetScaler® hiervoor kan zorgen. NetScaler integreert diverse beveiligingsmechanismen voor de netwerk- en applicatielaag, geavanceerde mogelijkheden voor toegangscontrole en controle over wat de gebruiker kan doen, en een schat aan extra features op het gebied van servicedelivery. Zo maximaliseert NetScaler de voordelen van virtuele desktops.

Desktopvirtualisatie en beveiliging

Over de hele wereld schakelen organisaties van alle soorten en maten massaal over op virtuele desktops. Gartner verwacht dat er in 2014 70 miljoen gebruikers zullen zijn met een gehoste virtuele desktop.[1] Verwonderlijk is dat niet, want de voordelen zijn groot. Met een complete desktopvirtualisatieoplossing heeft een organisatie minder desktops nodig en kunnen de bedrijfskosten fors en blijvend omlaag. Het aanbieden van flexibele werkplekken wordt sterk vereenvoudigd en de hele organisatie wordt wendbaarder gemaakt, wat belangrijk is voor de strategische aspecten van een organisatie, zoals fusies en overnames, expansie en dynamische samenwerkingsverbanden.

Een ander groot voordeel van desktopvirtualisatie is dat de informatiebeveiliging en compliance sterk worden verbeterd doordat data en applicaties worden gecentraliseerd in het datacenter van de organisatie. Gebruikers bekijken en gebruiken hun desktop op afstand. Mogelijk gevoelige informatie hoeft dus niet op het lokale apparaat zelf te staan.

De beveiliging wordt verbeterd doordat centrale desktopapplicaties en besturingssystemen gemakkelijker zijn aan te sturen voor de systeembeheerders. Centrale controle maakt het enerzijds gemakkelijker om te standaardiseren en daardoor de complexiteit, kosten en risico's te verminderen, en anderzijds om updates en beveiligingspatches sneller en grondiger door te voeren. Een ander voordeel van een gecentraliseerd model is dat het toewijzen en intrekken van rechten veel sneller en efficiënter kan verlopen. Bovendien hoeven gebruikers geen devices, software of data terug te bezorgen aan de organisatie. Desktopvirtualisatie werkt immers compleet anders.

[1] Forecast: Hosted Virtual Desktops, Worldwide, 2010-2014, Gartner, november 2010.

Het gaat niet vanzelf

Desktopvirtualisatie biedt de moderne organisatie veel voordelen. Maar die voordelen komen niet vanzelf. De organisatie moet er wel eerst voor zorgen dat (onder meer) de beveiliging van de geïmplementeerde desktopvirtualisatie in orde is. Dit lijkt misschien een cirkelredenering – een organisatie moet eerst in een bepaald pakket beveiligingsmaatregelen investeren om de voordelen van een ander pakket te kunnen verwezenlijken – maar de samenhang is absoluut belangrijk. Een goede beveiliging is om verschillende redenen noodzakelijk:

- **Toegang op afstand.** Mobiliteit en telewerken zijn sterk in opkomst. Veel gebruikers moeten op afstand bij hun desktop kunnen, vaak via een onveilig openbaar netwerk.
- **Uiteenlopende devices.** Door de zogeheten consumerisation van de IT moeten er tegenwoordig steeds meer verschillende clientdevices worden ondersteund, met uiteenlopende beveiligingskenmerken en profielen. Dat die devices meestal geen eigendom van de organisatie zijn en dus ook niet onder controle van de organisatie vallen, maakt de zaak alleen maar ingewikkelder. Belangrijk om te weten is dat een clientdevice nog altijd een risico kan vormen, ook al is het met desktopvirtualisatie niet meer nodig dat gegevens lokaal worden opgeslagen. Gevoelige gegevens kunnen nog wel worden bekeken en de rechten die aan de gebruiker of het device zijn toegewezen kunnen nog steeds worden misbruikt om een aanval op poten te zetten.
- **Toegang.** Met desktopvirtualisatie hebben gebruikers toegang tot een complete desktop. Ze kunnen niet alleen bij hun eigen, directe applicaties en data, maar ook bij alle resources verder downstream waartoe die desktop maar toegang heeft. Dit maakt beveiliging in het algemeen en toegangscontrole in het bijzonder belangrijker dan ooit.
- **Concentratie van resources.** Het belang van een goede beveiliging kan niet genoeg worden benadrukt, aangezien desktopvirtualisatie betekent dat een organisatie alles op één kaart zet. In tegenstelling tot bij het klassieke desktopmodel met verspreid opgestelde computers is het nu mogelijk om met één geslaagde aanval een heel groot aantal gebruikers en desktopsystemen te treffen. Ook het grote geheel mag niet uit het oog worden verloren. Hackers gaan tegenwoordig goed georganiseerd te werk. Ze willen zo veel mogelijk schade aanrichten of met waardevolle gegevens aan de haal gaan. Een goede verdediging is dus een vereiste.

Hoe Citrix NetScaler kan helpen

Als geavanceerde oplossing voor het aanbieden van applicaties en cloud- en enterprise-services biedt NetScaler tal van mogelijkheden en is het de ideale keuze als front-end voor de desktop-virtualisatie-infrastructuur. Belangrijk in dit verband zijn de vele beveiligingsmechanismen en features die NetScaler biedt om de virtuele desktopinfrastructuur te beschermen. Deze zijn in verschillende categorieën onderverdeeld.

Citrix NetScaler in het kort

NetScaler is een enterprise-class oplossing die applicaties en diensten vijfmaal zo goed laat presteren, dankzij een krachtige combinatie van netwerkgebaseerde applicatieversnelling, servers die worden ontlast, en een hoge beschikbaarheid en uitstekende applicatie-beveiliging. NetScaler wordt gebruikt door de grootste websites ter wereld.

Geraamd wordt dat dagelijks circa 75 procent van de internetgebruikers op een site komt die door NetScaler wordt aangeboden. Verder wordt NetScaler door duizenden organisaties gebruikt voor op het publiek gerichte webactiviteiten, intranetwerken en virtuele desktops.

Beveiliging van de netwerklaag

NetScaler biedt verschillende manieren om de netwerklaag van VDI (Virtual Desktop Infrastructure) te beschermen. Zo kan NetScaler door de systeembeheerders worden gebruikt om een basale vorm van toegangscontrole mogelijk te maken met simpele toegangscontrolelijsten (ACL's) voor laag 3 en 4 om daarmee legaal verkeer door te laten en verkeer dat onveilig wordt geacht tegen te houden. Verder is het ontwerp zodanig dat elke infrastructuur waarvoor NetScaler als front-end dient, automatisch wordt beveiligd. Zo heeft NetScaler een krachtige, aangepaste TCP/IP-stack (wel conform de standaarden) om het volgende mogelijk te maken:

- Verkeer met een afwijkend format dat een bedreiging kan zijn voor de hele desktop-infrastructuur, wordt automatisch gedropt.
- Low-level verbindingsgegevens (IP-adressen en serverpoorten bijvoorbeeld) kunnen verborgen worden gehouden voor hackers.
- Allerlei soorten DoS-aanvallen die zwakke plekken in de gangbare verbindingstechnieken misbruiken, kunnen worden gehinderd.

Beveiliging van de applicatielaag

Een ander groot voordeel van het NetScaler-design is de proxyarchitectuur. In combinatie met HTTP/URL-rewrites en L7-contentfilters maakt dit het volgende mogelijk:

- Connectionbrokers en andere VDI-componenten verder downstream kunnen worden beschermd tegen directe TCP- en UDP-verbindingen van externe gebruikers. Dit beschermt tegen malware en andere aanvallen.
- Deze componenten kunnen worden beschermd met cloaking en content-security om daarmee foutcodes van de server, echte URL's en andere informatie afgeschermd te houden, zodat misbruik door hackers onmogelijk wordt.

VDI-implementaties bevatten vaak webgebaseerde componenten die ook een goede beveiliging tegen aanvallen moeten krijgen. De geïntegreerde NetScaler App Firewall™ beschermt tegen aanvallen op de applicatielaag, zoals SQL-injection, cross-site scripting en bufferoverflows.

NetScaler App Firewall biedt:

- een flexibel, hybride beveiligingsmodel dat beschermt tegen onbekende gevaren op basis van een actuele database met handtekeningen van aanvallen en een positief beveiligingsmodel tegen zero-day attacks (nog zonder handtekening);
- eenvoudig te configureren beveiligingspolicy's en sjablonen voor een eenvoudige en snelle implementatie en dito beheer;
- volledige integratie met NetScaler, waardoor security en VDI-beschikbaarheid met één policy en console kunnen worden beheerd.

Een betere bescherming voor de applicatielaag is ook mogelijk dankzij de betere ondersteuning voor 2048-bits SSL-sleutels. Geheel volgens de richtlijnen van NIST Special Publication 800-57 worden voor certificaten voor cryptografie met openbare sleutels – een onderliggende component van SSL – nu routinematig 2048-bits sleutels gebruikt in plaats van de 1024-bits sleutels die eerder de norm waren. Deze verdubbeling van de sleutelgrootte vertegenwoordigt echter een exponentiële toename van het aantal processorcycli dat nodig is om SSL-transacties te verwerken (gemiddeld vijfmaal zoveel). Om de migratie naar 2048-bits SSL-certificaten vlotter te laten verlopen verbetert NetScaler de SSL-performance met geavanceerde vormen van acceleratie. Voor organisaties betekent dit dat ze serviceovereenkomsten en de daarin vastgelegde performance kunnen naleven zonder de beveiliging zwakker te maken.

Geavanceerde toegangscontrole en controle over handelingen

NetScaler Access Gateway™, dat een integrale component van het product vormt, is een complete SSL VPN waarmee een systeembeheerder heel gedetailleerd op applicatieniveau controle over de gebruikers heeft en de gebruikers externe toegang kan bieden tot hun virtuele desktop, ongeacht locatie. Met Access Gateway kan de systeembeheer de toegang beheren en bepalen welke handelingen mogelijk zijn binnen een sessie op basis van zowel de identiteit als het device van de gebruiker. Het resultaat is beter beveiligde applicaties en data en een betere compliance zonder nog meer apparatuur te installeren.

De eerste twee manieren waarop Access Gateway externe toegang tot virtuele desktops mogelijk maakt zijn een versleutelde tunnel en ondersteuning voor de meest uiteenlopende methoden voor gebruikersverificatie. Desktopsessies via een openbaar netwerk kunnen niet worden onderschept en de organisatie kan optimaal blijven profiteren van haar bestaande directory- en identity-management-infrastructuur.

De volgende stap is fijnmazige en adaptieve toegangscontrole. Met Access Gateway kan de systeembeheerder de toegang tot virtuele desktops strikt regelen met policy's op basis van zowel vaste als dynamische kenmerken, zoals de identiteit en rol van de gebruiker, de sterkte van de verificatie, de locatie, het tijdstip van de dag en de identiteit en beveiligingsstatus van het gebruikte clientdevice. Deze mogelijkheid steunt op een andere belangrijke beveiligingsfunctie: analyse van het eindpunt. Geïntegreerde scans van de eindapparatuur van de gebruikers kunnen dienen om de clientdevices continu te monitoren en zo te bepalen of de beveiligingssoftware van de client (antivirus, firewall of andere verplichte software) actief en up-to-date is. Devices die niet aan de eisen voldoen krijgen helemaal geen of slechts beperkte toegang, of ze worden in quarantaine geplaatst. Het enige wat de gebruiker dan nog kan doen, is naar een site gaan waar hij of zij de benodigde tools vindt om de configuratie wel aan de eisen te laten voldoen.

Aangezien het aantal clientdevices blijft toenemen en gebruikers zelf verantwoordelijk worden gemaakt voor die devices, zijn geavanceerde mogelijkheden om acties en data te sturen erg belangrijk voor de beveiliging. Gerelateerde features zijn:

- verbeterde split-tunneling, waarbij gebruikers wel toegang hebben tot hun eigen desktop en het lokale subnet van de client, maar niet rechtstreeks op internet kunnen;
- controle over handelingen, waarbij er door middel van adaptieve policy's restricties kunnen gelden voor het lokaal afdrukken, kopiëren, plakken en opslaan op schijf;
- opschonen van het cachegeheugen van de browser, waarbij alle objecten en data die in de lokale browser zijn opgeslagen worden verwijderd op het moment dat de sessie van de virtuele desktop wordt beëindigd.

Als laatste beveiligingsfeatures noemen we de uitgebreide logging-, auditing- en reporting-mogelijkheden van de centrale beheerconsole van NetScaler: Citrix Command Center. Deze functies zijn niet alleen onmisbaar bij het troubleshooten, maar ook bij het opsporen van misbruik en andere zaken die erop kunnen wijzen dat een client of virtuele desktop een risico vormt of dat er een bredere aanval tegen de virtuele desktopomgeving van de organisatie op komst is.

Andere overwegingen

Netwerkbeveiliging is slechts één stukje van de totale beveiligingsstrategie voor VDI, maar wel een heel belangrijk stukje. Tevens is het slechts één aspect van wat NetScaler te bieden heeft.

Meer dan NetScaler alleen

Hoe krachtig de features van NetScaler voor het beschermen van virtuele desktops ook zijn, ze hebben betrekking op maar één dimensie van een allesomvattende VDI-beveiligingsstrategie. Organisatie moeten niet alleen kijken naar de netwerkbeveiliging, maar ook nadenken over:

- **Beveiliging van de client.** Ondanks het centrale model van desktopvirtualisatie blijft een gecompromitteerd clientdevice een risico vormen. De features die NetScaler heeft om aan eindpuntanalyse te doen, om precies te bepalen wat de gebruiker wel en niet mag doen en om data te wissen zijn in dit opzicht een belangrijk instrument. In bepaalde risicovolle gevallen kan implementatie van een compleet pakket beveiligingssoftware voor het eindpunt echter ook noodzakelijk zijn.
- **Beveiliging van het virtuele systeem.** Hiermee wordt bedoeld dat de virtuele machines schoon en up-to-date worden gehouden (virtuele desktops moeten de laatste, volledig gepatchte versie van applicaties en besturingssysteem gebruiken en VM's die niet meer worden gebruikt moeten ook echt worden verwijderd). Hieronder valt ook netwerkisolatie voor alle VDI-componenten en eventueel implementatie van versleuteling voor gerelateerde opslagvolumes (afhankelijk van de concentratie resources).
- **Beveiliging van de virtuele desktop.** Met VDI bevinden de devices van de gebruikers – met het bijbehorende risicovolle gedrag (verbinding met netwerken en computers die niet altijd even betrouwbaar zijn) – zich in het hart van het datacenter van de organisatie. Daarom moet goed worden nagedacht over implementatie op VM- en/of hypervisor-niveau van antivirus-/antimalware-agents, software voor de monitoring van activiteiten en andere preventieve software. Wat ook een goed idee kan zijn: maak verschillende klassen gebruikers aan die een virtuele desktop krijgen met een verschillende configuratie en houd de VM's voor die virtuele desktops vervolgens apart op basis van betrouwbaarheid.

Meer dan beveiliging alleen

Om alle voordelen van desktopvirtualisatie goed te laten uitkomen moet goed worden nagedacht over de beveiliging van de virtuele desktopinfrastructuur. Organisaties moeten ook rekening houden met de beschikbaarheid, performance en schaalbaarheid van de oplossing die ze implementeren. Wat heb je aan een zwaar beveiligde omgeving voor virtuele desktops wanneer de beschikbaarheid sterk te wensen overlaat? Of aan een performance die zo slecht is dat de gebruikers denken dat het systeem onbeschikbaar is?

NetScaler is het perfecte front-end voor de virtualisatie-infrastructuur voor virtuele desktops. NetScaler heeft een aantrekkelijk pakket netwerkbeveiligingsfuncties en beschikt verder over:

- een combinatie van enterprise-class server load balancing, global server load balancing en health monitoring, en voorzieningen gericht op beschikbaarheid van de virtuele desktop en continuïteit voor de organisatie;
- de meest uiteenlopende mechanismen om de performance van virtuele desktops via het netwerk te verbeteren en de gebruikerservaring te stroomlijnen;
- features om de belasting op een intelligente manier te verdelen en servers minder te belasten, zodat de virtuele desktopinfrastructuur naadloos kan worden geschaald.

Tot slot

NetScaler, dat beschikbaar is als krachtige hardwarematige appliance of als flexibele softwarematige virtual appliance, kan gemakkelijk en kosteneffectief worden geïmplementeerd als front-end voor moderne virtuele desktops. Met zijn betrouwbare beveiliging voor de netwerk- en de applicatielaag en geavanceerde mogelijkheden op het gebied van toegang en gegevenscontrole maximaliseert NetScaler de voordelen die organisaties van desktopvirtualisatie verwachten. NetScaler is zoveel meer dan een beveiligingsoplossing. NetScaler maakt het mogelijk om ook de beschikbaarheid, prestaties en schaalbaarheid van de virtuele desktops sterk te verbeteren.

Wereldwijd Hoofdkantoor

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309 USA
Telefoon: +1 800 393 1888
+1 954 267 3000

Europees Hoofdkantoor

Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen
Zwitserland
+41 52 635 7700

Benelux Kantoren

Citrix Systems Nederland
Clarissenhof 3c
4133 AB, Vianen
Nederland
+31 347 324 800

Citrix Systems België
Pegasuslaan 5
1831 Diegem
België
+32 2 709 2231

Pacific Hoofdkantoor

Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central, Hong Kong
+852 2100 5000

Citrix Online divisie

5385 Hollister Avenue
Santa Barbara, CA 93111
+1 805 690 6400

Over Citrix

Citrix Systems, Inc. (Nasdaq:CTXS) transformeert de manier waarop mensen, bedrijven en IT-ers werken en samenwerken in het cloud-tijdperk. Met zijn cloud-, collaboration-, netwerk- en virtualisatietechnologieën maakt Citrix mobiel werken en cloud-diensten mogelijk, waardoor IT voor bedrijven eenvoudiger en toegankelijker wordt voor meer dan 250.000 organisaties wereldwijd. Citrix wordt dagelijks gebruikt door 75 procent van alle internetgebruikers wereldwijd, het bedrijf werkt samen met meer dan 10.000 partners in 100 landen. De jaarlijkse omzet in 2011 was 2,21 miljard Amerikaanse dollar.