

Ministerie van de Vlaamse Gemeenschap

Veilig en krachtig Cisco-netwerk achter een toekomstgerichte portaalsite

"HET CONTACT MET CISCO IS VAAK DYNAMISCH EN INSPIREREND. HET BEDRIJF KENT ALS GEEN ANDER DE BESTE MANIER VOOR HET OPSTELLEN VAN EEN NETWERKARCHITECTUUR. ZE LEVEREN NIET ALLEEN ALLE ONDERDELEN VAN HET NETWERK, MAAR OOK ALLE BEVEILIGINGSFUNCTIES EN EEN STABIELE LAY-OUT. ZO KAN JE VAN BEGIN TOT EINDE EEN OVERZICHTELIJKE, VEILIGE INFRASTRUCTUUR UITBOUWEN."

Godfried Verhamme, , ambtenaar bij de Entiteit Sturing en Controle Informatie- en Communicatietechnologie bij het Ministerie van de Vlaamse Gemeenschap

Voor de verwezenlijking van de portaalsite moest het netwerk van het Ministerie van de Vlaamse Gemeenschap ingrijpende veranderingen en uitbreidingen ondergaan. Vroeger was er immers enkel een website, het opzet van de portal was veel ruimer. SBS, de vaste IT-dienstverlener van het Ministerie van de Vlaamse Gemeenschap, en Cisco bouwden het netwerk van het ministerie om tot een homogene, veilige en toekomstgerichte infrastructuur. De modulaire opbouw laat toe het geheel vlot uit te breiden en uitstekend te beveiligen. De basis voor een interactieve site is daarmee voorzien.

Via haar portaalsite www.vlaanderen.be zorgt het Ministerie van de Vlaamse Gemeenschap voor een betere online communicatie en brengt zo de administratie dichterbij de burger. In eerste instantie fungeert de portaalsite als informatiebaken met links naar de sites van de verschillende Vlaamse overheidsinstellingen. Op termijn krijgt ze een dienstverlenende functie. Burgers zullen dan online hun administratie afhandelen via zogenaamde e-loketten. Door e-government slinkt de papierberg en wordt de doorlooptijd voor allerlei verrichtingen korter. Kortom, de burger en de ondernemingen kunnen rekenen op een efficiëntere dienstverlening. Om vele toepassingen ook realiteit te laten worden, is het nog even wachten op de elektronische identiteitskaart. Die zal de online verrichtingen een officieel karakter geven.

De klok rond, zeven dagen per week

De organisatie van zo'n portaalsite is een complex gegeven. Godfried Verhamme van de Entiteit Sturing en Controle Informatie- en Communicatietechnologie bij het ministerie, legt uit: "De communicatie met de burger via het internet verloopt heel anders dan het directe contact met ambtenaren. De technische vereisten voor het netwerk liggen helemaal anders dan wanneer het enkel intern wordt gebruikt ter ondersteuning van de ambtenaren. Niet alleen moet het systeem een groot aantal bezoekers kunnen ondersteunen. Het contact moet de klok rond, zeven dagen per week gegarandeerd zijn. De computertoepassingen moeten dus ook buiten de arbeidsuren draaien. Dat heeft een enorme impact op alle componenten van de infrastructuur. Alles moet ontdebeld worden, tot en met de elektrische voorzieningen en de koeling in de computerruimte. Het

EXECUTIVE SUMMARY

Background

Via een portaalsite zorgt het Ministerie van de Vlaamse Gemeenschap voor een betere online communicatie om de administratie dichterbij de burger te brengen. In eerste instantie moet de site fungeren als informatiebaken met doorverwijzingen naar de websites van de verschillende Vlaamse overheidsinstellingen. Op termijn krijgt ze een uitgebreide, dienstverlenende functie.

Challenge

Voor de verwezenlijking van de portaalsite moest het netwerk van het Ministerie van de Vlaamse Gemeenschap ingrijpende veranderingen en uitbreidingen ondergaan. Er was nood aan een krachtige, schaalbare infrastructuur met een hoge beschikbaarheid. Het publieke en interactieve karakter van de site vergde ook een maximale beveiliging.

Solution

Cisco Systems en Siemens Business Services (SBS) bouwden een modulaire, ontdebeldde infrastructuur uit waarop de principes van Cisco's SAFE beveiligingsblauwdruk werden toegepast. Krachtige Cisco routers en Cisco Catalyst switches regelen het netwerkverkeer. Voor een optimale beschikbaarheid en een evenwichtige belastingsverdeling van het systeem, staan Cisco Content Services switches borg. De veiligheid is gegarandeerd met firewalls op twee niveaus, inbraakdetectiesystemen, ingebelde beveiligingsfuncties in de switches en een volledig afgeschermd netwerkbeheer.

Results

De portaalsite www.vlaanderen.be werd intussen gelanceerd. Het achterliggende netwerk is klaar om e-governmentdiensten te bieden. Ook toegang aan thuiswerkers en andere netwerken werd voorzien. Het hele systeem kan tot duizend gebruikers per onderdeel gelijktijdig ondersteunen en biedt een capaciteit van tien megabit per seconde (Mbps). Omdat Cisco alle benodigde toestellen voor zo'n complexe infrastructuur in zijn aanbod heeft, beschikt het ministerie over een veilig, schaalbaar en overzichtelijk netwerk. Dat vergemakkelijkt niet alleen het beheer, het ministerie heeft voor vragen en problemen slechts één aanspreekpunt.



hele netwerk is dan ook redundant: wanneer een onderdeel het laat afweten kan een ander het overnemen. Bovendien moet je erop toezien dat het netwerk schaalbaar is als bezoekersaantallen blijven groeien. Het moet zonodig uitgebreid worden met extra servers zonder dat er elders componenten moeten worden toegevoegd."

Ook op het vlak van beveiliging lagen de vereisten voor de portaal-site zeer hoog. Godfried Verhamme: "Je stelt je netwerk open voor de buitenwereld en moet je dus indekken tegen alles wat er kan mislopen. Het internet is gegroeid vanuit de academische wereld waar men werkte op een basis van vertrouwen. Het doel was samenwerken en informatie delen. Wie vandaag zijn netwerk openstelt, is automatisch ook bereikbaar voor slinkse amateurs en computercriminelen. Bovendien is een portaal-site gelaagd interactief. Sommige onderdelen zijn enkel bedoeld voor bepaalde gebruikersgroepen. Dat betekent dat je een goede echtverklaring en personalisatie moet kunnen doorvoeren. Bovendien heb je een dubbel netwerk nodig met een logische scheiding ertussenin: het ene deel geeft de buitenwereld toegang, het andere deel de interne medewerkers die bijvoorbeeld voor het onderhoud zorgen."

Overzichtelijke en veilige architectuur

Het vernieuwde netwerk omvat uiteindelijk zowat 200 gebouwen met 12.000 medewerkers en een tweeduizendtal mensen die van thuis uit kunnen werken. Zo'n uitgebreide infrastructuur vraagt om een helder ontwerp. Daarvoor zorgde Cisco, in samenwerking met SBS. Die laatste beschikte over de nodige kennis van het netwerk van het ministerie om te evalueren welke apparatuur in aanmerking kwam voor hergebruik en wat moest worden vervangen en uitgebreid. Cisco voegde daar zijn expertise op het vlak van netwerkbeveiliging aan toe, die beschreven staat in Cisco's SAFE-blauwdrukken. Die zetten de principes op een rijtje voor een vereenvoudigde, modulaire uitbouw van veilige e-business-systemen.

Het Ministerie van de Vlaamse Gemeenschap is al acht jaar een tevreden gebruiker van de producten van Cisco. "Onze infrastructuur is uitgebouwd door SBS op basis van Cisco routers, switches, firewalls en ander materiaal. De samenwerking is steeds goed verlopen, anders was Cisco niet al die tijd onze leverancier gebleven. Het contact met Cisco is vaak dynamisch en inspirerend. Het bedrijf weet als geen ander wat de best practices zijn bij het opstellen van een netwerkkarchitectuur. Ze leveren niet alleen routers en switches, maar ook load balancers, firewalls, intrusion detection systems en beveiligingsfuncties op alle onderdelen. Zo kan je van begin tot het eind een overzichtelijke, veilige infrastructuur uitbouwen. Cisco heeft dan ook een flink stuk meegedacht met SBS over het design van de nieuwe installatie. Er is een open relatie tussen ons ministerie, SBS en Cisco zodat we snel op problemen en uitdagingen kunnen inspelen," aldus Godfried Verhamme.

"Het oorspronkelijk netwerk bestond al voor negentig procent uit Cisco-apparatuur. Als je daar nog infrastructuur voor een portaal-site aan toevoegt, moet je hele goede redenen hebben om voor een andere leverancier te kiezen. In zo'n groot netwerk --we spreken hier van ongeveer 300 routers-- probeer je best zo homogeen mogelijk te werken. Je mensen hebben het voordeel van de ervaring met dergelijke platformen. Bovendien geeft het ministerie er de voorkeur aan om het aantal leveranciers en dus aanspreekpunten te beperken," vult Patrick Debois, systeemarchitect bij SBS aan.

Volledig ontdebeld

Met het oog op een hoge beschikbaarheid is de infrastructuur redundant gemaakt. De meeste componenten zijn dus dubbel uitgevoerd. Ook de verbinding met het internet is redundant. Er zijn twee connecties van tien Mbps via Belnet op twee verschillende locaties. Indien noodzakelijk kan de capaciteit zonder enige onderbreking tot 34 Mbps en meer opgetrokken worden. Voor de toegang tot de ruggengraat van het netwerk zorgen krachtige Cisco routers. De switching in het productiegedeelte gebeurt met Cisco Catalyst-clusters en voor de switching naar de servers worden Cisco Catalysts met een grote poortdensiteit gebruikt.

Om bezoekers van de site een snelle responstijd te garanderen en om de spreiding van het verkeer te optimaliseren, werd loadbalancing voorzien in het ontwerp. Daartoe zijn Cisco Content Services Switches (CSS) in de structuur opgenomen. De loadbalancers beschermen de achterliggende infrastructuur zonder de snelheid van het netwerk te verlagen. Ze controleren ook de beschikbaarheid van web servers en andere toestellen die de site ondersteunen. Op die manier vermijden ze dat surfers foutmeldingen te zien krijgen. Voorts analyseren ze voortdurend de binnenkomende verzoeken van surfers. In tegenstelling tot klassieke switches kunnen de loadbalancers daarbij met meer informatie rekening houden, zodat ze het gegevensverkeer veel efficiënter over het achterliggende netwerk kunnen sturen. Bezoekers van de site surfen dus vlotter. Het netwerk kan daardoor per onderdeel tot duizend gebruikers gelijktijdig ondersteunen en haalt over het intranet transfersnelheden tot 400 Mbps die kunnen worden opgetrokken tot 1 Gbps.

Twee sets load balancers Cisco regelen de spreiding van het verkeer over de firewalls en de web servers. De eerste set load balancers, geplaatst in het front-end gedeelte vòòr de firewalls van het eerste niveau, verdeelt de trafiek over die firewalls. De tweede set load balancers, achter de firewalls, spreidt het verkeer over de web servers. Zo krijgen gebruikers altijd een verbinding met een beschikbare server. Het is ook mogelijk om surfers zoveel mogelijk door te verwijzen naar dezelfde webserver. Zodra ze bekend zijn bij een toestel, verloopt de bediening immers sneller. De web servers zijn gegroepeerd in een eerste demilitarized zone (DMZ) die het publieke en het privé-gedeelte van het netwerk scheidt en bemiddelt tussen beide. Publieke gebruikers komen niet verder dan een eerste zone.



Ingebedde beveiliging

De firewalls van het tweede niveau --krachtige Cisco PIX toestellen die geen load balancing vergen-- isoleren het front-end gedeelte van een tweede DMZ. Die groepeerde de servers met de toepassingen en de databases. Die servers zijn bovendien extra afgeschermd van het netwerk via een intrusion detection system (IDS), net zoals in het publieke gedeelte van het DMZ.

Het beheer van de hele infrastructuur gebeurt via out-of-band management en de private VLAN beveiligingsfunctie op de switches. Private VLAN (Virtual Local Area Network, een onderverdeling van een netwerk op basis van andere dan fysieke criteria) laat toe om poorten op eenzelfde switch toch van elkaar te scheiden door ze onder te brengen in aparte groepen. Servers die verbonden zijn met verschillende private VLAN's, kunnen daardoor niet onderling communiceren. Hackers die toch op een bepaalde server zouden terechtkomen, krijgen dus geen toegang tot de andere servers die zijn aangesloten op dezelfde switch.

Bovendien gaat het beheerverkeer nooit via de ruggengraat van het netwerk, wel via eigen kanalen. Elk toestel in het netwerk beschikt dan ook over minstens twee netwerkkaarten: een voor het gewone dataverkeer en een voor het beheerverkeer. De beheerstations worden

van de rest van het netwerk geïsoleerd door een aparte firewall en een IDS. Het IDS inspecteert alle dataverkeer en activiteiten in het gehele netwerk op verdachte patronen. Zo spoort het systeem aanvallen op het netwerk of pogingen tot inbraak of geknoei op en kan het die voorkomen of in een vroeg stadium tegengaan.

In de toekomst zal het netwerk worden uitgebreid om partners en medewerkers buitenshuis betere toegang te bieden. Nu de basisarchitectuur van het netwerk klaar is, concentreert de Entiteit Sturing en Controle Informatie- en Communicatietechnologie zich op de ontwikkeling van standaarden. Alle diensten van het ministerie moeten voortaan immers de portaalsite als uitgangspunt nemen. Samen met SBS zorgt men ervoor dat alle nieuw ontwikkelde onderdelen passen binnen het grotere kader van de portaalsite. Gedurende die tweede fase kan de portaalsite volop groeien.



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: +33 1 58 04 60 00
Fax: +33 1 58 04 61 00

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco.com Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela

Copyright © 2001, Cisco Systems, Inc. All rights reserved.

Cisco Systems and the Cisco Systems Logo are registered trademarks, and Empowering the Internet Generation is a service mark, of Cisco Systems, Inc. and its affiliates in certain other countries.