Flexibiliteit en productiviteitsverbetering door robuust en veilig netwerk bij Inspectie van het Onderwijs

Om ervoor te zorgen dat een inspecteur van de Inspectie van het Onderwijs vanaf zijn werkplek thuis, of vanaf elke andere gewenste locatie, veilig en vlot rapportages kan versturen en bestanden kan downloaden, koos de Inspectie voor een veilige netwerkinfrastructuur van Cisco Systems. Vosko Networking B.V. verzorgde de implementatie van de oplossing.

De Inspectie van het Onderwijs houdt toezicht op alle scholen en instellingen in het primair onderwijs, het voortgezet onderwijs, het beroepsonderwijs en de volwasseneneducatie in Nederland. De Inspectie van het Onderwijs bestaat uit verschillende dependances die allemaal gebruikmaken van gevoelige informatie. Jacques Molendijk, Hoofd Automatisering, is verantwoordelijk voor de implementatie van het netwerk bij de Inspectie. Hij vertelt waarom de keus viel op de netwerkinfrastructuur van Cisco: “We vonden het oude netwerk te traag en de beveiliging voldeed niet meer aan onze hoge eisen. Toen de Inspectie een aantal regiokantoren samenvoegde met behoud van alle medewerkers, werd het netwerk ineens zwaarder belast. De capaciteit van de verbinding tussen ons hoofdkantoor in Utrecht en de grotere regiokantoren in het land was onvoldoende. Het internetgebruik en e-mailverkeer hinderden de bedrijfsapplicaties, wat erg traag en frustrerend werken was: bij elke toets die je indrukte, moest je even wachten voordat er op het scherm iets gebeurde.”

Eén leverancier: optimale samenhang

De Inspectie van het Onderwijs zocht één leverancier voor het verbeteren van het hele netwerk. Jacques Molendijk: “Cisco bleek de enige partij met een assortiment dat makkelijk is uit te breiden. Alle apparatuur van Cisco draait immers op hun eigen software (IOS) waardoor alles goed op elkaar aansluit. Bovendien had Cisco een passende oplossing voor de beveiliging van ons netwerk. Naast Cisco zijn BBned, als leverancier van de WAN-verbinding, en Vosko Networking B.V., die de implementatie op zich nam, bij het project betrokken. Vooraf hebben we met alle partijen een document opgesteld om de samenhang van alle componenten binnen de gehele infrastructuur vast te leggen. Ook hebben we precies vastgelegd welke partij waar verantwoordelijk voor is: dat scheelde een hoop vergaderen.”

Economisch gebruik bandbreedte

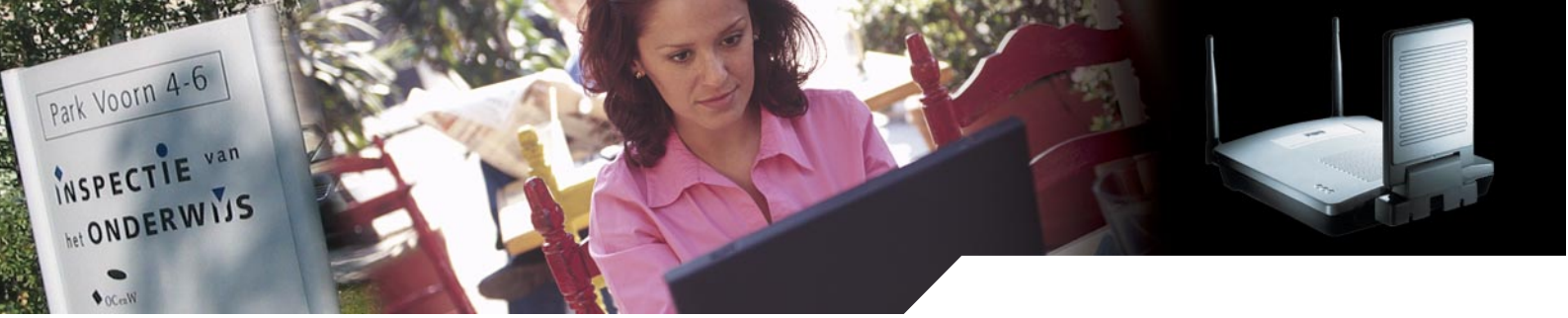
“In ons nieuwe netwerk gaan we heel kosteneffectief om met de bandbreedte,” vervolgt de heer Molendijk enthousiast. De Inspectie heeft nu de mogelijkheid de bandbreedte af te stemmen op incidentele, maximale behoeften. Dit gebeurt door optimaal gebruik te maken van de mogelijkheden van Quality of Service (QoS) in de Cisco routers. Quality of Service is een intelligente en flexibele manier om met bandbreedte om te gaan. De toepassing is te vergelijken met een verkeersagent die het dataverkeer regelt en onderscheid maakt tussen de soort databestanden die over het netwerk worden verzonden. Deze agenten geven voorrang aan het dataverkeer van bedrijfsapplicaties, vervolgens aan dat van de internetbrowser en e-mail en tot slot aan het dataverkeer om bestanden als back-up op te slaan. Hierdoor krijgt een bedrijfsapplicatie zoals Word, voorrang op bijvoorbeeld een e-mail met grote bijlagen. Op deze manier kunnen onze medewerkers ongestoord en snel doorwerken zonder dat we steeds bandbreedte hoeven bij te kopen. Bijkomend voordeel is dat de hardware sneller werkt. Het beheer van deze ‘verkeersagenten’ is heel gebruiksvriendelijk. Dit kunnen we zelf doen en dat scheelt in de kosten. De grootste besparing zit hem in het feit dat we met minder bandbreedte toekunnen omdat we er veel economischer mee omgaan. “

Verbluffende communicatie

Een ander aspect waar de heer Molendijk enthousiast over praat, is de draadloze verbinding tussen de hoofdvestiging en de decentrale vestiging in Utrecht: “Omdat het trekken van een kabel juridisch en logistiek gecompliceerd was, lag een draadloze verbinding voor de hand. Ik vind de kwaliteit van dit draadloze netwerk verbluffend; ik had interruptie verwacht, maar dat gebeurt niet. Een draadloze verbinding tussen de twee panden in Utrecht was ook nog eens goedkoper dan een vaste verbinding. De verbinding is zeer veilig omdat Cisco hiervoor extra, steeds wisselende, beveiligingssleutels heeft ingebouwd. Het is zelfs mogelijk om deze sleutel elke seconde te wijzigen, zodat het berichtenverkeer elke seconde op een andere manier wordt gecodeerd.”

Optimale beveiliging

Om toegang tot internet te krijgen, maakt de Inspectie gebruik van SURFnet, een internet provider die internettoegang via zeer hoge snelheden aanbiedt aan opleidingsinstituten. Jacques Molendijk: “De verbinding van de Inspectie naar SURFnet is fors verbreed tijdens het upgraden van het netwerk. Dat is prettig voor onze medewerkers, maar het biedt hackers ook een bredere toegangspoort. Daarom is de beveiliging hierop aangepast. Een Cisco firewall filtert nu al het verkeer op ongewenste binnendringers en laat deze dus niet binnen. Tegelijkertijd is er altijd een reserve firewall stand-by: voor het geval de actieve firewall uitvalt. Deze twee firewalls staan continu met elkaar in verbinding en kunnen de beveiliging op elk moment van elkaar



overnemen, zonder onderbreking.
De firewalls zijn gekoppeld aan een Intrusion Detection System (IDS) voor een veilige scheiding van het vertrouwde interne netwerk en het onveilige internet. Deze detector herkent ongewenst gedrag van schijnbaar correcte gebruikers en maakt het mogelijk om voor deze hackers meteen de toegang tot het interne netwerk te blokkeren. Mocht er een hacker actief zijn dan wordt dat direct gerapporteerd, inclusief de manier waarop de inbraak is verijdeld. In ons nieuwe netwerk hebben we dus niet alleen een 'parachute' voor de beveiliging, we hebben ook een aantal 'reserveparachutes'. Door deze robuuste beveiliging werd het mogelijk om de webserver die extern werd gehost naar het eigen hoofdkantoor te halen. Voortaan kunnen we dit zelf, veilig en wel. Hiermee besparen we tienduizenden euro's per jaar."

Werken op locatie

"Inspecteurs hebben vanaf elke locatie breedbandtoegang (ADSL of kabel) tot ons netwerk via internet. Met ons oude systeem konden inspecteurs wel al overal inbellen, maar dit gebeurde via een traag modem en een gewone telefoonlijn. De inspecteurs kunnen nu, door gebruik te maken van breedbandtoegang, hun rapporten vlugger aanmaken en zorgen dat zij vrijgegeven worden voor publicatie. Onlangs zijn de wettelijke eisen hiervoor nog aangescherpt. De ADSL-verbinding is beveiligd door het dataverkeer te versleutelen. Deze encryptie legt als het ware een tunnelverbinding via het internet tussen de inspecteur en ons centrale netwerk. Deze techniek staat bekend als Virtual Private Network (VPN). Het voordeel van een VPN systeem is dat het sterk is beveiligd, terwijl je gewoon en goedkoop gebruik kunt maken van bestaande, openbare infrastructuren, aldus de heer Molendijk.

Beheer in eigen hand

"Kortom: ons netwerk is aanzienlijk stabieler, veiliger, flexibeler, gebruiksvriendelijker, sneller en, last but not least, continu beschikbaar," concludeert Jacques Molendijk. "We zijn veel productiever geworden: kunnen sneller bedrijfsgegevens verwerken, sneller downloaden, sneller documenten van de server opvragen en sneller internetten. Mogelijke oorzaken van vertraging worden op voorhand opgelost. Allemaal zaken die de productiviteit ten goede komen. Terwijl de beveiliging relatief makkelijk maar zeer doeltreffend is geregeld. Onze medewerkers ontwikkelen en onderhouden het netwerk zoveel mogelijk zelf.

Beschermd tegen calamiteiten

In de toekomst gaan we via onze locatie in Eindhoven een tweede toegang tot SURFnet creëren. Door de inzet van VPN over SURFnet kunnen we tegen geringe kosten een uitwijkmogelijkheid creëren. Via de beveiligde VPN-tunnel versturen we 's nachts een back-up van alle data van onze bedrijfsapplicaties, de web- en e-mailserver van Utrecht naar Eindhoven. Dankzij de VPN-implementatie op ons netwerk maken we daarvoor gebruik van de bestaande lijnen van SURFnet. Mocht er in de vestiging van Utrecht bijvoorbeeld brand uitbreken waardoor de apparatuur daar onbruikbaar is geworden en we data kwijt zijn, dan is op de vestiging in Eindhoven een back-up van al onze data aanwezig. Via SURFnet kunnen we dan binnen een tot twee dagen alle locaties toegang tot deze back up in Eindhoven geven. Alle medewerkers hebben dan weer volledige beschikking over alle informatie die ze nodig hebben om gewoon door te werken."

Over de Inspectie van het Onderwijs

Het toezicht op het onderwijs wordt, zoals in de Grondwet is verankerd, uitgeoefend door de Inspectie van het Onderwijs. De Inspectie houdt toezicht op scholen en instellingen in het primair onderwijs, het voortgezet onderwijs, het beroepsonderwijs en de volwassenen-educatie. Het hoger onderwijs neemt een aparte positie in. Ook houdt de Inspectie toezicht op de zogenaamde expertisecentra. Dit zijn instellingen die speciaal gericht zijn op het geven van onderwijs aan leerlingen met leer- en gedragsstoornissen of gehandicapte leerlingen. Sinds 1 januari 2001 heeft de Inspectie ook toezicht op buitenschoolse cultuureducatie en amateurkunst.

Over Vosko Networking B.V.

Vosko Networking B.V. is een systeem integrator van datacommunicatie- en computernetwerken van ontwerp tot realisatie en verdere support. Vosko werkt met een omvangrijk team van specialisten en de nieuwste hoogwaardige technologieën. Sleutelwoorden hierbij zijn duurzaamheid en betrouwbaarheid.
Cisco Systems is de primaire technologiepartner op het gebied van netwerken.

Voor meer informatie kunt u terecht bij:

Public Relations
Karin van Geelen
Cisco Systems
T 020 - 357 3412
kgeelen@cisco.com
www.cisco.nl

Jacques Molendijk
Hoofd Automatisering
Inspectie van het Onderwijs
T 030 - 669 0600
j.molendijk@owinsp.nl
www.onwinsp.nl

Wim Coenen
director business development
Vosko Networking
T 0182 - 622822
sales@vosko.nl
www.vosko.nl

Technische bijlage

Centrale organisatie netwerk

De primaire processen van de Inspectie van het Onderwijs verlopen via een Wide Area Network (WAN). In feite knoopt het WAN via breedbandverbindingen van BBned de kleine netwerken op de verschillende locaties aan elkaar. De netwerkverbindingen naar Breda, Zwolle, Haarlem, Eindhoven, Zoetermeer en Groningen zijn ge-upgrade naar 2 Mbps. Vanuit alle locaties zijn deze programma's te gebruiken. Omdat de huurlijnen alleen voor de Inspectie van het Onderwijs toegankelijk zijn, is extra beveiliging op deze lijnen overbodig. Via een schotel is er een draadloze netwerkverbinding tussen het hoofdkantoor in Utrecht en de decentrale vestiging in Utrecht (Verderlaan). De capaciteit van de verbinding tussen deze twee panden is ge-upgrade naar 1 Mbps.

Cisco routers zorgen ervoor dat het dataverkeer op de juiste plaats aankomt. De router zoekt uit langs welke route de datapakketjes het snelste op de gewenste plaats van bestemming aankomen. De eigenlijke verbinding tussen de lokale netwerken van de verschillende gebouwen (LAN: Local Area Network) naar de hoofdvestiging vindt plaats via Cisco switches, die het dataverkeer analyseren en via een efficiënte verbinding doorsturen.

Behalve de bandbreedte van de verbindingen is ook de capaciteit van de servers ge-upgrade. Dankzij de upgrade van de servers kunnen programma's sneller worden opgeroepen, ook als veel medewerkers op hetzelfde moment van hetzelfde programma gebruikmaken.

SAFE blauwdruk

Voor de inrichting van de beveiliging van het netwerk heeft de Inspectie gebruik gemaakt van de Cisco SAFE blauwdruk. Hierdoor wordt optimaal gebruik gemaakt van de mogelijkheden van moderne security apparatuur, waardoor er veel tijd en geld bespaard wordt.

Een firewall controleert al het dataverkeer tussen het netwerk en internet en onderschept alle verdachte of niet toegestane pakketjes. Een hacker die een netwerk wil binnendringen of saboteren wordt zo tegengehouden. Een tweede firewall is stand by mocht de eerste firewall (tijdelijk) uitvallen. Behalve via een firewall is het netwerk van de Inspectie beveiligd met een IDS Sensor. Deze sensor herkent gebruikers die op het netwerk actief zijn (dus al zijn binnengelaten) maar die zich alsnog tot een hacker ontpoppen. De sensor heeft duizenden patronen van hacker-gedrag in zijn database om deze malafide gebruikers op te sporen. De database wordt regelmatig ge-update met patronen van hackergedrag. Heeft de sensor een gebruiker opgespoord, dan blokkeert hij het IP-adres van de hacker zodat deze geen toegang meer krijgt tot het netwerk.

Veilig en voordelig toegang via VPN

SURFnet verzorgt internettoegang via zeer hoge snelheid aan de Inspectie van het Onderwijs. Ook hier vervullen Cisco switches een schakelfunctie in het tot stand brengen van de verbinding. De toegangslijn tot SURFnet is ge-upgrade tot een razendsnelle gigabitverbinding.

Inspecteurs kunnen overal in het land via een breedbandverbinding toegang krijgen tot het netwerk van de Inspectie. Deze verbinding komt tot stand via internet. Om de informatie van de Inspectie te beveiligen tegen ongeautoriseerd gebruik, werkt de Inspectie via een VPN (Virtual Private Network). Een VPN Concentrator zorgt ervoor dat er een tijdelijke beveiligde 'privé-verbinding' wordt gelegd over het openbare internet waarover inspecteurs veilig data kunnen uitwisselen. Tot slot is er een ACS, Acces Control Service, die controleert of medewerkers geautoriseerd zijn voor programma's en voorzieningen alvorens ze toe te laten. De Acces Control Service maakt deel uit van de loginprocedure van elke medewerker van de Inspectie.