

Cisco IronPort

waakt over de Cloud

Cisco IronPort beschermt de randen van het bedrijfsnetwerk, waar bedreigingen aan de poorten staan. De randen van het netwerk zijn echter al lang niet meer de grenzen van het netwerk. "Doordat applicaties op afstand en via internet gebruikt worden, verdwijnen de grenzen. En de controle. Wij geven security managers weer de regie, ook in de wereld van Cloud Computing," zegt Jeroen Arends, SE Benelux van Cisco IronPort.

Beveiligingsbeheerders staan momenteel voor een groot probleem. Hoe kan men gebruikers op afstand controleren op zaken die ze op remote applicaties en devices doen? "We beschermen interne gebruikers al jaren bij veilig e-mail- en internetgebruik," zegt Arends. "Die kennis en ervaring passen we nu toe in het Cisco Borderless Networking-concept. Daarmee bieden we diezelfde beveiliging bij het gebruik van Cloud Computing en SaaS-diensten. Tenslotte wordt er tegenwoordig steeds vaker buiten het bedrijf en buiten het bedrijfsnetwerk gewerkt met bedrijfsgegevens. Dan is het beheer en beveiligen van gebruikers heel lastig."

Daarbij zijn volgens Arends twee scenario's denkbaar. "In het eerste scenario krijgen de

medewerkers via een VPN-verbinding veilige toegang tot het interne netwerk, de applicaties en de gegevens. Maar als zij gebruik willen maken van internet, moet dat via een VPN-verbinding tussen het interne netwerk en internet. Dat brengt het nadeel met zich mee dat gebruikers op afstand via internet naar het bedrijfsnetwerk gaan en van daaruit weer naar internet. Zodoende worden de netwerkverbindingen twee keer belast. Bovendien moet men twee keer inloggen: een keer voor de VPN-verbinding en een keer voor het bedrijfsnetwerk."

Cisco IronPort lost dit probleem op met appliances die voorzien zijn van het Security Assertion Markup Language (SAML)-protocol. Dit is een op XML gebaseerde open standaard voor het

uitwisselen van authenticatie- en autorisatiegegevens tussen beveiligingsdomeinen. Bijvoorbeeld tussen een bedrijfsnetwerk en een webservice. SAML biedt de mogelijkheid om interne gebruikersgegevens en -rechten ook toe te passen op de autorisatie bij online applicaties. De appliance van Cisco IronPort verzorgt de communicatie tussen online applicaties en de interne Active Directory. Zodoende worden online accounts van medewerkers aangemaakt met hun interne inloggegevens."

In het tweede scenario maakt de organisatie de accounts aan bij Cloud- of SaaS-diensten voor de medewerkers. De verbinding tussen de gebruiker op afstand en de online applicatie is dan direct, wat de VPN-verbinding ontlast. "De organisatie moet dan echter voor al die

medewerkers de online gebruikeraccounts beheren, wat bijzonder omslachtig is," weet Arends. "Met de integratie van Scansafe en IronPort is dat niet meer nodig. De gebruiker wordt dan namelijk niet beveiligd vanuit de interne Active Directory, maar bij de Cloud- of SaaS-dienst zelf. Scansafe is een SaaS-dienst die bescherming biedt door het filteren van downloads en URLs. Voor mobiele apparaten is Scansafe gecombineerd in de AnyConnect VPN-client die men kan downloaden als App. Inloggen vanaf de smartphone gebeurt dan altijd via een rechtstreekse en versleutelde verbinding met Scansafe. Ook als men met de smartphone gebruik maakt van een browser, wordt het verkeer door AnyConnect onderschept en via Scansafe geleid en gecontroleerd." ●●

Cisco IronPort beschermt gebruikers en gegevens

De C-Serie appliances van Cisco IronPort beveiligen e-mailgebruikers tegen virussen, spam en kwaadaardige content. De S-Serie appliances voor internetbeveiliging bieden een gelaagde verdediging tegen internetbedreigingen. URL-filters zien toe op het naleven van bedrijfsbeleid over welke websites wel of niet bezocht mogen worden. De Cisco Security Intelligence Operations, Cisco IronPort Web Reputation Filters en het Cisco IronPort Anti-Malware System bieden bescherming tegen webgebaseerde malware. Bovendien biedt de leverancier hiermee de mogelijkheid om uitgaande gevoelige en vertrouwelijke gegevens te filteren. De oplossingen voor e-mail- en internetbeveiliging worden aangevuld door de M-Serie appliances voor beveiligingsbeheer. Deze bieden centraal beheer, opslag en controle van alle beleidsregels van een organisatie.

De appliance van Cisco IronPort waken ook voor verlies of diefstal van vertrouwelijke of gevoelige gegevens. Hiervoor is een Data Loss Prevention (DLP)-oplossing geïntegreerd die e-mail berichten scant en voorkomt dat vertrouwelijke gegevens worden uitgestuurd. DLP maakt het ook onmogelijk om vertrouwelijke gegevens te uploaden naar internet of sociale media-applicaties zoals Facebook en Twitter.