Achter de Great Firewall van China

Machines beheren op plekken waar internet gecensureerd is

Er zijn op de wereld een aantal landen waar internet zwaar gecensureerd wordt zodat sites als Facebook en Google niet bereikbaar zijn. Alleen door de overheid goedgekeurde sites mogen bekeken worden. Voor de inwoners van die landen, is dit een vervelende zaak, maar zelfs voor ons kan deze censuur gevolgen hebben.

China, maar ook Iran en Noord Korea zijn maar een aantal landen waar internet niet vrij toegankelijk is. In deze landen bepaalt de overheid wat wel en niet op internet bekeken mag worden en met name sites als Facebook en Twitter zijn taboe. Nu zijn voor ons de laatste twee landen niet echt zo belangrijk, omdat er ook geen belangrijk economisch verkeer bestaat, maar bij China ligt dat anders. Heel veel westerse bedrijven laten de meest geavanceerde producten in China maken die volledig voldoen aan alle richtlijnen en die vaak ook geproduceerd worden met machines die door machinebouwers in Europa vervaardigd zijn.

Nu weet u dat het ondertussen vrij gebruikelijk is dat machines uitgerust worden met een netwerkverbinding zodat de PLC op afstand via internet toegankelijk is. Software, statusmelding en meetdata kunnen zo door de machinebouwer bij storingen vanuit zijn eigen kantoor uitgelezen en aangepast worden zonder dat hij daarvoor naar het andere eind van de wereld hoeft te reizen. De voordelen hiervan mogen duidelijk zijn, maar gaan alleen op als de verbinding met de machine via een veilige weg loopt en niet geblokkeerd wordt door een overheid die anders over het gebruik van internet denkt dan wij hier in het westen.

Golden Shield Project

Iedereen kent de Chinese muur als een bouwwerk uit lang vervlogen tijd. De muur heeft al lang geleden zijn functie verloren, maar hij heeft ondertussen een modern elektronisch broertje gekregen, namelijk de minder zichtbare maar net zo aanwezige grote Chinese Firewall, officieel bekend als het 'Golden Shield Project'. In de afgelopen jaren heeft China de technologie achter de grote Chinese Muur verder ontwikkeld om nu ook Virtual Private Network (VPN) verbindingen te blokkeren. Deze verbindingen worden immers veelal gebruikt om op een veilige manier met een machine te kunnen communiceren en te voorkomen dat hackers ongewenst toegang krijgen tot de machine. Voor de machines in China werd daarnaast de VPN-verbinding gebruikt om zo de grote Chinese Firewall te omzeilen.

Nu het ook niet meer mogelijk is om een betrouwbare VPN-verbinding op te kunnen bouwen, kunnen machinebouwers en system integrators geen service meer op afstand verlenen. Men moet weer in het vliegtuig stappen voor elk wissewasje, hetgeen tijd en geld kost.

Wie nu denkt dat de Chinese overheid wel gevoelig is voor de argumenten van de machinebouwer, die heeft het mis. Via de VPN-verbinding is het immers mogelijk om ook sites als Facebook te bereiken en dat is nu juist wat de Chinese overheid niet wil.

Stunnel

Voor één van Nederlands grootste machinebouwers was het een groot probleem dat VPN niet meer betrouwbaar werkte. Door gebruik te maken van de IXrouter, waren zij gewend om hun machines op afstand te beheren om snelle en betrouwbare service te kunnen verlenen aan klanten wereldwijd. Omdat zij niet langer op afstand toegang hadden tot de PLC's, HMI's of andere op het netwerk aangesloten hardware, waren zij niet langer in staat om klanten in China dezelfde service te bieden. Het probleem werd voorgelegd aan IXON, fabrikant van de IXrouter. IXON kwam tot de conclusie dat zodra de grote Chinese Firewall OpenVPN data detecteert, de verbinding geblokkeerd wordt. Na diverse mogelijkheden te hebben getest, bleek het gebruik van stunnel uitkomst te bieden. Stunnel is een open-source multi-platform computerprogramma dat gebruikt wordt om een universele TLS/SSL- tunneling service te bieden. Met behulp van stunnel worden OpenVPN datapakketten via Secure Sockets Layer (SSL) nogmaals versleutel. De stunnel verbinding tussen de IXrouter en de IXserver kan enkel worden gebruikt voor het versturen en ontvangen van service data voor de machine. Dat deze verbinding niet geschikt is voor reguliere internetdoeleinden, maakt het tot een alternatief dat wel wordt toegelaten.

In samenwerking met een lokale partner in China werd getest of de IXrouter vanuit China een beveiligde verbinding op kon stellen met de bijbehorende IXserver in Europa. Deze testen bleken succesvol waardoor machinebouwers hun klanten wereldwijd wederom snelle en lokale service op afstand kunnen bieden - ook in China.

In de router

Ten opzichte van de normale VPN-verbinding, is er eigenlijk niet zoveel anders. Het enige verschil is dat er nu een stunnel-laag tussen is gekomen. Zoals in figuur 1 is te zien, is elke machine via een VPN-verbinding gekoppeld aan een centrale server. Voor het gebruik van stunnel moet zowel de server zijn uitgebreid met de coderings- en decoderingssoftware. De IXrouter is hiervoor geschikt gemaakt wat inhoudt dat er bij de machine simpelweg een geüpdate router geplaatst moet worden die de verbinding over internet via stunnel laat lopen naar een server die ook stunnel verstaat.

De toekomst

Omdat elke beveiligde internetverbinding waaronder internetbankieren gebruik maakt van SSL, is de kans groot dat het gebruik van stunnel nog lange tijd wordt toegelaten en dit een goede weg is om door de Chinese firewall heen te komen. Ook China weet immers dat banken een grote macht hebben en dat in feite de hele wereld draait om geld.

Voor meer informatie zie www.etotaal.nl/achtergrond. Artikel "Achter de Great Firewall van China".

Ewout de Ruiter

Figuur 1. Om stunnel te kunnen toepassen, moet de server en de router zijn voorzien van de software voor deze coderingsmethode.