OPEN VPN-NL CODEMO PROJECT

OP WEG NAAR EEN BETAALBARE EN EENVOUDIGE LGI-CRYPTO

Dhr. A. (Antoine) Wittebols, Senior Innovation Manager DMO/JIVC/KIXS

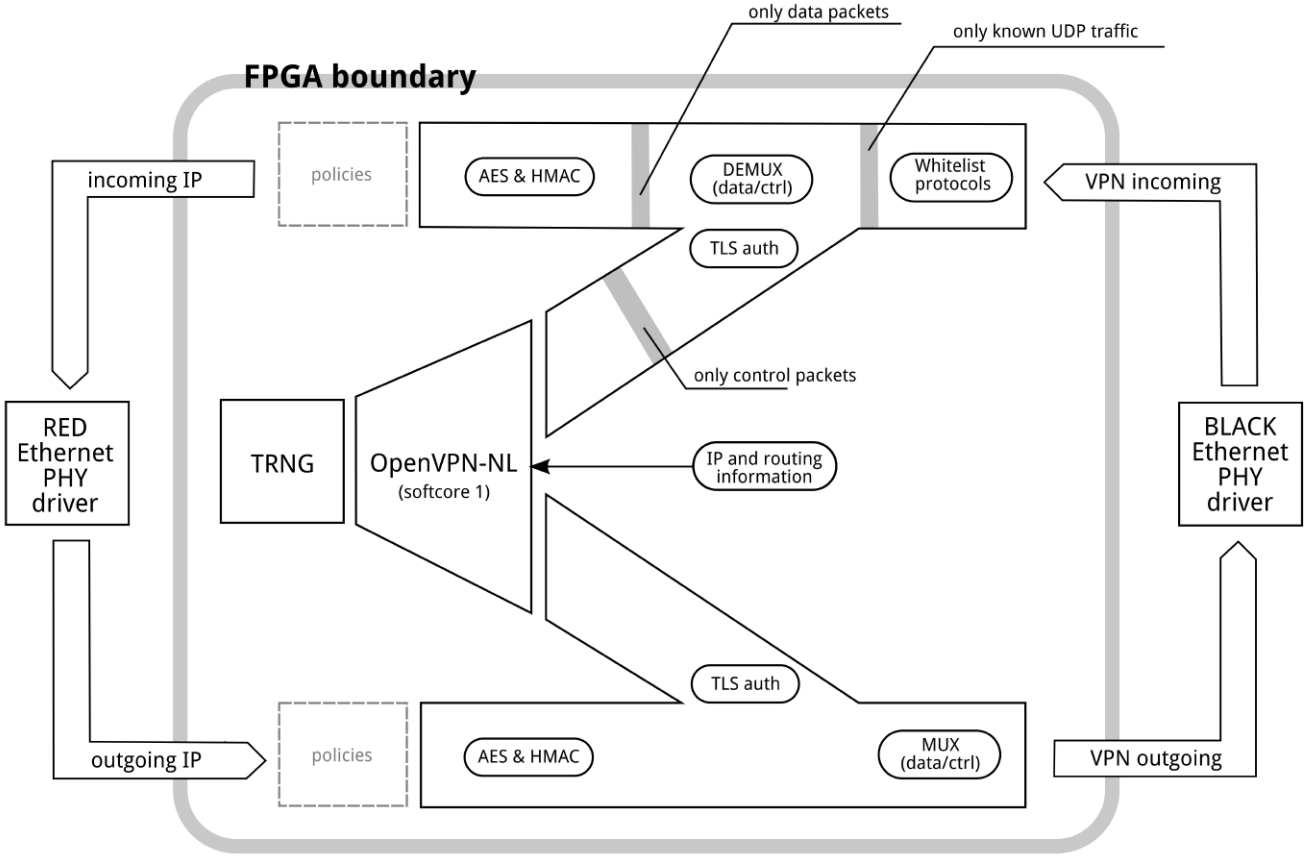
Er is een steeds grotere behoefte binnen defensie om Departementaal Vertrouwelijke Informatie (DVI) tussen systemen op een veilige manier uit te wisselen, veelal ondersteund door cryptografische toepassingen. Maar de hardware crypto oplossingen die hiervoor op de markt beschikbaar zijn, bevatten vaak een overkill aan functionaliteit, zijn kostbaar en vergen een aanzienlijke beheerinspanning. Dit heeft ertoe geleid dat KIXS in 2016 een innovatieproject is gestart om middels een *demonstrator* aan te tonen dat door het implementeren van geaccrediteerde OpenVPN-NL crypto software in programmeerbare chips *(Field Programmable Gate Array, FPGA)*, *crypto appliances* kunnen worden ontworpen die een stuk betaalbaarder en eenvoudiger in gebruik zijn. →

Het Nederlandse bedrijf Technolution dat betrokken was bij het innovatieproject heeft eind 2016 een aanvraag bij de Commissie Defensie Materieel Ontwikkeling (CODEMO) ingediend en is sinds januari 2017 volop bezig om samen met defensie deze *demonstrator* tot een bruikbaar eindproduct te ontwikkelen.

De start: KIXS innovatieproject

Defensie gebruikt op dit moment verschillende merken en types cryptoapparaten voor de beveiliging van haar informatie. Dit zijn vaak kostbare apparaten vanwege de security en functionele eisen die hieraan gesteld worden; eisen die noodzakelijk zijn bij inzet voor beveiliging van Hoog Gerubriceerde Informatie (HGI). Maar ook Laag Gerubriceerde Informatie (LGI) wordt steeds vaker beveiligd met crypto. Mogelijke toepassingen voor LGI cryptoapparaten zijn onder meer het beveiligen van NAFIN-uitlopers en TITAAN ZWART verbindingen. Voor het niveau Departementaal Vertrouwelijk (DepV) is vrij op de markt te verkrijgen crypto (business crypto) niet voldoende en de huidige beschikbare goedgekeurde DepV crypto's zijn vaak een afgeleide van crypto's voor hogere niveaus en bevatten een scala aan functionaliteiten die niet gebruikt worden.

De toenemende behoefte aan LGI crypto's heeft ervoor gezorgd dat beheerders ook meer op zoek zijn naar LGI crypto's die eenvoudiger geconfigureerd, ingezet en beheerd kunnen worden dan de huidige cryptoapparaten. KIXS heeft daarom begin 2016 een innovatieproject opgestart waarbij een al in gebruik zijnde geaccrediteerde software-oplossing voor DepV – OpenVPN-NL – in hardware wordt gerealiseerd zodat een robuustere implementatie en betere performance tegen lagere kosten bereikt kunnen worden. In een Proof-of-Concept (PoC) zijn uiteindelijk de belangrijkste componenten van OpenVPN-NL code in een FPGA geïmplementeerd op een demoboard. Bij de PoC spelen twee belangrijke onderzoeksvragen een rol: heeft de oplossing inderdaad een acceptabele performance en welke stappen moeten ondernomen worden



Figuur 1: High Level Design Open VPN-NL Hardware (gebaseerd op FPGA)

OpenVPN-NL

OpenVPN-NL is een geharde versie van OpenVPN, een open source VPN software product, dat dankzij een aantal aanpassingen een versterkte beveiliging biedt. Dit wordt gerealiseerd door een aantal patches en verbeterde documentatie. OpenVPN-NL voldoet hiermee aan alle evaluatiecriteria van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen- en Veiligheids Dienst (AIVD) voor de verwerking van vertrouwelijke informatie tot op het niveau van Departementaal VERTROUWELIJK. OpenVPN-NL wordt bij defensie gebruikt om een veilige verbinding op te zetten met de Telestick en de smartphone naar de MULAN omgeving.

Figuur 2: PrimeLink 3015 in 19" uitvoering (gebaseerd op FPGA)

om tot een productwaardige oplossing te kunnen komen?
Het gehele ontwerp is uiteindelijk in opdracht van KIXS beoordeeld door het bedrijf Technolution. De conclusie is dat het implementeren van OpenVPN-NL in een FPGA met een toereikende performance zeker haalbaar is.
De PoC heeft daarnaast waardevolle inzichten en informatie opgeleverd met betrekking tot de behoeften van de doelgroep, de architectuur van het toekomstige product, een conceptueel *Very High-speed Integrated Circuit Hardware Description Language* (VHDL) implementatie en een validatie framework. Maar tegelijkertijd is er nog veel doorontwikkelingswerk noodzakelijk om van een *demonstrator* tot een productwaardige oplossing te komen.

Het vervolg: CODEMO

Behalve de doorontwikkeling zijn nog andere zaken van belang zoals support- en lifecyclemanagement op het moment dat het product verkrijgbaar is. Iets waar de markt meer ervaring mee heeft dan een innovatieafdeling bij defensie. Gelukkig was Technolution – dat eerder betrokken was bij het innovatieproject – zo enthousiast dat ze een CODEMO-aanvraag indiende om de demonstrator door te ontwikkelen naar een bruikbaar product.

Bij CODEMO vergoedt Defensie 50% van de projectkosten en vraagt ze een royalty per verkocht product (met een bepaald plafond en/of tijdsduur). Naast de vergoeding van een deel van de kosten levert defensie ook gedurende het project input van bijvoorbeeld gebruikers (veelal beheerders) zodat het product zo optimaal mogelijk kan worden afgestemd aan de eisen en wensen.
KIXS is begeleider van het CODEMO-project dat begin 2017 van start is gegaan en aan het einde van dit jaar zal worden afgerond met de oplevering van een bruikbaar OpenVPN-NL hardwareproduct.

Figuur 3: PrimeLink 3015 als desktop uitvoering

Het resultaat: PRIMELINK 3015

Vanaf begin 2017 is Technolution voortvarend te werk gegaan en heeft middels verschillende gebruikersgroepsessies met defensiegebruikers (OPS en SATS) requirements verzameld met betrekking tot gebruik, beheer, techniek en security. Ook buiten Defensie (verschillende andere ministeries) is er interesse voor het product en die potentiële klanten worden uiteraard ook betrokken bij de ontwikkeling. In juni is het elektronisch ontwerp voor Printed Circuit Board (PCB) afgerond en de eerste prototypes worden eind augustus verwacht. Een aantal defensieonderdelen zal dan tests uitvoeren om te kijken of het product voldoet aan de verwachtingen.
Inmiddels heeft het product ook een naam gekregen: PrimeLink 3015.
Het zal één van de producten zijn uit JelloPrime, een pakket hoogwaardige securityproducten en -diensten van Technolution. De eerste versie van PrimeLink zal begin 2018 geleverd kunnen worden in twee uitvoeringen: een 19" uitvoering voor *dataracks* en een desktopvariant. Deze eerste versie heeft een maximale snelheid van 1 Gbit/s (met zowel elektrische als optische ingangen). Later zal - door een eenvoudige *firmware upgrade* - hetzelfde apparaat snelheden tot 10 Gbit/s aan kunnen. Het apparaat is inzetbaar zowel op laag 2 (Ethernet) als laag 3 (IP). Sleutelmanagement geschiedt door een *Crypto-Ignition Key* (CIK). De verkoopprijs van het product is beduidend lager dan die van bestaande DepV crypto's. Als ook uit de veldtesten blijkt dat het eindproduct voldoet aan de eisen van defensie, dan heeft defensie een betaalbare en eenvoudige LGI crypto binnen handbereik!

Meer informatie over het product is te vinden op www.jelloprime.com.

VHDL en FPGA

VHDL staat voor Very High-speed Integrated Circuit Hardware Description Language en is een hardware beschrijvingstaal waarmee digitale schakelingen en programmeerbare logica (zoals FPGA's) kunnen worden beschreven en gemodelleerd. Oorspronkelijk is de programmeertaal ontworpen door het Amerikaanse Department of Defense maar het is inmiddels wereldwijd een veel gebruikte taal voor digitale schakelingen. FPGA staat voor Field-Programmable Gate Array en is een geïntegreerde schakeling bestaande uit programmeerbare logische componenten, die geprogrammeerd kunnen worden als logische functies (bijv. AND, XOR).