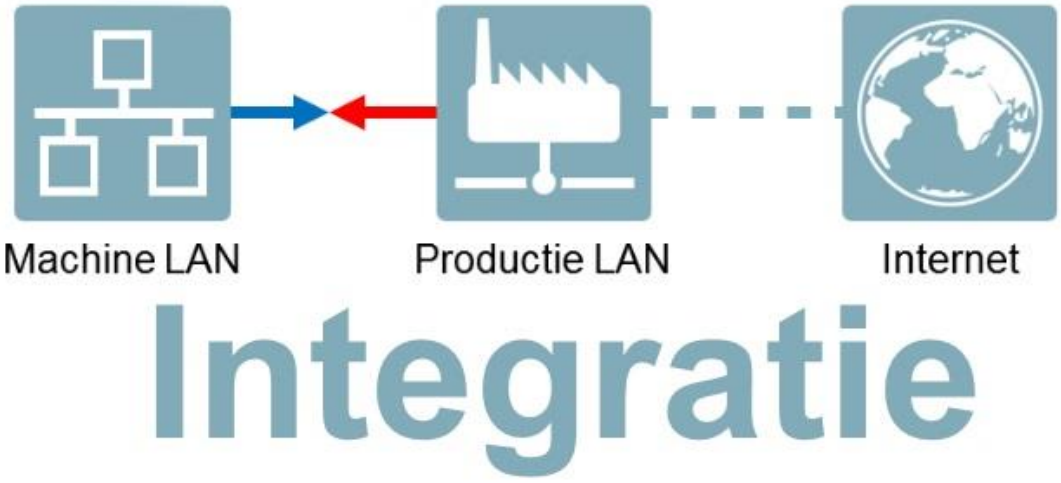


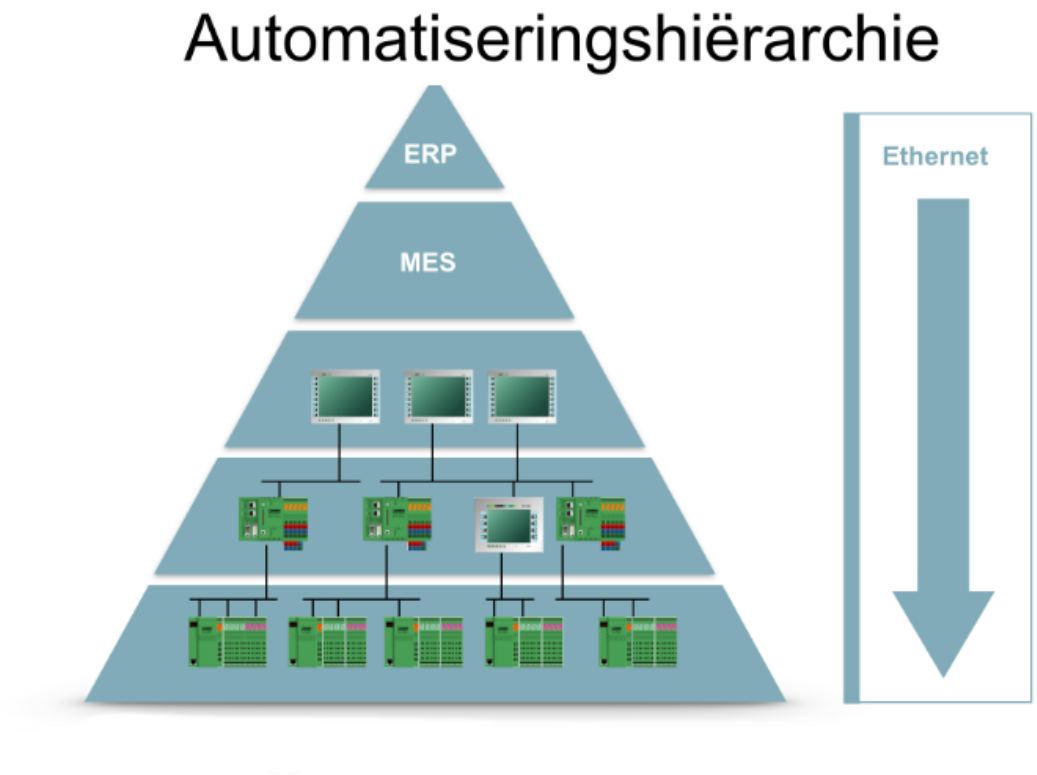
Sjoerd Hakstege - van Eekhout
Network & Security Specialist at Phoenix Contact

Volgen

Vervolg: Uw Machines integreren in een bestaand netwerk?

Op 26 maart jl. heb ik tijdens het Industrial Ethernet Event in het Evoluon een presentatie mogen geven over hoe je op een veilige en efficiënte manier één of meerder machines kunt integreren in een bestaand netwerk. In deze post zal ik dit nogmaals uiteenzetten.

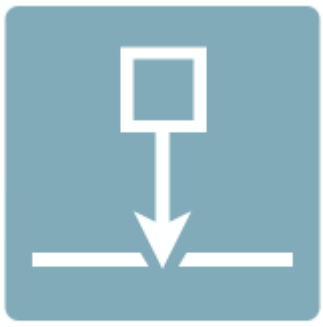
Laten we beginnen met de opkomst van Ethernet binnen de industrie. Wanneer we kijken naar de traditionele automatiseringshiërarchie dan is deze op te delen in 5 lagen, beginnend bij het Enterprise Resource Planning systeem eindigend op I/O niveau.



Tot op SCADA niveau was Ethernet al geruime tijd gemeengoed, maar op I/O niveau is dit nog niet altijd het geval. Wel staat vast dat met de opkomst van Ethernet binnen de Industrie er veel voordelen zijn op het vlak van transparante communicatie en diagnose. Maar er is ook een keerzijde; IP adressen dienen afgestemd te worden, netwerken dienen gekoppeld te worden en dan het liefst ook nog middels een firewall zodat u ook met het oog op cybersecurity maatregelen heeft getroffen.

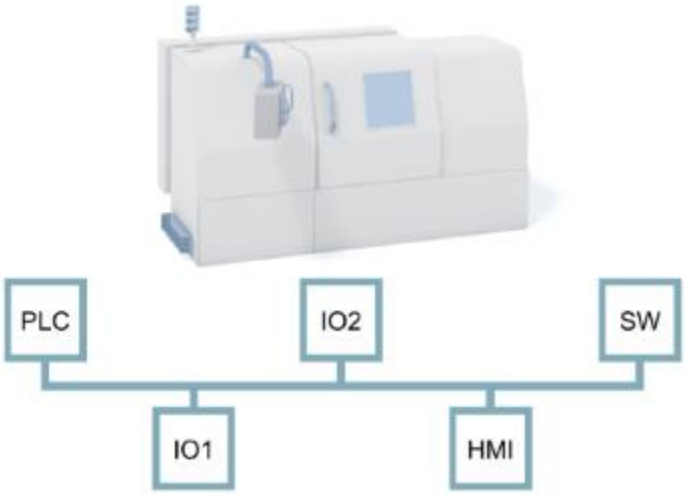
Wanneer we naar een productiehal kijken dan vinden we daar tal van machines die allemaal informatie uitwisselen met de bovenliggende systemen. Bij de integratie van deze machines binnen het netwerk kunnen we 3 aandachtspunten definiëren:

- Integratie: hoe kan ik de machine opnemen in het netwerk
- Security: welke maatregelen kan ik nemen om de machine te beschermen tegen kwaadaardige software
- Remote access: Hoe kan ik van afstand deze machine servicen?



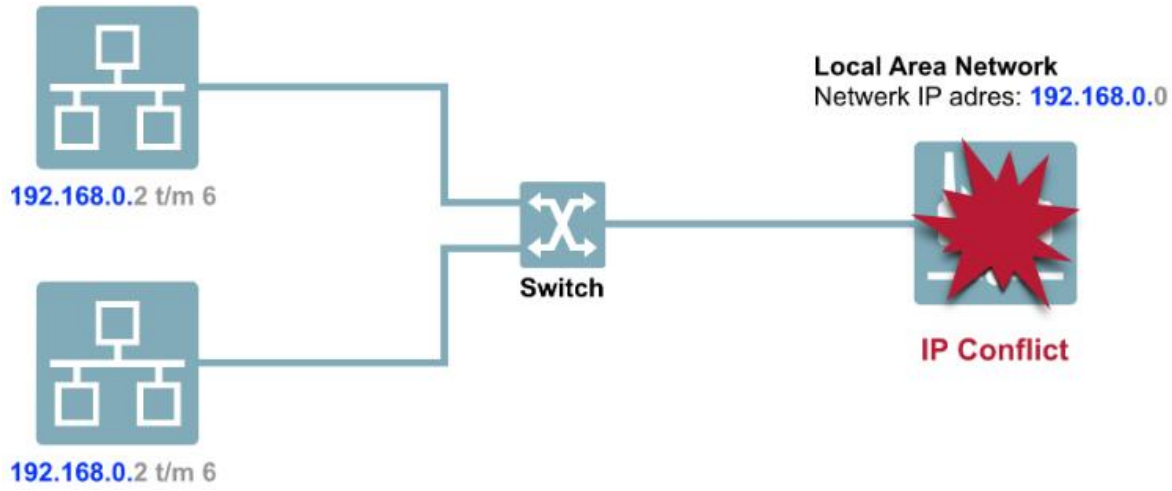
Integratie

Moderne machines hebben tegenwoordig tal van ethernet deelnemers, denk hierbij aan de PLC, IO systemen (bijv. Profinet), gemanagede switches, HMI's etc etc. Tijdens de productie van de machine worden de IP nummers door de fabrikant ingesteld zodat alle onderdelen van de machine vlekkeloos samenwerken. In dit voorbeeld gaan we uit van een 5-tal deelnemers welke in het ***192.168.0.0.*** subnet zijn ingesteld. N.B. in deze post heeft ieder subnet een eigen kleur en wordt er soms ook gerefereerd aan deze kleur i.p.v. de IP nummers.



- **PLC** : 192.168.0.2
- **IO station 1** : 192.168.0.3
- **IO station 2** : 192.168.0.4
- **HMI** : 192.168.0.5
- **Switch** : 192.168.0.6

Kortom, moderne machines zijn kleine LAN netwerken op zich en wanneer we twee van dergelijke machines willen integreren binnen hetzelfde netwerk krijg je uiteraard te maken met IP-conflicten.

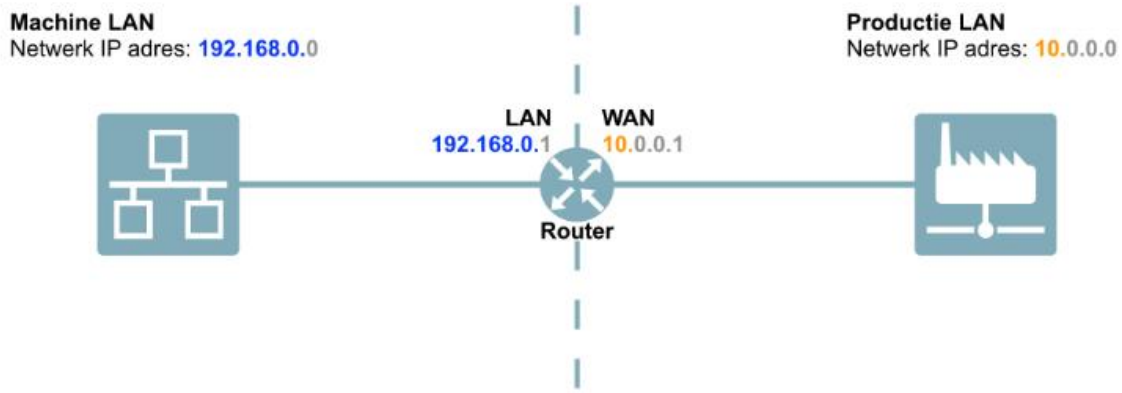


Welke oplossingen zijn er voor dit probleem? U kunt natuurlijk de IP nummers van één van de machines aanpassen zodat ze weer uniek zijn, maar dit heeft een paar flinke nadelen:

1. Het kost veel tijd om alle IP nummers aan te passen
2. PLC programma's moeten aangepast worden omdat de I/O modules ook een ander IP adres hebben gekregen
3. De machine is lastiger te onderhouden omdat de IP nummers per machine verschillend zijn, denk hierbij aan het uitwisselen van een IO station of het uitlezen van de PLC met een servicelaptop.

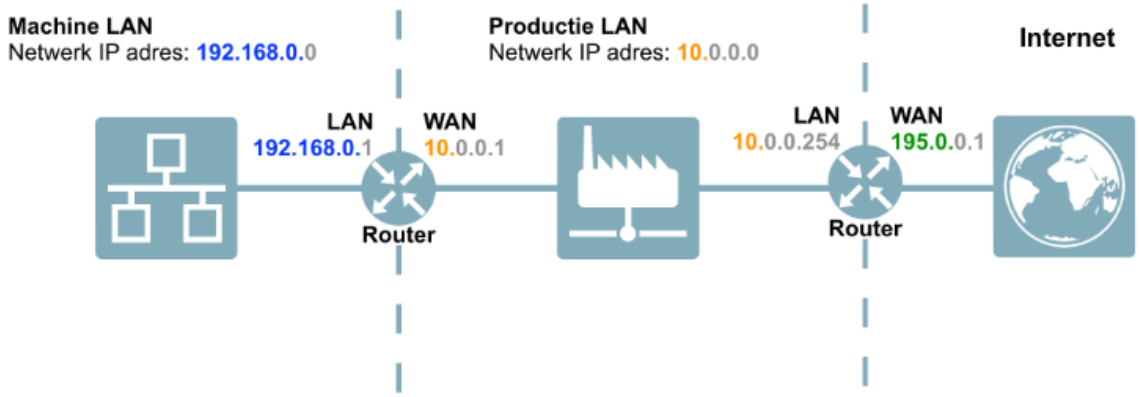
Een router misschien? Routers zijn immers ideaal om twee netwerken met elkaar te verbinden. Laten we eerst eens kijken wat een router precies doet. Een router leest bij het ontvangen van een ethernet pakket het IP adres en het poort nummer en beslist op basis van deze gegevens waar het pakket naartoe gestuurd moet worden.

Stelt u zich twee netwerken voor, een "blauwe" en een "oranje":



De twee netwerken zijn middels een router met elkaar verbonden. Wanneer een deelnemer uit het blauwe netwerk wil communiceren met een deelnemer in het oranje netwerk dan zal hij de berichten aan de router moeten richten. Dit zal hij doen indien de zogeheten "default gateway" ingesteld staat op het IP adres van de router: ***192.168.0.1.***

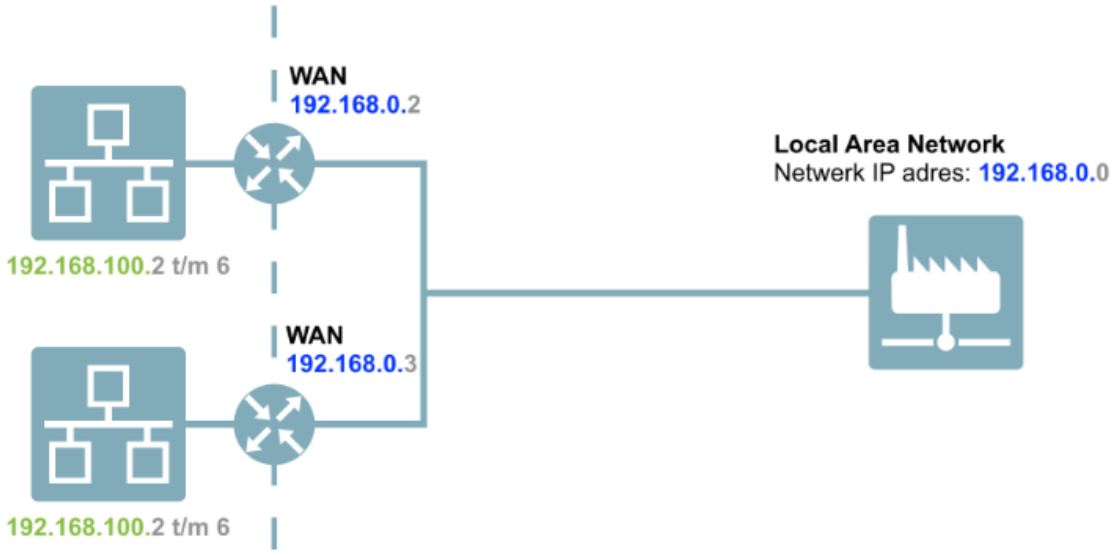
Andersom dienen de deelnemers in het oranje netwerk een default gateway te hebben met IP ***10.0.0.1.*** Wanneer de pakketten ontvangen worden door de router zal deze op IP-niveau kunnen zien waar de pakketten naartoe moeten. Maar wat als er nog een derde netwerk bij komt?



Elke ethernet deelnemer kan maar 1 default gateway hebben en we hebben gezegd dat de deelnemers uit het oranje netwerk als default gateway IP-adres ***10.0.0.1.*** hebben. Als een deelnemer uit het oranje netwerk nu wil communiceren met een deelnemer op het internet dan zullen deze pakketten dus naar IP ***10.0.0.1.*** worden gestuurd, echter heeft deze router geen toegang tot het internet en weet dus niet waar deze pakketten naartoe moeten. Om dit op te lossen kan men gebruik maken van zogeheten "static routes". Dit houd in dat er in de router ingesteld kan worden achter welk IP adres zich een volgend netwerk bevind.

In ons voorbeeld is het aan te bevelen dat de deelnemers uit het oranje netwerk als default gateway ***10.0.0.254.*** krijgen en dat in de router tussen het oranje en groene netwerk een static route wordt toegevoegd die zegt dat IP adressen uit het subnet ***192.168.0.0.*** zich achter IP adres ***10.0.0.1.*** bevinden. Zodoende worden deze pakketten door gerouteerd naar de juiste router. Kort samengevat heeft een router dus twee IP adressen; één aan de LAN zijde en één aan de WAN zijde. De twee IP adressen moeten ieder in een ander subnet zitten. Met deze kennis kunnen we kijken of een router een goede oplossing is voor ons probleem.

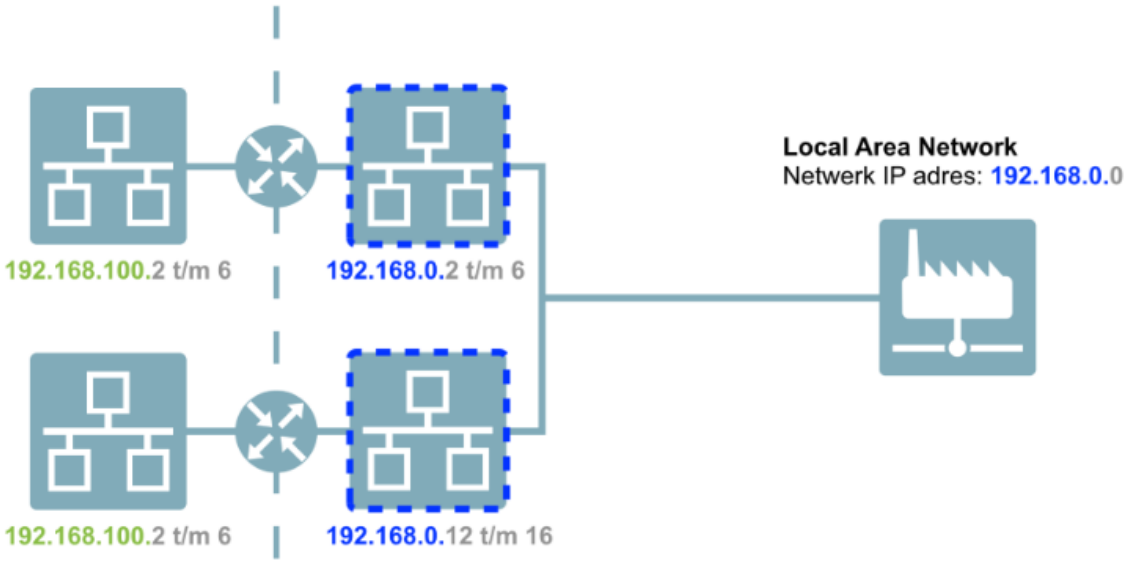
Onderstaande afbeelding geeft nu de twee machines weer welke beiden via een router verbonden zijn met het productie netwerk. De switch is achterwege gelaten evenals de LAN IP adressen van de routers, dit om de tekening leesbaar te houden.



Is het u opgevallen dat het machine netwerk nu een ander subnet heeft? (***192.168.100.0.*** i.p.v. ***192.168.0.0.***) Dit is noodzakelijk om te kunnen routeren tussen de twee netwerken. Het LAN en WAN IP adres mogen immer niet in hetzelfde subnet zitten. Elke machine neemt nu nog maar één IP nummer in beslag op het blauwe netwerk. Wanneer een deelnemer uit het groene netwerk (de machine) nu wil communiceren met bijvoorbeeld een SQL server in het blauwe netwerk dan zal de router het pakket ontvangen en doorsturen in het blauwe netwerk. Middels de NAT (Network Address Translation) functie zal de router de afzender van het pakket (bijv. ***192.168.100.2.***) vervangen voor zijn eigen IP adres aan de WAN zijde (***192.168.0.2.***) zodoende lijkt het voor de ontvanger (SQL server) net alsof de aanvraag vanuit zijn eigen subnet komt en zal hij zonder tussenkomst van de default gateway kunnen antwoorden. Deze variant van NAT heet dynamic NAT.

Het word echter een ander verhaal indien er vanuit het blauwe netwerk naar het groene netwerk gecommuniceerd dient te worden. Omdat er twee groene netwerken zijn met dezelfde IP nummers is het onmogelijk vast te stellen naar welke router de pakketten gestuurd moeten worden. Om deze reden is deze oplossing ook niet 100% geschikt.

Welke oplossing is dan wel geschikt? Wel, er is nog een andere variant van NAT, naast dynamic NAT is er ook een zogeheten **1:1 NAT**. Dit houd in dat er per IP adres een vaste vertaling kan worden ingesteld naar het andere subnet. Met andere woorden; u kunt de IP adressen virtueel aanpassen zodat het net lijkt of de machine niet achter een router zit. De enige voorwaarde is dat er voldoende IP adressen beschikbaar zijn in het Productie netwerk (blauwe netwerk). In het onderstaande voorbeeld zijn de IP adressen ***192.168.100.2.*** *t/m* ***6*** van de ene machine 1:1 vertaald naar de IP adressen ***192.168.0.2.*** *t/m* ***6*** en van de andere machine zijn deze 1:1 vertaald naar IP adressen ***192.168.0.12.*** *t/m* ***16***.

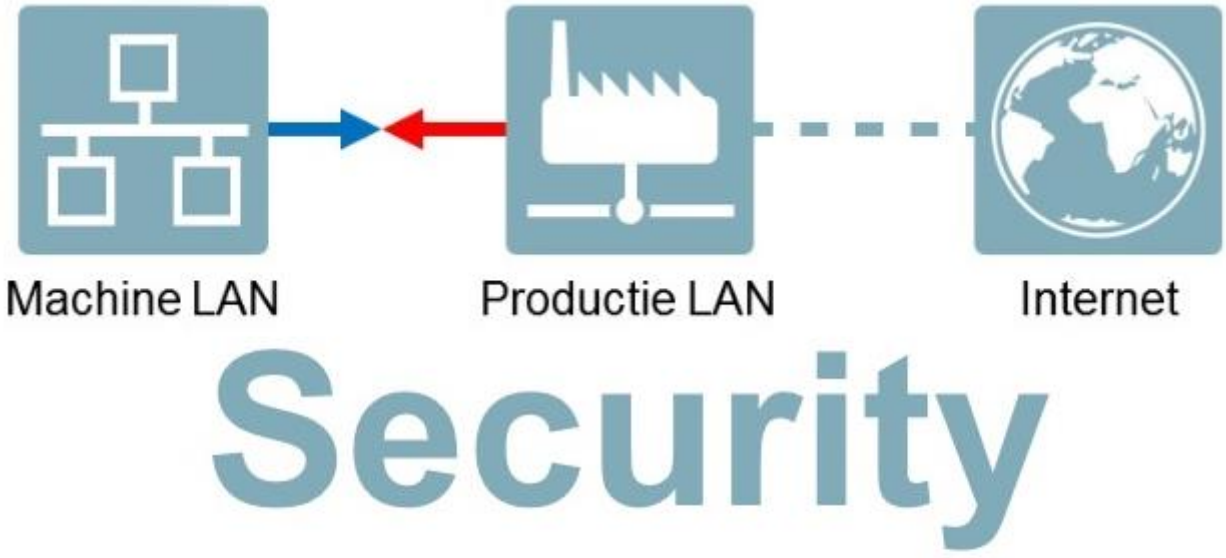


Op deze manier zijn beide machines uniek geadresseerd in het Productie netwerk en zijn de interne IP adres identiek waardoor het onderhoud eenvoudiger wordt en de eventuele servicemonteur altijd uit kan gaan van dezelfde IP nummers in de machine. Al met al stelt dit u in staat om seriematig geproduceerde machines eenvoudig te integreren binnen 1 netwerk.

Hoe het zit met het **Security** en **Remote Access** aspect leg ik u graag een volgende keer uit.

U kunt ook altijd contact met mij opnemen om uw specifieke vragen rond deze thema's te bespreken. Mijn contactgegevens staan vermeld in mijn LinkedIn profiel.

Ontdek hier onze oplossingen voor industrieel ethernet



Sjoerd Hakstege - van Eekhout
Network & Security Specialist at Phoenix Contact

Volgen

Vervolg: Security + Remote Access

Beste lezer,

In mijn vorige post heb ik behandeld hoe u machines kunt integreren in een bestaand netwerk. Deze post kunt u hier vinden. Ditmaal wil ik het security en remote access aspect hieromtrent bespreken.

Een belangrijk verschil tussen de IT wereld en de industrie (OT) wereld is dat er verschillende prioriteiten worden gesteld aan de functies van een netwerk. Wanneer we vanuit het security oogpunt naar een netwerk kijken kunnen we 3 hoofdtaken onderscheiden, te weten:

- Confidentiality
- Integrity
- Availability

* **Confidentiality** is de eigenschap dat de data niet zomaar onderschept kan worden door derden. Het zorgt er dus voor dat alleen de beoogde ontvangers toegang hebben tot de informatie.

* **Integrity** is zekerheid dat de informatie vertrouwd kan worden en accuraat is. Het voorkomt dat data gemanipuleerd kan worden zonder dat dit gedetecteerd wordt.

* **Availability** is de garantie dat de data beschikbaar is voor diegene die er toegang tot moeten hebben. In de praktijk houdt dit in dat het netwerk betrouwbaar moet zijn met een hoge up-time.

In de IT wereld word doorgaans de C-I-A volgorde aangehouden (van belangrijk naar minder belangrijk). In de OT wereld is dit vaak omgekeerd: A-I-C. De beschikbaarheid van de installatie is dus het belangrijkste. Hierdoor is er ook een verschil in patch-management; updates kunnen niet zomaar geïnstalleerd worden, vaak worden deze tijdens geplande stops geïnstalleerd. Ook is het soort data anders dan in de IT wereld, de Realtime eisen zijn hierbij een stuk belangrijker.

Een ander belangrijk verschil is de locatie van de beveiligingscomponenten (firewalls e.d.).

* IT: **Centraal**

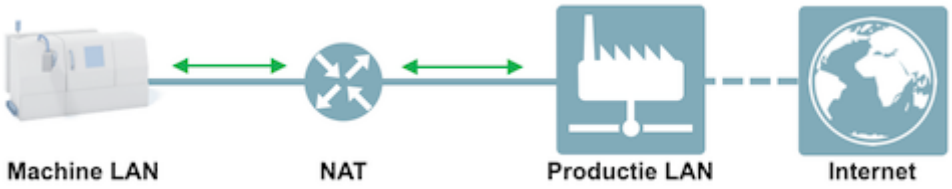
- Firewall waar internet binnen komt

* OT: **Decentraal**

- Firewall zo dicht mogelijk tegen de te beschermen machine

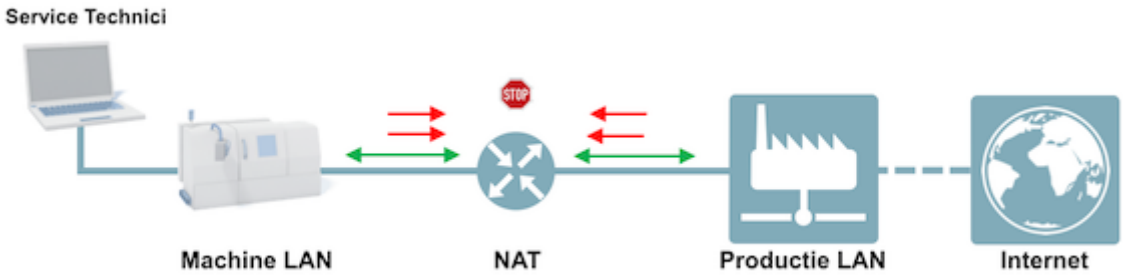
Een decentrale plaatsing van firewalls heeft als voordeel dat het netwerk hierdoor gesegmenteerd wordt. Bij een eventuele aanval of infectie met mallware worden de gevolgen beperkt tot een deel van het netwerk.

Terugkomend op mijn vorige post (1:1 NAT) kunnen we nu concluderen dat zonder extra maatregelen er een potentieel security risico aanwezig is. Verkeer van en naar de machine is zonder beperkingen mogelijk.



Op zich hoeft dit nog geen probleem te zijn als er geen verbinding is met het internet of het office netwerk en er ook geen vreemde apparaten worden toegelaten op het productienetwerk (USB sticks, Laptops e.d.) Vanuit service oogpunt is dit echter geen realistische situatie en omdat de machines dankzij de 1:1 NAT functionaliteit allemaal identieke interne IP nummers hebben is het voor de Service Technici efficiënt om de laptop aan het machine netwerk te koppelen voor service doeleinden.

Maar wat als deze laptop geïnfecteerd is met een virus? Op zo'n moment wil je het productienetwerk hiertegen beschermen. Dit is mogelijk met een firewall functie, deze heeft als bijkomend voordeel dat deze in twee richtingen bescherming kan bieden. De firewall dient dan zo ingesteld te worden dat alleen die data die nodig is voor het proces toegestaan is. Zodoende is de machine beveiligd tegen gevaren uit het productienetwerk en is het productienetwerk beveiligd tegen gevaren uit de machine.



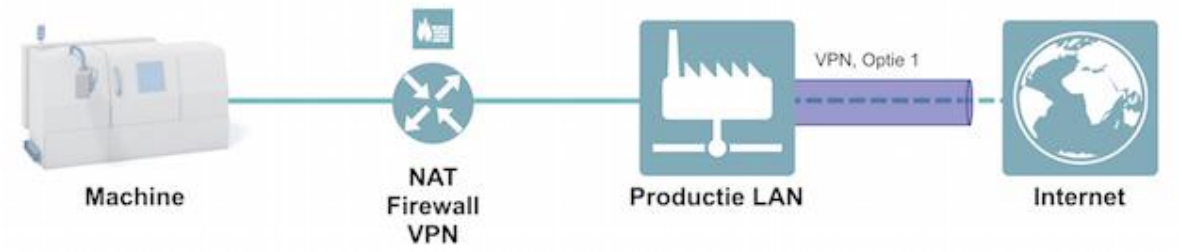
Maar wat zijn de mogelijkheden als er van afstand service verleend moet worden?

Remote access

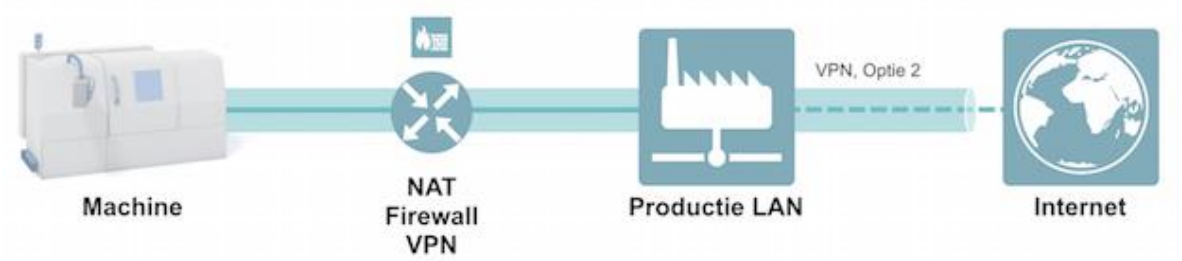
Dankzij de integratie van TCP/IP zijn er mogelijkheden om via het internet toegang te krijgen tot de machine, maar dit dient wel op een veilige manier te gebeuren. Om deze communicatie te beveiligen dienen we weer te voorzien in de C-I-A eigenschappen. Middels VPN tunnels kunnen we hierin voorzien.

Ten opzichte van de Router met NAT, Firewall en VPN functie zijn er 3 soorten tunnels te definiëren

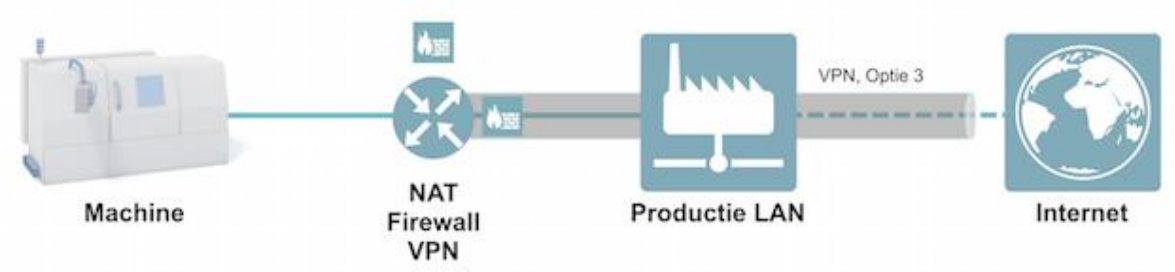
1: De VPN tunnel stopt voor de router (bijvoorbeeld bij de router welke het productie LAN verbind met het internet. In deze situatie kan het netwerkverkeer richting de machine door de firewall gecontroleerd worden.



2: De VPN tunnel loopt door de router (wordt bijvoorbeeld door een VPN router in de machine opgebouwd). In deze situatie kan het netwerkverkeer richting de machine niet meer door de firewall gecontroleerd worden omdat de data gecodeerd is.



3: De VPN tunnel stopt op de router (wordt dus door deze router opgebouwd). In deze situatie kan het netwerkverkeer richting de machine door middel van separate firewall regels in de tunnel gecontroleerd worden.



Uiteraard dienen bij remote access de noden versus de risico's afgewogen te worden. Moet een machine wel altijd "Online" zijn? Daarnaast wilt u als eindklant zelf de regie hebben wanneer iemand toegang kan hebben tot uw machine. En als leverancier van die machine wilt u uw klant gerust kunnen stellen dat hij zelf "in control" kan zijn als dat gewenst is.

Hiervoor bieden we een oplossing middels een potentiaalvrij contact. Middels dit contact kan een VPN tunnel geactiveerd worden of bepaalde firewall regels actief worden, denk hierbij bijvoorbeeld aan de benodigde regels om een PLC te kunnen programmeren.

Ontdek hier onze oplossing voor security en remote access.