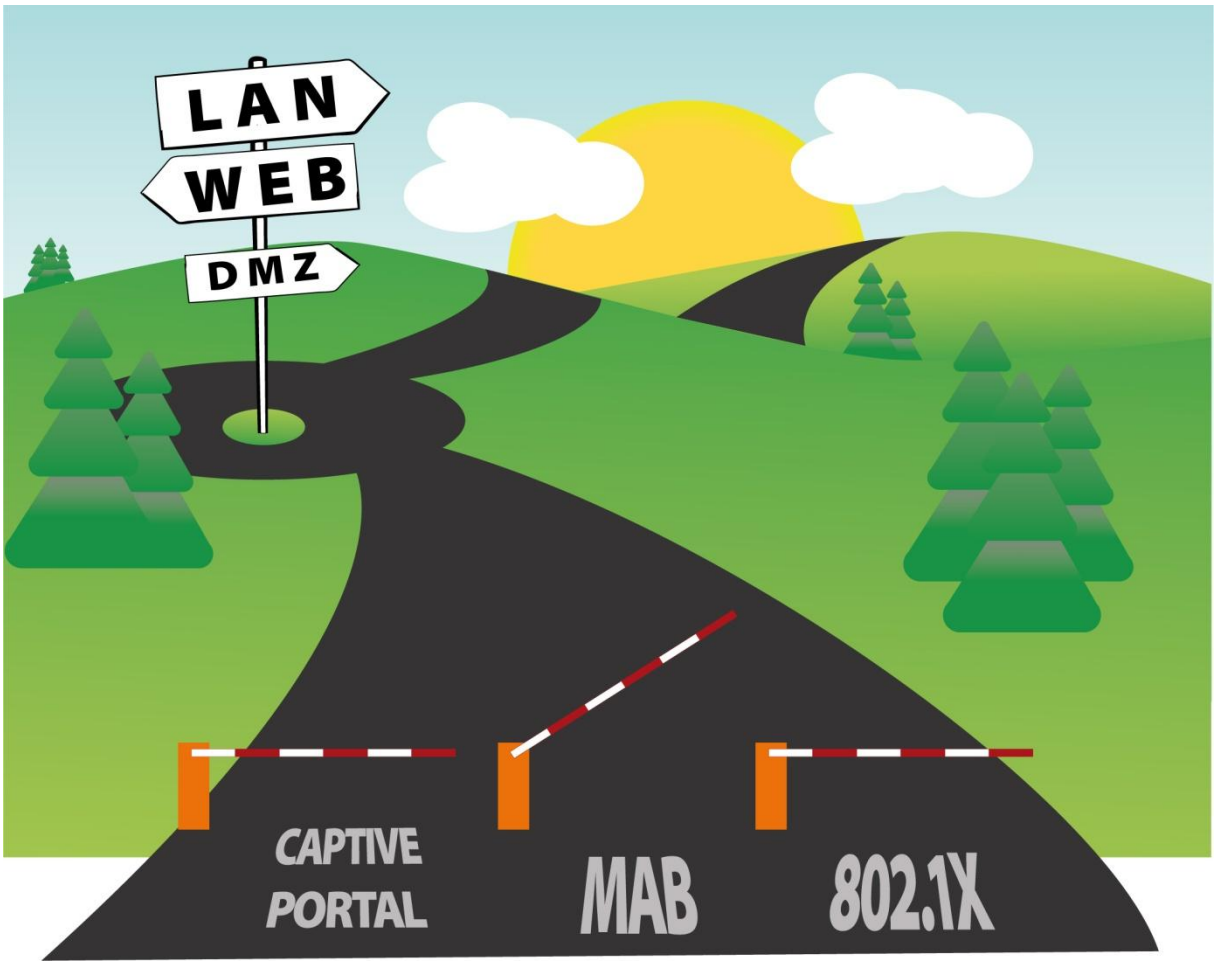
Knibbel Knabbel Knuisje

Netwerktoegangscontrole binnen Sligro Food group



Knibbel Knabbel Knuisje	
Documenttype	Afstudeerverslag
Status	Definitief
Versie	1.00
Auteur	Rob Maas
Datum	17-06-2010

Documentbeheer

Versieoverzicht

Datum	Wat	Versie
29-03-2010	Eerste opzet	0.01
09-04-2010 – 15-05-2010	Verdere uitwerking (opzet, intro & test)	0.02
16-05-2010 – 25-05-2010	Verdere uitwerking (pilot)	0.03
16-05-2010 – 08-06-2010	Spelling en grammatica verbeterd + pilot uitgewerkt	0.04
10-06-2010	Titelpagina + spelling en grammatica	0.05
14-06-2010	Spelling en grammatica	0.06
17-06-2010	Definitief gemaakt	1.00

Voorwoord

In de periode januari tot en met juni 2010 heb ik, ter afronding van mijn deeltijd opleiding HBO Technische Informatica aan de Avans hogeschool in Breda, mijn afstudeerproject uitgevoerd. Dit afstudeerproject met als titel “Knibbel Knabbel Knuisje“ heb ik uitgevoerd bij Sligro Food Group in Veghel. Het verslag wat nu voor u ligt is het resultaat van dit project.

Graag wil ik in dit voorwoord van de gelegenheid gebruik maken om een aantal personen te bedanken die deze afstudeerscriptie mede mogelijk hebben gemaakt. Allereerst wil ik Alexander Hermans en Jos Mulder bedanken voor hun begeleiding vanuit respectievelijk Sligro Food Group en school. Daarnaast wil ik mijn dank betuigen aan mijn collega’s voor hun hulp, advies en zeker ook begrip tijdens mijn afstudeerperiode. Ook wil ik Sligro bedanken voor het beschikbaar stellen van hardware, zodat ik naast de uren op kantoor ook thuis de mogelijkheid had om te werken aan dit verslag.

Als laatste wil ik ook graag mijn familie bedanken en met name mijn vriendin Mariëlle te Lindert voor hun steun, zorg en belangstelling tijdens de afstudeerperiode.

Ik wens u veel informatief leesplezier.

Veghel, juni 2010
Rob Maas

Managementsamenvatting

Op het moment van schrijven van dit verslag, wordt er binnen Sligro Food Group nauwelijks aandacht aan interne netwerk beveiliging besteed. Dit betekent dat elk apparaat die aan het interne netwerk wordt gekoppeld, zonder al te veel problemen een netwerkverbinding tot stand kan brengen. De controle die in het verleden is ingebouwd is zeer onderhoudsgevoelig en relatief makkelijk te omzeilen. Mede doordat het gebruik van mobiele apparaten in rap tempo toeneemt, is het steeds belangrijker om juist het interne netwerk te beschermen tegen ongewenste apparaten.

De opdracht was dan ook om een pilot omgeving op te bouwen met netwerktoegangscontrole. In deze pilot omgeving was naast beveiliging, ook de onderhoudsgevoeligheid een zeer belangrijk punt.

Om tot een juiste oplossing te komen, zijn eerst alle typen apparaten binnen het netwerk geïnventariseerd. Vervolgens werd bekeken welke beveiligingsmechanismen allemaal mogelijk zijn op zowel de netwerkcomponenten als de (eind-)apparaten (cliënts). Na deze inventarisatie werd gestart met het bouwen van een test omgeving. Deze omgeving was compleet gescheiden van het Sligro netwerk. In deze testomgeving zijn alle configuraties uitvoerig getest en bijgeschaafd tot ze naar tevredenheid functioneerden.

Na deze test is een pilot omgeving opgebouwd, die onderdeel uitmaakte van het daadwerkelijke productienetwerk. Hierin is getest met productiesystemen, om zodoende tot een zeer representatief beeld te komen van de impact van netwerktoegangscontrole binnen Sligro.

Uit deze pilot is gebleken, dat de implementatie van een netwerktoegangscontrole binnen Sligro het netwerk niet alleen veiliger maakt, maar dat ook het beheer aanzienlijk eenvoudiger en minder tijdrovend wordt. Ook geeft het implementeren van netwerktoegangscontrole de mogelijkheid meer zicht op het netwerk te houden, zoals welk apparaat verbinding heeft gemaakt en hoeveel dit apparaat verbruikt. Voor beheerders bestaat de mogelijkheid om op alle plekken binnen het netwerk, beheer uit te voeren, zonder dat hier aanpassingen voor nodig zijn.

Ondanks dat het Sligro breed implementeren van een netwerktoegangscontrole een tijdrovende klus is, luidt mijn advies om netwerktoegangscontrole stap voor stap verder uit te bouwen. Eerst op het hoofdkantoor en vervolgens op de distributiecentra. Als deze locaties gereed zijn, kan verder gekeken worden naar de decentrale locaties. Hierbij moet nog wel goed naar redundantie worden gekeken. Op het hoofdkantoor en de distributiecentra is deze relatief eenvoudig in te bouwen. Op de decentrale locaties moet hier nog goed naar gekeken worden om niet afhankelijk te worden van de KPN Lijn, die de locatie met het Sligro hoofdkantoor verbindt.

Inhoud

1. Inleiding

In het kader van mijn opleiding HBO Technische Informatica deeltijd aan de Avans hogeschool in Breda, heb ik in de periode januari tot en met juni 2010 gewerkt aan mijn afstudeerproject " Knibbel Knabbel Knuisje" . Opdrachtgever voor dit project is Alexander Hermans, teamleider van de afdeling Beheer & Ondersteuning van Sligro Food Group. Het doel van dit project was om een pilot op te zetten van een zogenaamde Network Access Control (NAC), in het vervolg genoemd als netwerktoegangscontrole. Met deze pilot opstelling wordt onderzocht of dit een oplossing is die men kan en wil gebruiken en zo nodig deze oplossing Sligro breed te implementeren.

De opbouw van dit verslag luidt als volgt.
In het eerste gedeelte van het verslag wordt er aandacht besteed aan Sligro Food Group als bedrijf. Vervolgens wordt het probleem geanalyseerd en besproken wat de eisen van een eventuele oplossingen moeten zijn. Nadat dit allemaal bekend is worden de verschillende mogelijkheden onderzocht Met het resultaat van dit onderzoek, wordt vervolgens een testomgeving opgebouwd. Zo kunnen eventuele problemen, welke zich zouden kunnen voordoen in de productieomgeving, opgelost worden. Na afronding hiervan wordt de oplossing in een pilot opgebouwd, zodat er gekeken kan worden hoe deze omgeving in productie reageert. Tevens krijgen de medewerkers van ICT Beheer op deze manier inzicht in de oplossing. Hierbij hoort een presentatie waarbij het een en ander wordt uitgelegd. Na een periode met de pilot omgeving te hebben gewerkt, wordt hier verslag van gemaakt. Uiteindelijk zal dit leiden tot een conclusie en aanbevelingen.

2. Sligro Food Group

Sligro Food Group is een beursgenoteerd bedrijf, dat zich richt op de etende en drinkende mens. Dit uit zich in de verkoop van food-, semi-vers-, dagvers- en aan food gerelateerde non-foodartikelen. De verkoop van deze artikelen gebeurt zowel via foodretail als via de foodservice branche.

In foodretail branche, vinden we de EMTÉ en Golff supermarkten. De EMTÉ supermarkten zijn in eigen beheer van Sligro. De Golff supermarkten worden beheerd door eigen ondernemers. In de loop van dit jaar, gaan de Golff supermarkten ook onder de EMTÉ vlag draaien. Weliswaar blijven dit supermarkten met eigen ondernemers. Hierbij wordt dan ook gesproken van EMTÉ Franchise.
Op dit moment zijn er zo'n 80 EMTÉ supermarkten en 50 Golff supermarkten.

Naast foodretail, is er de foodservice branche, deze richt zich voornamelijk op de horeca, bedrijfsrestaurants en winkels bij benzinestations. Sligro Food Group heeft ongeveer 45 Sligro zelfbedieningsfilialen, dit zijn filialen waar klanten zelf hun boodschappen kunnen doen. Daarnaast heeft Sligro Food Group ongeveer 10 bezorglocaties. Ook Inversco-Van Hoeckel valt onder de foodservice vlag, dit is een dochteronderneming die de grotere horecaketens en instellingskeukens in Nederland verzorgt. Denk hierbij aan grote gaarkeukens en penitentiaire inrichtingen.

Naast de verkoop, heeft Sligro Food Group een aantal bedrijven die zich bezig houden met de productie van voedsel. Culivers is een bedrijf dat conveniencemaaltijden[1] produceert. Deze maaltijden worden onder andere gemaakt voor horeca en zorginstellingen. Naast Culivers heeft Sligro Food Group nog een visverwerkingsbedrijf, genaamd SmitVis. Dit bedrijf levert zowel aan de foodservice als aan de foodretail van Sligro Food Group. Ook Maison Niels de Veye, patisseriespecialist[2], is onderdeel van Sligro Food Group en richt zich op de horeca.

Hieronder volgt een schematische opzet van de bedrijven die binnen Sligro Food Group met elkaar verbonden zijn:

<table>
<tr><th colspan="4">Centraal distributiecentrum en hoofdkantoor Veghel</th></tr>
<tr><th colspan="2">Foodretail</th><th colspan="2">Foodservice</th></tr>
<tr><td>EM-TÉ
80 eigen supermarkten</td><td>Golff
50 franchise supermarkten</td><td>Sligro
Horeca, recreatie, catering, pompshops, grootverbruik</td><td>Inversco-Van Hoeckel
Institutioneel, nationale ketens, grootschalige horeca</td></tr>
<tr><td colspan="2">2 distributiecentra</td><td>Landelijk netwerk van 45 zelfbedienings- en 10 bezorggroothandels</td><td>2 distributiecentra</td></tr>
<tr><th colspan="4">Sligro Fresh Partners & Productiebedrijven</th></tr>
<tr><td colspan="4">5 gespecialiseerde productiefaciliteiten voor convenience (CuliVers), vis (SmitVis) en patisserie (Maisson Niels de Veye) en vier deelnemingen in versbedrijven</td></tr>
</table>

Tabel 1: Bedrijfsstructuur Sligro Food Group

Bron: http://www.sligrofoodgroup.nl

[1] Kant en klaarmaaltijden
[2] Taart en gebakspecialist

Over het jaar 2009 is een omzet gerealiseerd van € 2.258 miljoen met een nettowinst van € 74 miljoen.

Kerncijfers

	x € miljoen 2009	Toename in %
Bruto bedrijfsresultaat (ebitda)	149	1,3
Bedrijfsresultaat (ebit)	98	(0,4)
Netto winst	74	4,2
Operationele kasstroom	123	19,9
Netto rentedragende schuld	131	(28,4)

Tabel 2: Kerncijfers Sligro Food Group 2009

2.1 ICT organisatie

Aangezien het project ICT georiënteerd is, wordt hier in het kort beschrijven hoe de ICT afdeling is georganiseerd. Binnen ICT zijn er ongeveer 70 mensen werkzaam. De ICT afdeling is op te splitsen in drie onderdelen, te weten ICT Beheer, ICT Ontwikkeling en Winkelautomatisering.

Naast deze drie afdelingen, is er een extra functie, die niet gebonden is aan een afdeling. Dit is de functie Manager IT Projecten en IT Security. Deze functie is gecreëerd om het management van de ICT afdeling te ondersteunen.

2.1.1 ICT Beheer

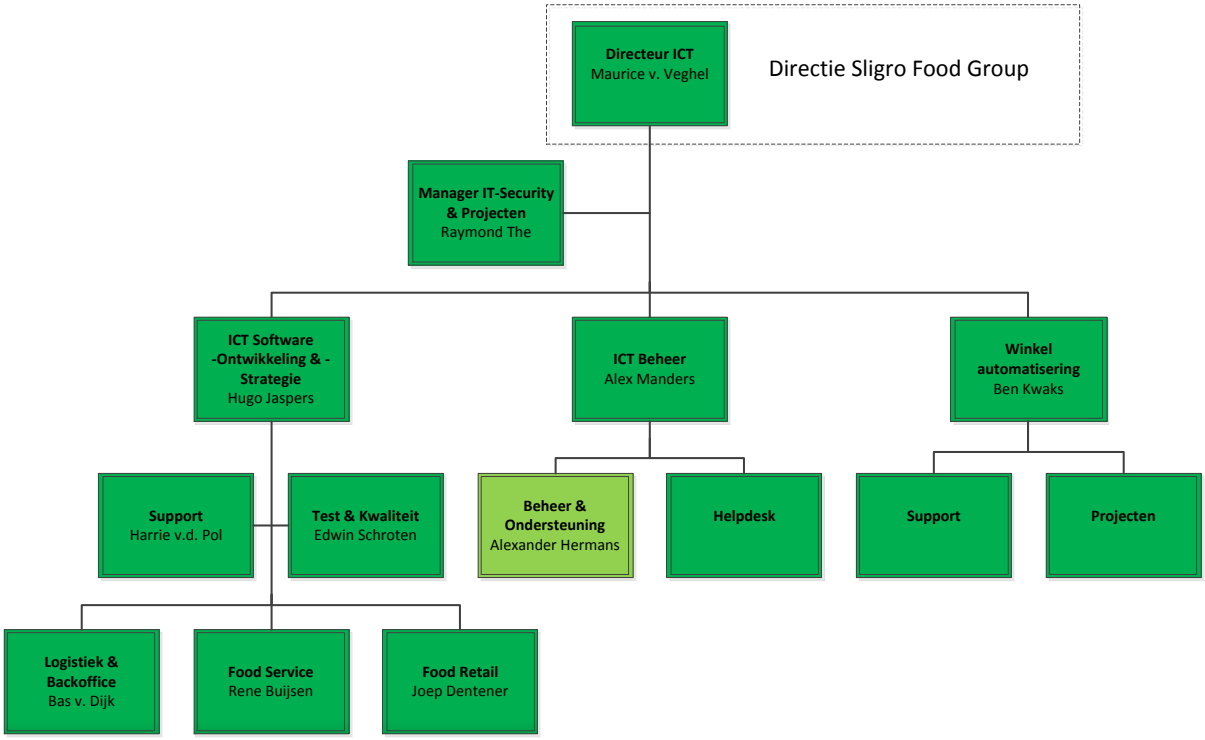
ICT Beheer, is zoals de naam al doet vermoeden, gericht op het beheren van de ICT omgeving. Deze afdeling is verantwoordelijk voor de complete ICT infrastructuur en de daarbij behorende systemen. Denk hierbij aan ongeveer 250 servers, 5000 werkplekken en 450 netwerkapparaten.
Naast het beheer worden binnen deze afdelingen ook de nodige projecten uitgevoerd om de continuïteit, beheersbaarheid en veiligheid te waarborgen. Deze afdeling bestaat uit twee subafdelingen, te weten; Beheer & Ondersteuning en Helpdesk.

2.1.2 ICT Ontwikkeling

De afdeling ICT ontwikkeling houdt zich bezig met het ontwikkelen van software. Deze software wordt gebruikt om de efficiëntie te verbeteren in de organisatie. Deze afdeling bestaat uit vijf subafdelingen, te weten Support, Test & Kwaliteit, Logistiek & Backoffice, Food Service en Food Retail.

2.1.3 Winkelautomatisering

De afdeling winkelautomatisering, heeft twee subafdelingen. De afdeling support en de afdeling projecten. Deze afdeling is verantwoordelijk voor de ICT in de retail winkels.



Figuur 1: Organigram Sligro Food Group ICT Afdeling

3. Projectbeschrijving

3.1 Probleemstelling

Op dit moment is er nauwelijks een vorm van netwerkbeveiliging. Vrijwel elk apparaat kan gekoppeld worden aan het netwerk en heeft vrijwel direct een verbinding met dit netwerk. In het verleden zijn een aantal pogingen gedaan om dit beter te beveiligen, namelijk;

- MAC beveiliging – Elke poort leert een apparaat en deze mag niet gewijzigd worden.
- Niet gebruikte poorten dichtzetten.

Deze oplossingen bleken in de praktijk slecht toepasbaar door het intensieve onderhoud. Daarbij is deze manier van beveiliging relatief makkelijk te omzeilen.

Door de grote toename van mobiele apparaten die veelal ongevraagd en soms ongewenst gebruik (willen) maken van het netwerk van de Sligro bestaat de wens voor een goede netwerkbeveiliging. Het ontbreken van een goede beveiliging brengt namelijk een aantal risico's met zich mee, zoals bijvoorbeeld;

- Virussen en Spam, welke zich verspreiden via een besmet systeem op het netwerk.
- Vertrouwelijke informatie, welke in verkeerde handen komt.

Om deze en andere problemen in de toekomst te voorkomen, is de onderstaande opdracht ontstaan.

3.2 Opdracht

Zoals in de probleemstelling al duidelijk werd, is er geen zicht op apparaten die zich in het netwerk bevinden. Een niet Sligro systeem kan aan het netwerk gekoppeld worden, zonder dat de afdeling Beheer & Ondersteuning hiervan op de hoogte is. Op dit moment is bestaat er geen alternatief en worden er regelmatig niet Sligro systemen aan het netwerk gekoppeld. Zoals hiervoor te lezen is, brengt dit allerlei risico's met zich mee.

De opdracht is dan ook geformuleerd om er voor te zorgen, dat alle systemen die toegang willen tot het netwerk, zich bekend maken. De algemene term c.q. techniek die hiervoor staat heet Network Access Control (NAC). Vanwege het feit dat Sligro graag met Nederlandse bewoordingen werkt, zal in document verder gesproken worden van Netwerktoegangscontrole.

Naast het feit dat de netwerktoegangscontrole moet zorgen voor identificatie van systemen, is het ook de bedoeling dat er aan de hand van die identificatie een classificatie wordt gemaakt. Welke systemen worden er vertrouwd en welke systemen krijgen beperkte toegang of zelfs geen toegang.

Vanwege de impact van een netwerktoegangscontrole op de infrastructuur van Sligro, zal deze opdracht zich beperken tot het opzetten van een representatieve pilot.

3.3 Doelstellingen

De concrete doelstelling van het project is om een pilot op te zetten, waarbij duidelijk wordt wat de impact is van een netwerktoegangscontrole in de Sligro ICT omgeving. De pilot dient uiteraard aan een aantal doelstellingen te moeten voldoen en die luiden als volgt.

1. Overzicht houden van alle apparaten die zich in het netwerk bevinden of bevonden.
2. (Beperkte/geen) Internet/netwerk toegang voor niet of minder vertrouwde systemen.
3. Het detecteren van ongewenst (netwerk) gedrag en hierop reageren.
4. Het vroegtijdig detecteren van virussen en hierop reageren.
5. Het beheer moet zeer gebruiksvriendelijk zijn en gedaan kunnen worden door de 2e lijns helpdesk.
6. Het dynamisch een netwerk(VLAN) aan een gebruiker toe kennen.
7. Het geheel moet kunnen werken, zonder extra applicaties op de “cliënt”.
8. Het geheel moet redundant uitgevoerd kunnen worden.

Bij het project hoort tevens een presentatie voor de afdeling ICT Beheer, waarin een duidelijk beeld geschept wordt van netwerktoegangscontrole en de betekenis voor het beheer.

3.4 Opdrachtgever

De opdracht is ontstaan, vanuit de afdeling Beheer & Ondersteuning om betere controle te krijgen over welke apparaten zich in het netwerk bevinden. Omdat de afdeling Beheer & Ondersteuning onder leiding staat van Alexander Hermans, is hij aangewezen als opdrachtgever.

Naam:	Alexander Hermans
Afdeling:	ICT Beheer (Beheer & Ondersteuning)
Functie:	Teamleider
E-mail:	ahermans@sligro.nl
Telefoon:	0413-343500 (1333)
Mobiel:	0653989228

3.5 Scope

Vanwege de omvang van dit project en de impact hiervan op de infrastructuur, is er besloten een pilot op te bouwen. Omdat het erg lastig te bepalen is, hoeveel tijd er in de verschillende fasen van het project gaan zitten, is een onderverdeling van de projectdelen gemaakt middels de MoSCoW methode. Deze methode geeft de mogelijkheid om zeer flexibel om te gaan met het project. Let wel, de “Must have this”, moeten behaald worden om het project te laten slagen.

- **Must have this:**
  - Mogelijkheid om alle type apparaten te koppelen aan het netwerk.
  - Overzicht van alle apparaten in het netwerk.
  - Automatische indeling van het netwerk (VLANs).
  - Detectie mogelijkheid virussen of misbruik.
- **Should have this if at all possible:**
  - Duidelijke beheersomgeving.
- **Could have this if it does not affect anything else:**
  - Locatie(s) buiten het hoofdkantoor betrekken in de pilot.
- **Would like to have but won’t have this time around:**
  - Grafische schil voor captive portal.
  - Overeenkomst gebruik Internet.
  - Gebruikershandleidingen aanmelden netwerk.
  - Handleidingen beheer (2^{e} lijns helpdesk).
  - Implementatie in het complete netwerk.

3.6 Producten / Resultaat

Tijdens het project zullen de volgende producten worden opgeleverd. De oplevering van de onderstaande producten zal niet noodzakelijk in de onderstaande volgorde geschieden.

- Plan van Aanpak
- Onderzoek- en testrapport
- Test omgeving
- Pilot omgeving
- Presentatie
- Uitgebreid verslag pilot omgeving.
- Scriptie / Presentatie (Afstuderen)

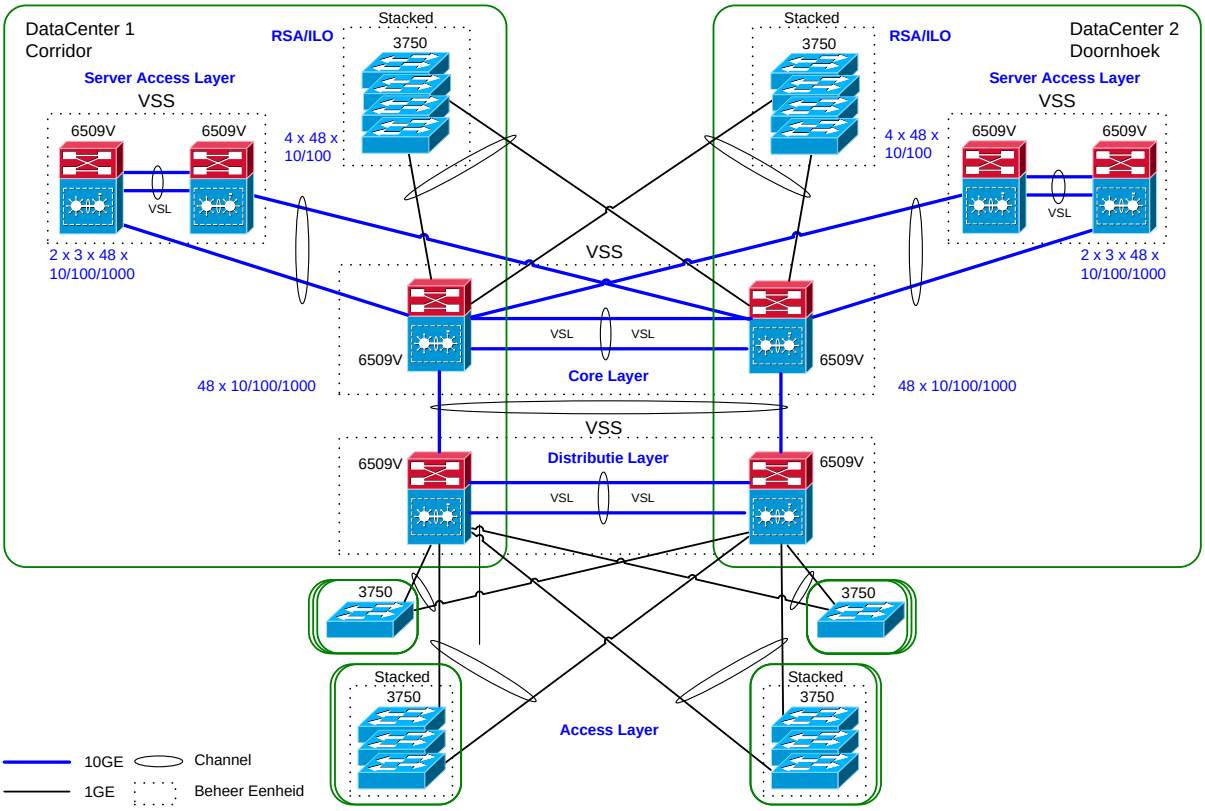
3.7 Uitgangspunten

De onderstaande uitgangspunten zijn leidend voor de projectaanpak.

1. Het project heeft een tijdsbeperkende omvang.
2. Het project is gebaseerd op een zo'n representatief mogelijke pilot omgeving.
   (Deze omgeving wordt later in dit document beschreven)
3. Het grootste gedeelte van dit project zat iteratief aangepakt worden.

3.8 Relaties met andere projecten

Binnen Sligro Food Group, loopt een ander project, met direct raakvlak met dit project. In dit project worden alle HP Procurve apparatuur op het hoofdkantoor en de bijhorende distributiecentra vervangen door Cisco apparatuur. Dit project is momenteel in volle gang en moet eind mei gereed zijn. Om dit project representatief te laten zijn voor de toekomst wordt dan ook gebruik gemaakt van de Cisco apparatuur. Hieronder staat een tekening van de toekomstige netwerk infrastructuur.



Figuur 2: Toekomstige netwerkomgeving Sligro hoofdkantoor en distributiecentra

Net na dit project wordt vervolgens een project gestart om het complete draadloze netwerk binnen het hoofdkantoor en de distributiecentra geschikt te maken voor gebruik van laptops, zowel laptops in eigen beheer als van externen. Dit project start op 15 juli. De ervaringen die in deze pilot opgedaan worden, zullen meegenomen worden in dit project.

3.9 planning

Taak	Uur
Schrijven PVA	15
Inventarisatie van verschillende apparaten	10
Uitzoeken verschillende authenticatie mogelijkheden per device	20
Uitzoeken geschikte NAC software + eisen	15
Uitzoeken geschikte IDS software + eisen	15
Onderzoeksrapport schrijven	20
NAC Software testen	40
IDS Software testen	40
Opzetten testomgeving (plan + realisatie)	120
Beschrijven resultaten testomgeving	25
Pilot opzetten	100
Presentatie maken en geven	25
Verslag pilot omgeving	40
Scriptie en presentatie (Afstuderen)	120
Totaal	**605**

4. Onderzoek

4.1 Inventarisatie hardware

"De ketting is zo sterk als de zwakste schakel", deze uitspraak wordt vaak gebruikt als het aankomt op beveiliging. Ook in dit project is deze uitspraak van toepassing. Het is daarom heel belangrijk om te weten welke apparaten er binnen Sligro toegang hebben tot het netwerk en hoe deze apparaten om zullen gaan met netwerktoegangscontrole.

Voordat er daadwerkelijk met het bouwen van een netwerktoegangscontrole kan worden begonnen, is het belangrijk om een inventarisatie te maken van alle verschillende apparaten die zich binnen het huidige Sligro netwerk bevinden. Deze inventarisatie is gesplitst in twee delen, te weten

- Hoofdkantoor en de distributiecentra in Veghel.
- Decentrale vestigingen.

Deze splitsing is gemaakt, omdat er op decentrale vestigingen andere apparatuur aanwezig is, denk hierbij aan weegschalen en kassa's.

4.1.1 Het hoofdkantoor en de distributiecentra in Veghel

Hieronder worden alle verschillende apparaten, die te vinden zijn op het hoofdkantoor en de distributiecentra in Veghel, even benoemd en kort toegelicht.

- **Hubs**: op dit moment zijn er nog een aantal hubs aanwezig, met de implementatie van de Cisco apparatuur zullen deze apparaten definitief verdwijnen.
- **Laptops**: zowel Sligro laptops, als laptops van andere partijen (partners), maken geregeld onderdeel uit van het netwerk.
- **Mac's (Apple)**: de afdeling "Studio" maakt gebruik van Apple Mac desktopcomputers.
- **NC's (Thinclient)**: er wordt zoveel mogelijk getracht gebruik te maken van zogenaamde netwerk computers (NC) om via Server Based Computing (SBC), diensten aan te bieden.
- **PC's (Windows)**: verschillende afdelingen maken gebruiken van "zware" applicaties, die niet gemakkelijk door NC's kunnen worden vervangen.
- **PDA's / Smartphones**: steeds vaker bieden deze apparaten mogelijkheden om gebruik te maken van netwerken buiten het "standaard" GSM netwerk.
- **Printers / Multifunctionals**: alle afdelingen hebben minimaal één of meerdere printers. Er is getracht zoveel mogelijk dezelfde typen te gebruiken, maar doordat sommige afdelingen andere eisen hebben, zijn er verschillende typen aanwezig.
- **PTL Boxen(QNX)**: in de distributiecentra wordt gebruik gemaakt van Pick To Light (PTL), deze techniek maakt gebruik van apparatuur, waar het QNX besturingssysteem op draait.
- **Servers**: alle diensten worden zo gecentraliseerd mogelijk aangeboden. Er zijn ongeveer 200 servers, die deze diensten mogelijk maken.
- **Switches**: om alle werkplekken aan te sluiten aan het netwerk wordt gebruik gemaakt van Cisco switches (op het moment van schrijven is dit nog HP Procurve).

4.1.2 Decentrale vestigingen

Onder decentrale vestigingen, vallen een aantal verschillende type vestigingen, namelijk;

- Bezorgservices
- Distributiecentra (retail)
- Productiebedrijven
- Supermarkten
- Zelfbedieningsgroothandels

Al deze vestigingen hebben verschillende apparatuur die verbinding maakt met het netwerk. Hieronder een kort overzicht van de apparaten, die op één of op meerdere van de bovenstaande locaties te vinden zijn.

- **Hubs**: op een aantal locaties zijn nog hubs aanwezig.
- **Laptops**: regelmatig wordt op deze locaties gebruik gemaakt van Sligro laptops door mensen van het hoofdkantoor
- **NC's (Thinclient)**: op alle locaties wordt zoveel mogelijk gebruik gemaakt van NC's.
- **PC's (Windows)**: op verschillende locaties staan een aantal PC's.
- **PDA's / Smartphones**: de aanwezigheid van deze apparaten is niet te controleren, maar zeker niet ondenkbaar. (denk hierbij aan persoonlijke apparaten van personeel en/of klanten).
- **Pinpads**: de huidige generatie pinpads zijn allemaal gekoppeld aan het netwerk.
- **Printers / Multifunctionals**: alle vestigingen hebben meerdere typen printers.
- **PTL Boxen(QNX)**: in de distributiecentra wordt gebruik gemaakt van Pick To Light (PTL). Deze techniek maakt gebruik van apparatuur, waar het QNX besturingssysteem op draait.
- **Reflex**: deze systemen staan op productiebedrijven en zijn voorzien van Windows XP Embedded.
- **Servers**: op sommige vestigingen staan verschillende servers.
- **Switches**: om alle werkplekken aan te sluiten aan het netwerk wordt gebruik gemaakt van Cisco switches (op het moment van schrijven is dit nog HP Procurve).
- **Weegschalen**: op diverse locaties wordt gebruik gemaakt van weegschalen welke gekoppeld zijn aan het netwerk.

4.2 Inventarisatie beveiligingsmechanismen

Nu de apparaten zijn benoemd, dient geïnventariseerd te worden op welke manieren deze apparaten veilige toegang tot het netwerk kan worden verschaft. Hieronder worden de verschillende vormen van toegangscontrole uitgebreid belicht.

4.2.1 AAA Protocol

Het AAA protocol is een veel gebruikt proces voor toegangscontrole.
Dit protocol is geen op zichzelf staande oplossing. Het beste kan dit protocol gezien worden als een leidraad voor toegangscontrole. Dit protocol wordt met name in de netwerkwereld veelvuldig gebruikt.

Het AAA protocol beschrijft drie stappen;

- Authenticatie
- Autorisatie
- Accounting

Deze stappen worden altijd in de bovengenoemde volgorde doorlopen, echter niet alle stappen zijn verplicht. Vooral stap drie wordt geregeld achterwege gelaten.

4.2.1.1 Authenticatie

Authenticatie is de eerste stap binnen het AAA protocol. In deze stap wordt gecontroleerd of je wel echt bent wie je zegt te zijn. De meest bekende vorm hiervan is middels een combinatie van gebruikersnaam en wachtwoord. Dit proces kan echter uitgebreid worden, bijvoorbeeld door certificaat controle, vingerafdrukken e.d.

4.2.1.2 Autorisatie

Als de authenticatie met goed resultaat is doorlopen, wordt begonnen met de autorisatie. In deze stap wordt gekeken naar wat je mag. In geval van netwerktoegangscontrole bijvoorbeeld het feit dat slechts personen van ICT Beheer toegang hebben tot de servers in het DMZ vanuit het LAN.

4.2.1.3 Accounting

Na de stappen authenticatie en autorisatie is er een netwerkverbinding. In deze derde stap wordt gekeken wat iemand op het netwerk “verbruikt”, denk hierbij aan bijvoorbeeld bandbreedte. Voor dit project is deze stap niet van belang.

4.2.2 RADIUS

Zoals eerder verteld is het AAA protocol geen op zichzelf staande oplossing. Een voorbeeld van een oplossing die gebruik maakt van het AAA protocol is het RADIUS protocol. RADIUS staat voor Remote Authentication Dial In User Service en bestaat sinds 1991. Deze service verzorgt de daadwerkelijke, authenticatie, autorisatie en accounting, het AAA principe. Het RADIUS protocol is zo opgezet, dat deze het afhandelpunt kan zijn voor alle AAA verzoeken. De RADIUS server is zeer modulair en kan gemakkelijk met andere servers samenwerken. Zo kan deze bijvoorbeeld zelf de gebruikergegevens bevatten, maar deze taak kan ook uitbesteed worden aan bijvoorbeeld een LDAP, SQL, Active Directory en zelfs een andere RADIUS server behoort tot de mogelijkheden. Zoals de naam al doet vermoeden ligt de oorsprong van het RADIUS protocol in de netwerkwereld, Zelfs bijna 20 jaar later is dit nog steeds een veelgebruikt protocol.

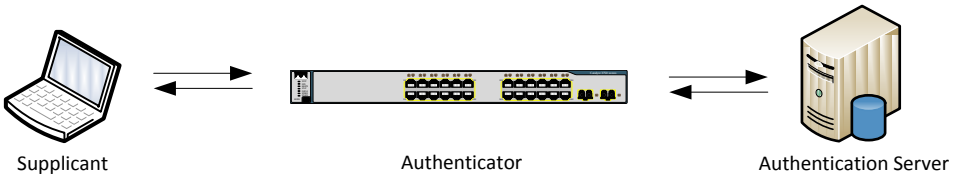
4.2.3 802.1x

802.1x is een relatief jong protocol binnen de netwerkwereld, daar de laatste revisie stamt uit 2004. Dit protocol is specifiek ontwikkeld voor netwerktoegangscontrole. Het grootte voordeel van dit protocol is, dat een cliënt zeer beperkte netwerktoegang nodig heeft om de authenticatie te kunnen uitvoeren. Dit geschiedt namelijk via zogenaamde Ethernet frames, die zich bevinden op laag 2 van het OSI model. Voor 802.1x toegangscontrole zijn de volgende drie componenten vereist:

- Supplicant
- Authenticator
- Authentication Server

De supplicant is de cliënt, het netwerkapparaat, dat toegang wil tot het netwerk, bijvoorbeeld een laptop. De authenticator is de switch die de cliënt gaat authenticeren. De authentication server, is de server welke het authenticatieverzoek afhandelt. Voor 802.1x is dit altijd een RADIUS server.

De communicatie vindt alleen plaats tussen de supplicant en de authenticator en tussen de authenticator en de authentication server. De supplicant kan dus nooit rechtstreeks bij de authentication server, alvorens deze geauthenticeerd is.



Figuur 3: 802.1x communicatie

Voor het authenticatie proces tussen de verschillende componenten, wordt standaard het EAP (Extensible Authentication Protocol) protocol beschreven. EAP is net als AAA geen op zichzelf staand protocol. EAP beschrijft hoe een authenticatie dient te verlopen en wordt daarom ook wel een framework genoemd. Een aantal veelgebruikte implementaties van EAP zijn;

- EAP-TLS:
  Bij deze vorm maken beide partijen gebruik van een certificaat. Dit protocol wordt als zeer veilig gezien. Het nadeel is wel, dat elke cliënt een eigen certificaat nodig heeft. Dit kan een enorme impact op de beheersomgeving hebben. Vaak worden de sleutels die bij het certificaat horen opgeslagen in zogenaamde smart-cards of tokens.
- EAP-MD5 (Authenticatie):
  Deze vorm van authenticatie die in het verleden veelvuldig gebruikt werd, maakt gebruik van hashes. Dit protocol wordt steeds minder gebruikt, omdat MD5 hashes tegenwoordig makkelijk te kraken zijn.
- EAP-MSCHAPv2:
  Hierbij wordt door de authenticator een uitdaging verstuurd naar de cliënt, de cliënt verstuurt een zogenaamde “one-way” hash terug naar de authenticator die deze vergelijkt met zijn eigen berekening. Dit is niet het meest veilige protocol, maar wordt wel veelvuldig gebruikt. In de besturingssystemen van Microsoft (Windows) wordt EAP-MSCHAPv2 standaard gebruikt.

Om deze authenticatie veilig over het netwerk te versturen, wordt hiervoor vaak een beveiligde tunnel gebruikt. Men spreekt dan over PEAP, dat staat voor Protected Extensible Authentication Protocol.

Het 802.1x protocol volgt het AAA protocol zoals hiervoor beschreven. Dit betekent dat naast “standaard” authenticatie ook autorisatie en, indien gewenst, aan accounting gedaan kan worden.

Een groot nadeel in het verleden was dat 802.1x ondersteund moest worden door de cliënt. Deze moet immers de gebruikersgegevens goed en binnen ethernet frames aanleveren. Tegenwoordig is deze functionaliteit binnen de meeste besturingssystemen standaard aanwezig. Helaas blijven randapparaten in dezen nog wat achter, denk hierbij aan printers, multifunctionals, pinpads, weegschalen etc.

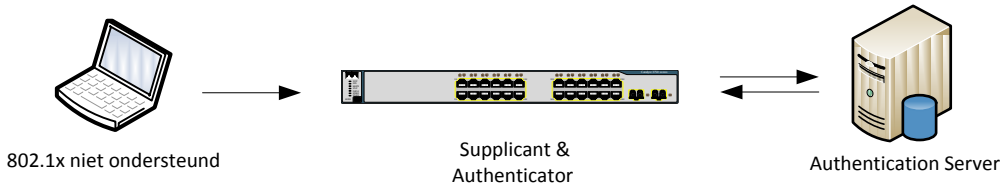
Op het moment van schrijven is 802.1x de meest veilige manier voor netwerktoegangscontrole.

4.2.4 MAB

Zoals in het voorgaande hoofdstuk omschreven, zijn er helaas nog vrij veel typen apparaten die geen 802.1x ondersteunen. Zonder 802.1x is het zeer lastig om zonder eerst een netwerkverbinding op te zetten, een authenticatie af te dwingen. Naast dat het heel lastig is, wordt het nog lastiger als dit bijvoorbeeld op een pinpad of weegschaal zou moeten gebeuren. Meestal zijn deze apparaten namelijk voorzien van een zeer beperkt toetsenbord.

Elk apparaat heeft een uniek MAC adres, dit MAC adres is dan ook uitermate geschikt om te gebruiken voor authenticatie. Nu zijn er twee technieken die gebruik maken van het MAC adres als beveiligingsmethode. Deze techniek MAB (MAC Authentication Bypass) is een techniek die door Cisco is ontworpen en thans alleen in Cisco apparaten is te gebruiken.

Deze techniek werkt hetzelfde als 802.1x. Echter de supplicant wordt verplaatst naar de authenticator. Indien een apparaat op de switch wordt aangesloten, zal deze proberen zo snel mogelijk het MAC adres te leren van het apparaat (Dit is namelijk de standaard functionaliteit van een switch). Als MAB is ingesteld om te authenticeren, dan zal de switch het geleerde MAC adres als gebruikersnaam en wachtwoord (bijvoorbeeld 00-0F-FE-C7-D7-22/00-0F-FE-C7-D7-22) versturen. Hier is de switch de supplicant. De gegevens worden net als in 802.1x naar de authenticator verstuurd. Dit is nog steeds de switch. Vervolgens zal de authenticator net als bij 802.1x de gegevens naar de authentication server sturen.



Figuur 4: MAB communicatie

Het grote voordeel van MAB als beveiligingsmechanisme is, dat deze hetzelfde proces volgt als 802.1x, waardoor relatief weinig aanpassingen nodig zijn in een bestaande 802.1x omgeving. Tevens kan er gebruik gemaakt worden van het AAA protocol. Zodat functies als dynamisch een netwerk toewijzen (Autorisatie) nog steeds beschikbaar zijn.

Één van de grootste nadelen van de bovenstaande techniek is, dat deze gebaseerd is op het MAC adres van een apparaat. Het is namelijk relatief eenvoudig om een fictief MAC adres op een apparaat te zetten. Op deze manier is het bijv. mogelijk om een laptop te authenticeren als een pinpad.

Een ander belangrijk punt dat gezien kan worden als nadeel is, dat deze techniek momenteel alleen binnen Cisco apparaten te gebruiken is en het geen officiële standaard is.

HP switches ondersteunen ook MAC authenticatie, middels het RADIUS protocol. Echter is hier geen sprake van MAB. Het is namelijk of 802.1x of MAC authenticatie. Het is niet mogelijk om automatisch van 802.1x over te schakelen naar MAC authenticatie.

4.2.5 Port-Security

Port-Security, is de tweede techniek, die naast MAB gebruik maakt van het MAC adres voor Authenticatie. Voor deze techniek wordt op elke poort op de switch een MAC adres ingesteld, welke een verbinding mag maken. Ter verduidelijking een tabel.

Switchpoort	MAC-adres
1	00-0F-FE-C7-D7-22
2	00-0F-FE-DE-23-C2
3	00-0F-FE-12-DD-E2
…	…

Figuur 5: MAC Authenticatie Tabel

Uit bovenstaande tabel blijkt, dat het apparaat met MAC adres 00-0F-FE-C7-D7-22, alleen een verbinding mag maken op poort 1. Op het moment dat de kabel van poort 1 in poort 2 wordt gestoken, zal de switch de poort dichtzetten en is er geen verbinding mogelijk.

Op deze techniek bestaan een aantal variaties, die per leverancier verschillen, doch elke leverancier ondersteunt deze techniek. Zo is het bijvoorbeeld vaak mogelijk om een dynamische lijst op te bouwen van MAC adressen die verbinding kunnen maken via elke poort. Soms is het zelfs mogelijk om deze lijst te distribueren over meerdere switches. Ook kun je vaak meerdere MAC adressen per poort definiëren, dit kan bijv. nodig zijn, wanneer een HUB gekoppeld wordt aan een poort.

Deze techniek heeft net als MAB het grote nadeel, dat deze beveiliging relatief makkelijk te omzeilen is. Daarnaast is een groot nadeel dat deze techniek erg onderhoudsgevoelig is. Er moet vaak per switch een lijst met MAC adressen worden bijgehouden die verbinding mogen maken. Op het moment dat gebruik wordt gemaakt van statische koppelingen, zal tijdens een verhuizing van systemen elke poort handmatig moeten worden aangepast. Ook verlies je met deze techniek de mogelijkheid voor het AAA protocol.

Om het beheer te vereenvoudigen zijn er wel softwarepakketten en scripts beschikbaar, die dit automatiseren. Deze scripts en software zijn echter wel vaak toegespitst op een specifiek merk of type.

4.2.6 Captive Portal

De Captive Portal, ook wel Web Authentication of hotspot genoemd, is een techniek die in tegenstelling tot MAB en MAC Authenticatie gebruik maakt van “dynamische” inloggegevens. Meestal zal dit een combinatie van een gebruikersnaam en wachtwoord inhouden. In sommige gevallen kan deze authenticatie ook bestaan uit het accepteren van bepaalde voorwaarden voor het gebruik van het netwerk.

Bij de captive portal maakt een apparaat verbinding met het netwerk, maar dit zal een zeer beperkt netwerk zijn. Als de gebruiker binnen dit netwerk zijn Internet browser opstart en naar een pagina gaat, die zich niet op zijn eigen systeem bevind. Dan zal de browser een webpagina laten zien, waarbij gevraagd wordt om te authenticeren.

Figuur 6: Voorbeeld Captive Portal

De technische implementaties om een cliënt altijd op een specifieke webpagina uit te laten komen variëren enigszins. De technische details zijn niet belangrijk om het project tot een goed einde te brengen en reiken buiten de scoop van het project. Om toch een korte indicatie te geven, worden hieronder twee veelgebruikte methoden benoemd;

- Alle http requests afvangen en als response de inlogpagina geven.
- De DNS servers vervangen middels DHCP en alle DNS requests naar de inlogpagina door verwijzen of als subdomein, bijv. “www.google.com.nactest.local”.

In de meeste gevallen wordt in deze oplossing een RADIUS server gebruikt voor authenticatie, waardoor het AAA protocol weer beschikbaar is. Ook is deze oplossing vaak te gebruiken op vrijwel alle apparaten, als deze maar de beschikking hebben over een web browser. Een nadeel van deze oplossing is, dat er vrij veel manieren zijn om deze te implementeren. Ook is er een “beperkte” verbinding met het netwerk vereist.

4.2.7 Conclusie beveiligingsmechanismen

Zoals uit het voorgaande blijkt is 802.1x het meest gewenste beveiligingsmechanisme. Helaas wordt deze niet ondersteund door alle apparaten. Voor deze apparaten zal gebruik moeten worden gemaakt van MAB of Captive Portal. MAC authenticatie kan het beste zoveel mogelijk vermeden worden, omdat de MAC gebaseerde oplossingen het minst veilig zijn en onderhoudsgevoelig. Ook is AAA in dit project gewenst, omdat deze de mogelijkheid biedt om middels Autorisatie dynamisch een netwerk toe te kennen. Helaas is het soms de enige optie en is het altijd nog beter als geen beveiliging.

	AAA	Gebruiker bekend	MAC gebaseerd
802.1x	√	√	X
MAB	√	X	√
MAC	X	X	√
Captive Portal	√	√	X

Tabel 3: Beveiligingsmechanismen

Het is belangrijk om te weten dat de meeste netwerkapparaten meerdere vormen van beveiliging op één poort kunnen zetten. Hierdoor is het mogelijk om zeer flexibel om te gaan met de beveiliging en apparaten te verhuizen van de ene switchpoort naar de andere, zonder dat configuraties gewijzigd hoeven te worden.

4.3 Toegangscontrole matrix

Nu de apparaten en de beveiligingsmechanismen zijn besproken, is het belangrijk om te weten welke beveiligingsmechanismen op welk apparaat toepasbaar zijn. Het kan immers niet zo zijn dat een pinpad niet op het netwerk kan komen, omdat deze geen 802.1x ondersteunt.

Ook hier wordt onderscheid gemaakt tussen hoofdkantoor inclusief de distributiecentra in Veghel en de decentrale vestigingen.

Apparaat	802.1x	Web-based	MAC	Toestaan
Hubs	Nee	Nee	Ja	Nee
Laptops (Buiten)	Meestal	Ja	Ja	Ja
Laptops (Sligro)	Ja	Ja	Ja	Ja
Mac's	Ja	Ja	Ja	Ja
NC's	Ja	Ja	Ja	Ja
PC's	Ja	Ja	Ja	Ja
PDA's / Smartphones	Soms	Meestal	Ja	Ja
Printers / multifunctionals	Soms	Soms	Ja	Ja
PTL Boxen (QNX)	Nee	Nee	Ja	Ja
Servers	Ja	Ja	Ja	Ja
Switches	Soms	Nee	Ja	Nee

Tabel 4: Beveiligingsmechanisme per apparaat hoofdkantoor en distributiecentra Veghel.

Uit de tabel blijkt dat hubs en switches in de toekomst ongewenst zijn. Onder switches wordt in dit geval verstaan de "losse" switches, die buiten het netwerkdesign vallen. Reden hiervoor is dat deze switches het netwerk onoverzichtelijk maken en de beveiliging extra gecompliceerd. Ook brengen deze apparaten een verhoogd risico op storingen met zich mee. Denk hierbij bijvoorbeeld aan spanningtree loops (oneindige lussen in het netwerk).

Verder wordt geen netwerktoegangscontrole geconfigureerd voor de servers. Deze bevinden zich namelijk allemaal in een afgesloten locatie, die alleen onder toezicht van de datacenter beheerder kan en mag worden bezocht.

Apparaat	802.1x	Web-based	MAC	Toestaan
Hubs	Nee	Nee	Soms	Nee
Laptops (Buiten)	Meestal	Ja	Ja	Nee
Laptops (Sligro)	Ja	Ja	Ja	Ja
NC's	Ja	Ja	Ja	Ja
PC's (Sligro)	Ja	Ja	Ja	Ja
PDA's / Smartphones	Soms	Meestal	Ja	Nee
Pinpads	Nee	Nee	Ja	Ja
Printers / multifunctionals	Soms	Soms	Ja	Ja
PTL Boxen (QNX)	Nee	Nee	Ja	Ja
Reflex	Soms	Ja	Ja	Ja
Servers	Ja	Ja	Ja	Ja
Switches	Soms	Nee	Ja	Nee
Weegschalen	Nee	Nee	Ja	Ja

Tabel 5: Beveiligingsmechanisme per apparaat decentrale vestigingen.

Voor de vestigingen willen we evenmin hubs en switches op het netwerk. Op de vestigingen willen we daarnaast ook geen netwerk toegang voor PDA's, Smartphones en laptops die niet in het beheer van Sligro zijn. Op deze locaties worden de servers ook buiten de toegangscontrole gehouden.

4.4 Intrusion Detection

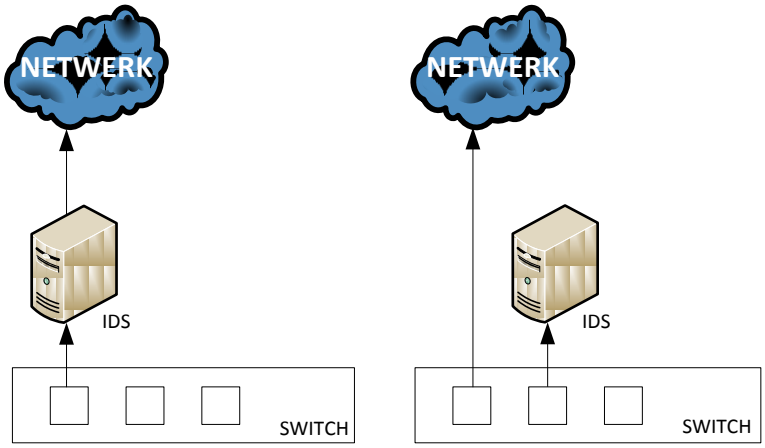
Middels AAA is het mogelijk om apparaten dynamisch een netwerk toe te kennen. Hiermee is het mogelijk om een classificatie te maken. Zo worden bijvoorbeeld apparaten die toegang verkrijgen tot het netwerk middels MAC authenticatie in een apart netwerk geplaatst. Deze beveiligingsmethode is namelijk relatief makkelijk te omzeilen, hetgeen als gevolg heeft dat deze apparaten minder vertrouwd zijn.

Deze apparaten kunnen onderling van het netwerk worden gescheiden. Zo kunnen printers worden opgenomen in een apart netwerk waar een restrictie aanwezig is, zodat enkel gecommuniceerd kan worden met de printserver. Tevens kan gebruik worden gemaakt van een Intrusion Detection systeem.

Een netwerk Intrusion Detection systeem scant al het netwerkverkeer en zoekt naar ongewenst gedrag. Meestal gebeurt dit door al het verkeer te toetsen aan vooropgestelde regels. Indien het verkeer overeenkomt met zo'n regel, dan is sprake van een alarm. De plaats van een Intrusion Detection System (IDS) in het netwerk is erg belangrijk. Als een IDS verkeerd geplaatst wordt, kan dit het hele netwerk vertragen of zelfs onwerkbaar maken.

Er zijn twee oplossingen om een IDS te plaatsen, dit is enerzijds "in-line", in dit geval moet al het verkeer door de IDS heen, alvorens dit doorgestuurd wordt. Dit heeft als voordeel dat ongewenst verkeer, onmiddellijk kan worden tegen gehouden. Het nadeel hiervan is, dat de IDS als een trechter kan werken, daar al het verkeer hier immers doorheen moet. Als dit systeem het verkeer niet snel genoeg scant en doorstuurt, heeft het achterliggende verkeer hier last van.

Anderzijds kan de IDS "out-of-band" geplaatst worden. Hierbij staat de IDS als het ware buiten het netwerk. Er wordt op de switch een zogenaamde monitorpoort (remote-span) aangemaakt, waar de IDS aan gekoppeld wordt. Op deze monitorpoort wordt ingesteld, dat deze ook al het verkeer van een bepaalde poort of netwerk (VLAN) naar buiten stuurt. Voordeel hiervan is, dat het overige netwerkverkeer hiervan geen hinder ondervindt op het moment dat de IDS het te druk heeft. Nadeel hiervan is, dat een reactie altijd reactief en daardoor te laat is. Het verkeer is namelijk gelijktijdig ook over een andere poort naar buiten gestuurd.



Figuur 7: Links IDS "in-line", rechts IDS "out-of-band"

Een IDS is een extra beveiliging, die netwerkverkeer en vooral het misbruik hiervan goed in kaart kan brengen. Helaas zijn vrijwel alle IDS oplossingen zeer onderhoudsgevoelig. De regels die gebruikt worden om het verkeer aan te toetsen moeten namelijk up-to-date blijven, zodat ook nieuwe risico's gedetecteerd worden. Naast het bijhouden van deze regels, heeft een IDS ook alleen nut als er actie ondernomen wordt op de gegenereerde alarmen. Ook dit kost de nodige inspanning. Wel kunnen vaak de acties op repeterende alarmen geautomatiseerd worden.

5. Testomgeving

In het onderzoek zijn de mogelijkheden voor netwerktoegangscontrole behandeld. Nu dit kader is geschetst, kan de testomgeving worden opgebouwd. Deze testomgeving moet een goed beeld kunnen geven, hoe de netwerktoegangscontrole in de pilot opstelling zal reageren. Tevens zullen de verschillende voor- en nadelen in kaart worden gebracht.

5.1 Opzet testomgeving

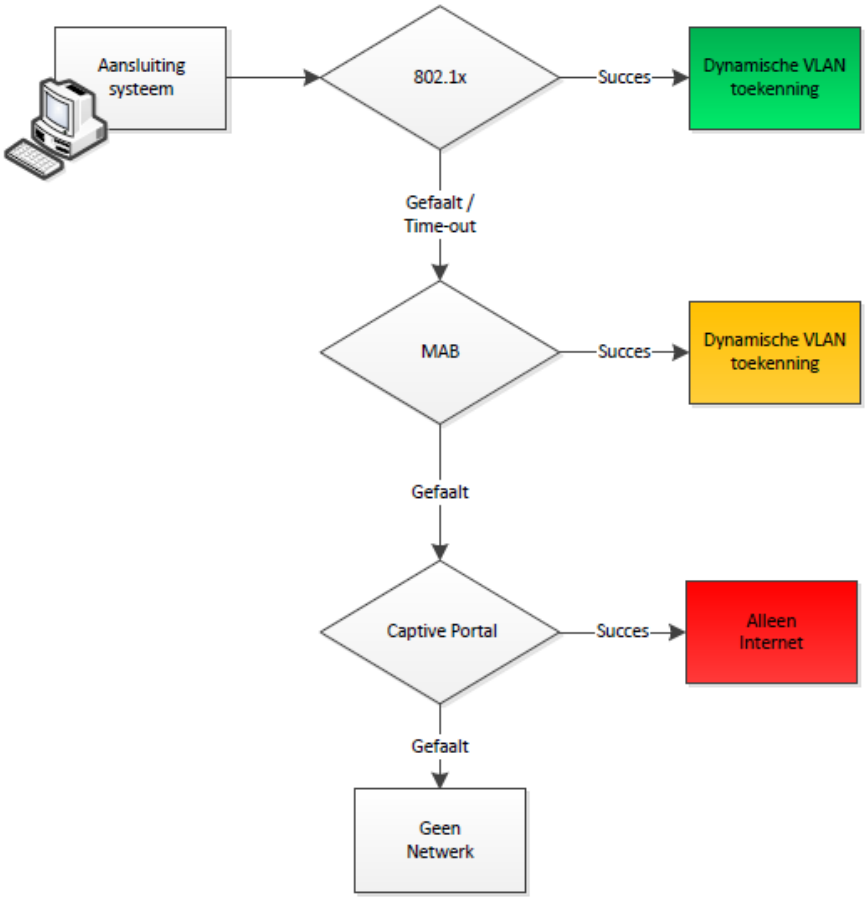
Evenals bij het onderzoek, wordt onderscheid gemaakt tussen het hoofdkantoor met de distributiecentra in Veghel en de decentrale vestigingen. Naast de verschillende systemen die toegang tot het netwerk nodig hebben, zijn de apparaten die deze toegang verlenen verschillend. Op het hoofdkantoor en de distributiecentra worden alle aansluitpunten verzorgd door Cisco 3750 switches en op de decentrale vestigingen wordt gebruik gemaakt van HP Procurve 2600 switches. Ook dient rekening gehouden te worden met de centrale opzet van de ICT omgeving. Dit zou kunnen betekenen dat alle apparaten die gecontroleerd moeten worden, afhankelijk zijn van de server die zich op het hoofdkantoor bevindt. Dit kan extra risico's met betrekking tot de continuïteit met zich brengen. Als deze server uit zou vallen, zou dit betekenen dat er geen apparaten op de decentrale vestigingen op het netwerk kunnen. Als laatste punt willen we op de decentrale vestigingen alleen apparaten toestaan die in het beheer van Sligro zijn. Op het hoofdkantoor moeten ook apparaten die niet in Sligro beheer zijn op het netwerk kunnen. Dit kunnen bijvoorbeeld laptops zijn van ICT partners of leveranciers. Dit netwerk zal de gebruikers alleen toegang geven tot het Internet.

5.1.1 Hoofdkantoor en distributiecentra Veghel

Doelstelling is dat alle apparaten gekoppeld kunnen worden, waaraan toegang is verleend. In de eerste instantie willen we zoveel mogelijk apparaten laten authenticeren via het 802.1x protocol. Dit is namelijk het meest veilig.

Het 802.1x protocol wordt niet door alle apparaten ondersteund. Voor de apparaten waar dit protocol niet werkt wordt geschakeld naar MAB, dit is immers apparaatonafhankelijk. Hiervoor dient er wel een database met MAC adressen te worden bijgehouden. Dit is geen probleem voor apparaten die in eigen beheer zijn, omdat hier de MAC adressen van bekend zijn. Daarnaast dient men wel voor ogen te houden dat deze methode (MAB) relatief makkelijk te omzeilen is. Hiervoor worden apparaten die zich middels deze manier authenticeren in een apart netwerk geplaatst. Op dit netwerk zullen restricties komen te staan en wordt actief gecontroleerd op ongeoorloofd gedrag.

Met de voornoemde methoden kunnen alle apparaten die in eigen beheer zijn authenticeren, alvorens ze toegang tot het netwerk verkrijgen. De laatste stap is dan ook om de apparaten die niet in eigen beheer zijn een mogelijkheid tot authenticatie te geven. Dit kan door middel van een Captive Portal. Apparaten die zich middels een Captive Portal hebben aangemeld, krijgen alleen toegang tot een netwerk waar Internet toegang is.

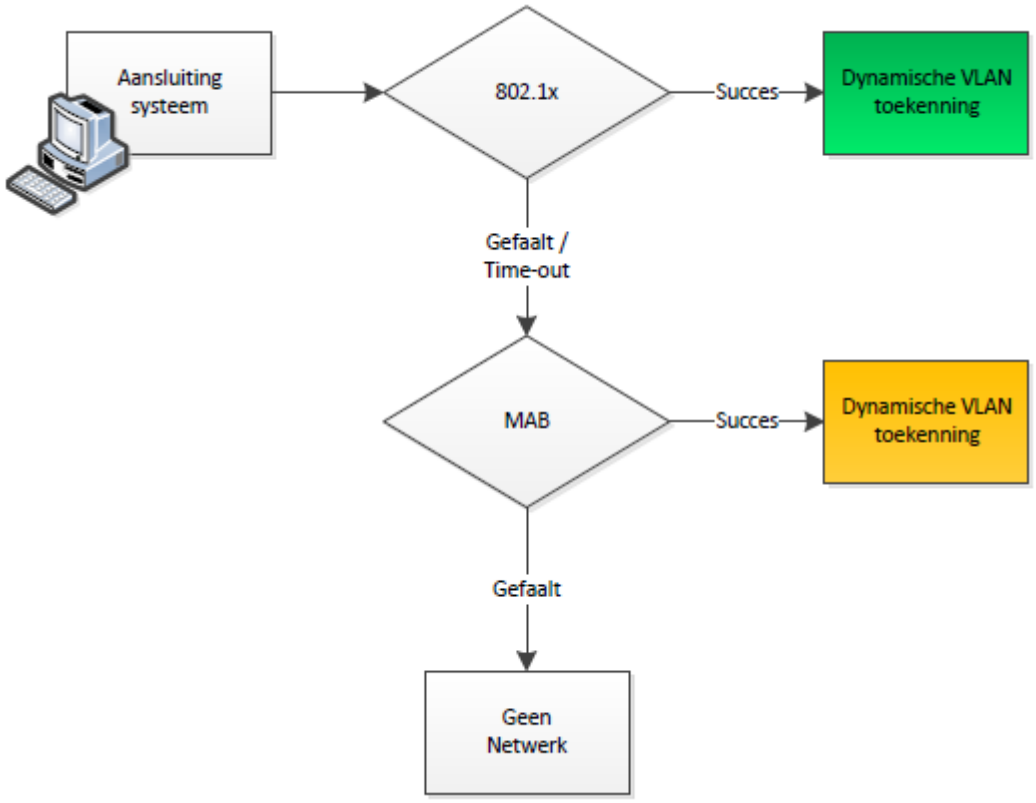


Figuur 8: Netwerktoegangscontrole proces Sligro hoofdkantoor en distributiecentra in Veghel

Zoals reeds genoemd, zijn alle switches op het hoofdkantoor en de distributiecentra in Veghel Cisco 3750 switches. Het is belangrijk om te weten of deze switches de bovengenoemde beveiligingsmechanismen ondersteunen en of deze ook in de bovenstaande volgorde uitgevoerd kunnen worden. Dit is gelukkig het geval, indien de switch van een bepaalde firmware versie is voorzien (dit moet minimaal versie 12.2(50)SE zijn.

5.1.2 Decentrale vestigingen

Voor decentrale vestigingen is het proces minder gecompliceerd. Hier mogen immers geen externe apparaten op het netwerk, die niet in eigen beheer zijn. Een schematisch overzicht van het proces ziet er dan als volgt uit.



Figuur 9: Netwerktoegangscontrole proces decentrale vestigingen.

Op de decentrale vestigingen wordt gebruik gemaakt van HP Procurve 2600 switches. Deze switches ondersteunen eveneens de voornoemde beveiligingsmechanismen. De firmware voor deze switches moet minimaal versie 10.59 zijn voor een correcte werking.

5.2 Testopstelling

De testomgeving werd zo identiek mogelijk opgebouwd, om de verschillen tussen de pilot omgeving de “werkelijke” omgeving zo veel mogelijk te beperken. Hieronder worden de verschillende componenten benoemd.

5.2.1 Cisco 3750

Op het hoofdkantoor en de distributiecentra in Veghel zijn alle access switches[3]: Cisco 3750’s. Voor de testomgeving hebben we dan ook eenzelfde Cisco 3750 gebruikt. De firmware is in de testomgeving naar versie 12.2 (53) SE1 gebracht, zodat alle beveiligingsmechanisme getest kunnen worden.

5.2.2 HP 2650

Op alle decentrale vestigingen wordt gebruik gemaakt van HP Procurve switches. Dit is altijd de 2600 serie. In de meeste gevallen is het een 26 poorts switch, de HP 2626. Op sommige locaties wordt echter gebruik gemaakt van een 50 poorts variant, de HP 2650. De functionaliteiten zijn voor beide switches hetzelfde en ze maken eveneens gebruik van dezelfde firmware. In de testomgeving is gebruik gemaakt van firmware versie 10.83.

5.2.3 Radius server

De gewenste beveiligingsmechanismen, zoals 802.1x, MAB/MAC-authenticatie en Captive Portal kunnen op de achtergrond allemaal gebruik maken van een RADIUS server. Hierdoor kan gewerkt worden met het AAA protocol en is het beheer te centraliseren.

Voor de RADIUS server is gekozen voor Microsoft Network Policy Server. Dit is Microsofts RADIUS server en de opvolger van Internet Authentication Server (IAS) die nog in Windows 2003 te vinden was. De NPS draait op Windows 2008 en heeft een directe koppeling met Active Directory. Dit heeft onder meer als voordeel, dat:

- Beheer bekend is met Windows 2008 & Active Directory;
- Er geen extra server benodigd is in de uiteindelijke situatie;
- Een centrale database (LDAP/AD) voor alle gebruikers bestaat;
- In de toekomst makkelijk NAP (Network Access Protection) te implementeren is;
- Cisco en MS nauw samen werken m.b.t. Netwerktoegangscontrole. [4]

Om de testomgeving realistischer te maken, heeft de server naast RADIUS nog een aantal functionaliteiten, te weten, Domain controller, DHCP server en DNS server.

[3] Access switches, zijn de switches waaraan de apparaten van de eindgebruikers gekoppeld worden.
[4] http://www.cisco.com/web/BE/press/pdfs/NAC-NL.pdf

5.2.4 Netwerk

Voor het netwerk is gekozen om een opstelling te maken, die gebruik maakt van beide typen switches. De onderstaande VLANs die als gescheiden netwerken gezien mogen worden, zijn beschikbaar gemaakt op beide switches. De Cisco 3750 kan naast deze netwerken aanbieden ook routeren. Zo kan er ook verkeer tussen de verschillende VLANs plaatsvinden.

Hieronder een overzicht van de aanwezige netwerken en het bijbehorende IP plan.

VLAN ID	Naam	IP Reeks
11	802.1x authenticated cliënts	10.10.11.0/24
14	Beheerders	10.10.14.0/24
31	MAC authenticated Cliënts	10.10.31.0/24
300	Servers	10.2.50.0/24
666	Internet	192.168.1.0/24
900	Beheer	10.0.0.0/24

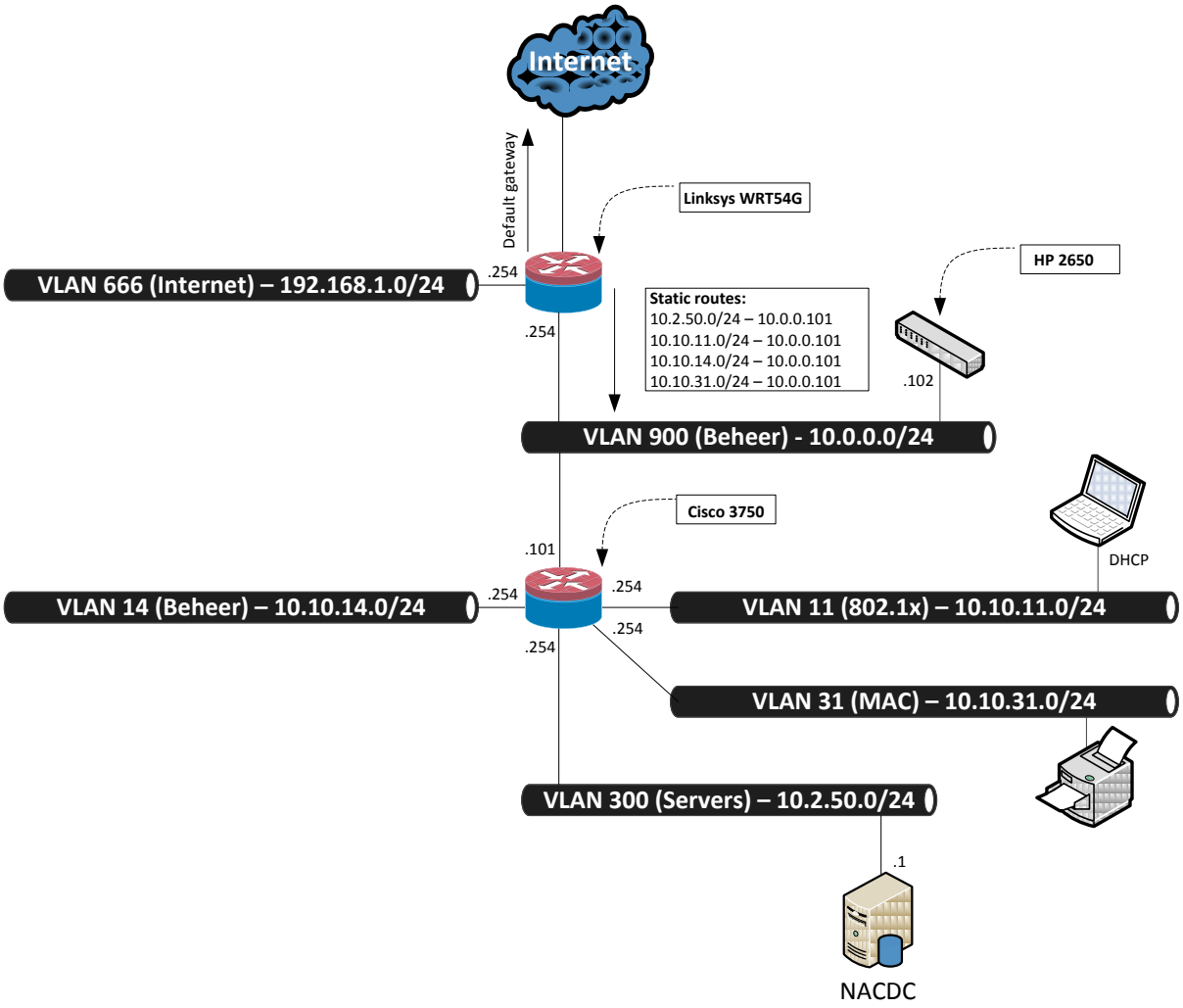
Tabel 6: VLAN Plan met bijbehorende IP-Reeksen

IP adres	Functie	Apparaat
10.0.0.101/24	Beheer / Gateway	Cisco 3750
10.0.0.102/24	Beheer	HP 2650
10.0.0.254/24	Internet Gateway	Linksys WRT54G
10.10.11.1 – 10.10.22.150	DHCP pool	802.1x authenticated clients. (domein computers)
10.10.11.254	Gateway VLAN 11	Cisco 3750
10.10.14.0 – 10.10.14.150	DHCP Pool	802.1x authenticated clients. (Beheerders)
10.10.31.1 – 10.10.31.150	DHCP pool	MAB authenticated cliënts. Bijv. Printers.
10.10.31.254	Gateway VLAN 31	Cisco 3750
10.2.50.1	NPS (RADIUS) / DC / AD / NPS	NPS Server
10.2.50.254	Gateway VLAN 300	Cisco 3750
192.168.1.0 – 192.168.1.150	DHCP pool	Captive Portal Authenticated cliënts.
192.168.1.254	Gateway VLAN 666	Linksys WRT54G

Tabel 7: IP adressen met bijbehorende functie en apparaat

Hieronder is een schematisch overzicht te zien, waarin aangegeven wordt welk apparaat waar gekoppeld zit en hoe de communicatie tussen de verschillende apparaten verloopt. Dit wordt een zogenaamde laag 3 (OSI model) tekening genoemd.

Let op! Belangrijk om te weten is dat de HP2650 switch te bereiken is op IP adres 10.0.0.102, maar dat deze wel alle netwerken ondersteunt, middels VLANs. Dit is in een laag 3 tekening niet te zien, omdat niet elk netwerk op elke switch een IP adres (interface) hoeft te hebben.



Figuur 10: Testopstelling netwerktoegangscontrole (Laag 3)

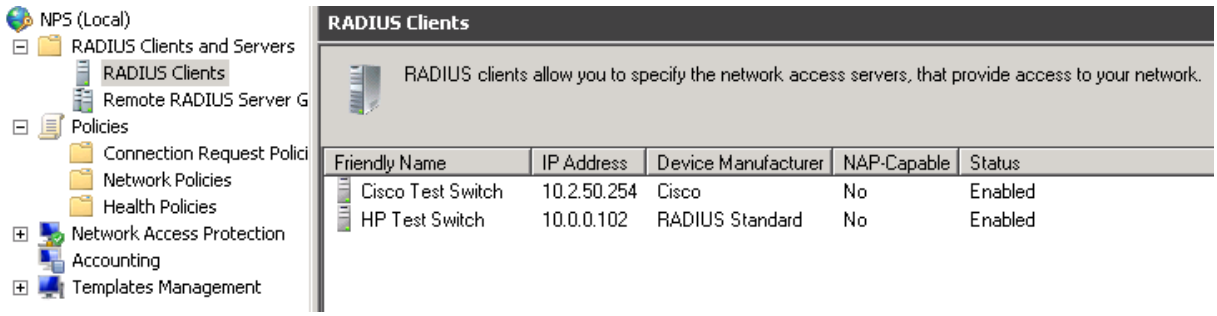
5.2.5 Configuratie

Als we terugblikken op het proces wat doorlopen moet worden, dan is hier maar een kleine afwijking tussen decentrale vestigingen en het hoofdkantoor en distributiecentra in Veghel. Hieronder staat dan ook de configuratie van beide type switches.

5.2.5.1 NPS

De verschillende beveiligingsmechanismen maken gebruik van een RADIUS server. Als RADIUS server is gekozen voor Microsoft Network Policy Server. Na de installatie hiervan, moeten de RADIUS Cliënts toegevoegd worden. De cliënts zijn de switches welke een authenticatie mogen doen bij de NPS.

In de NPS configuratie, moeten de switches toegevoegd worden onder “RADIUS Cliënts”. Hierbij moet een “key” opgegeven worden, zodat niet elk apparaat met de RADIUS server kan communiceren. Deze “key” is verplicht, bleek tijdens de tests. In de testomgeving is de volgende key gebruikt “nackey”.



Figuur 11: NPS Radius Clients (authenticators)

Vervolgens zal op de switches bekend gemaakt moeten worden welke RADIUS server deze moeten gebruiken en welke “key” ze hiervoor benodigd hebben.

Hieronder staan voor beide switches welke commando’s gebruikt moeten worden om de RADIUS server bekend te maken.

HP Procurve 2650

```
radius-server host 10.2.50.1 auth-port 1645 acct-port 1646
radius-server key nackey
```

Cisco 3750

```
aaa new-model
radius-server host 10.2.50.1 auth-port 1645 acct-port 1646
radius-server key nackey
```

Microsoft NPS maakt standaard nog gebruik van de oude standaard poorten 1645 en 1646 voor respectievelijk authenticatie en autorisatie. De switches willen gebruik maken van poorten 1812 en 1813, die de nieuwe standaard zijn.

De specifieke NPS configuratie die benodigd is voor elk beveiligingsmechanisme, wordt hieronder per mechanisme toegelicht.

5.2.5.2 802.1x

Voor 802.1x kunnen twee vormen van authenticatie plaats vinden. Voor alle computers die lid zijn van het domein, gebeurt dit middels het computeraccount[5]. Naast de mogelijkheid om computers te laten authenticeren, moet er een mogelijkheid zijn voor beheerders om computers buiten het domein, toegang te geven tot het netwerk. Door deze scheiding te maken, wordt voorkomen dat elke gebruiker met zijn privé pc/laptop en met zijn gebruikersnaam en wachtwoord toegang krijgt tot het Sligro netwerk.

De computers die lid zijn van het domein krijgen na een succesvolle authenticatie toegang tot het "default" switch VLAN. Elke "Secondary Equipment Room" (SER), krijgt een eigen VLAN tot zijn beschikking. Dit VLAN wordt het default VLAN voor de switches in deze ruimte. In de testopstelling is VLAN 11 het default VLAN.

Een beheerder die middels 802.1x toegang verschaft krijgt echter een dynamisch VLAN toegewezen. Het zogenaamde "beheerders" VLAN. Middels dit VLAN zijn specifiekere onderdelen in het netwerk te bereiken, denk hierbij aan DMZ en RSA VLANS.

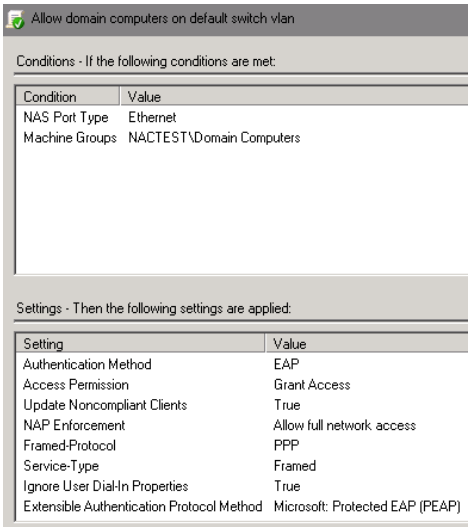
Nadeel van deze methode is wel, dat cliënts in het domein moeten worden geplaatst, door "beheerders" die middels 802.1x authenticatie connectie met het netwerk kunnen maken.

Om het bovenstaande te realiseren, dienen er twee regels binnen de NPS aangemaakt te worden. De eerste regel voor domein computers ziet er als volgt uit.

Binnen de "Connection Request Policies" word niks verandert. In de "Network Policies" wordt een nieuwe regel toegevoegd.

In deze regel wordt een conditie toegevoegd, dat deze regel bedoeld is voor alle computers die lid zijn van de groep "Domain Computers".

Verder moet aangeven worden welk protocol voor authenticatie wordt gebruikt. Dit is standaard MS Protected EAP (PEAP). Ook is het belangrijk om te controleren of er bij Access Permission "Grant Access" is ingevuld.

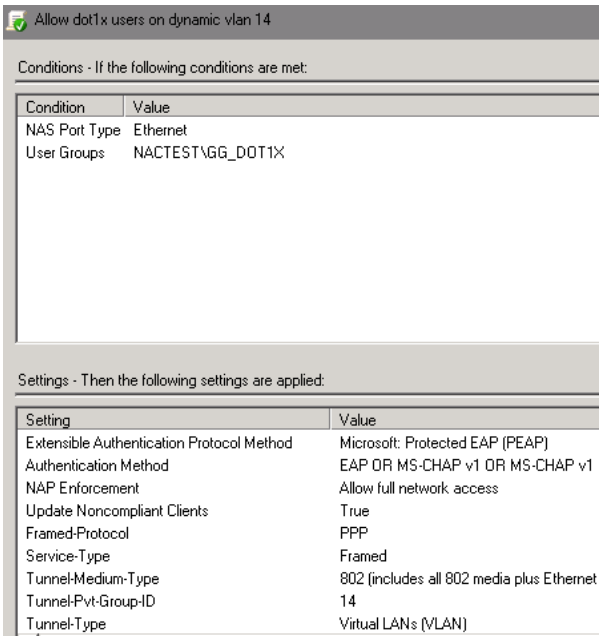


Figuur 12: NPS toegang domein computers

De tweede regel die toegevoegd moet worden, is de regel die specifieke gebruikers de mogelijkheid geeft om zichzelf aan te melden middels gebruikersnaam en wachtwoord. Zodat deze de mogelijkheid hebben om extra rechten op het netwerk te verkrijgen of met apparaten verbinding te maken die wel 802.1x ondersteunen, maar geen lid zijn van het domein.

[5] Computers die lid zijn van een domein krijgen een domeinaccount, deze bestaat uit computernaam en wachtwoord.

Om deze tweede regel aan te kunnen maken moet allereerst een nieuwe groep gemaakt worden in Active Directory. Hierin worden gebruikers geplaatst, die de bovenstaande mogelijkheid moeten krijgen. In de testomgeving heet deze groep “GG_DOT1X” en is de gebruiker “maasr” hier lid van.



Figuur 13: NPS toegang specifieke gebruikers

Deze tweede regel wordt eveneens toegevoegd aan “Network Policies”.

Echter aan de conditie wordt nu de groep toegevoegd, die zojuist binnen Active Directory is aangemaakt.

PEAP is hier voldoende voor authenticatie, maar deze kan uitgebreid worden met andere methoden.

Om dynamisch een VLAN toe te kennen, dienen er nog drie extra parameters ingevuld te worden. Dit zijn Tunnel-Medium-Type, Tunnel-Pvt-Group-ID en Tunnel-Type.

In de Tunnel-Medium-Type wordt het medium aangegeven aan, dit is 802[6].In Tunnel-Pvt-Group-ID wordt het VLAN ID aangegeven. Dit wordt VLAN 14. En bij Tunnel-Type wordt aangegeven dat het om VLAN toekenning gaat.

Nu de NPS (RADIUS) ingericht is, moeten we de authenticator inrichten.

HP Procurve 2650

```
aaa authentication port-access eap-radius
aaa port-access authenticator 1-48
aaa port-access authenticator active
vlan 11
   name "Auth_Vlan"
   untagged 1-48
   tagged 49-50
   exit
vlan 14
   name "Beheerders"
   tagged 49-50
   exit
```

[6] Alle IEEE standaarden voor netwerken beginnen met 802.

Cisco 3750

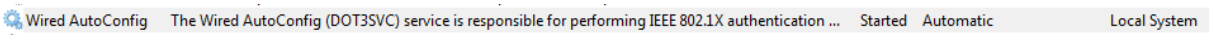
```
aaa authentication dot1x default group radius
aaa authorization network default group radius
interface FastEthernet1/0/1
   switchport access vlan 11
   switchport mode access
   switchport nonegotiate
   authentication port-control auto
   dot1x pae authenticator
   spanning-tree portfast
!
interface Vlan11
   description AuthenticatedClientVlan
   ip address 10.10.11.254 255.255.255.0
   ip helper-address 10.2.50.1
!
interface Vlan14
   description Administrators
   ip address 10.10.4.254 255.255.255.0
   ip helper-address 10.2.50.1
!
```

Op de Cisco 3750 wordt per poort (interface FastEthernet) ingesteld of deze wel of geen 802.1x authenticatie ondersteunt. Hierboven is dit alleen voor poort 1 afgebeeld. Verder staan hier ook de gateways voor de VLANS gespecificeerd.

Om het “online” komen van de poort na succesvolle authenticatie te bespoedigen zijn er twee extra opties meegegeven aan de poort. Spanning-tree portfast en switchport nonegotiate. Beiden voorkomen dat de switch een aantal zaken gaat controleren alvorens de cliënt toegang te geven. Dit duurt zonder deze extra parameters zo’n 30 seconden, met deze parameters is dit zo’n 2 seconden.

Nu de switches zijn ingesteld, hoeven we alleen nog de cliënts (supplicant) in te stellen, zodat deze authenticeren middels 802.1x.

De authenticatie door middel van de computer account, werkt alleen voor computers die lid zijn van het domein. De instellingen zijn vrij eenvoudig te maken. Allereerst moet gezorgd worden dat de service “Wired Autoconfig” gestart is. Deze word dan ook op automatisch starten gezet.



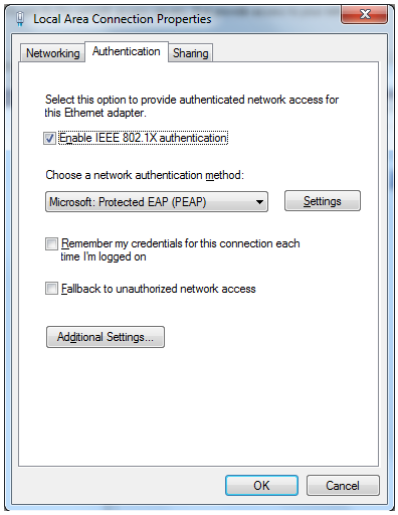
Figuur 14: Wired AutoConfig service

Deze service zorgt, dat onder de eigenschappen van de netwerkverbinding een extra tabblad “Authenticatie” verschijnt.

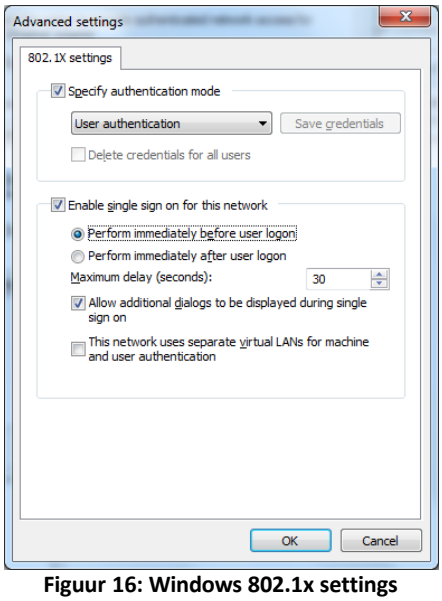
Om 802.1x te activeren, moet op dit tabblad een vinkje gezet worden voor “Enable IEEE 802.1X authentication”.

Vervolgens moet de authenticatie methode gekozen worden. PEAP is in ons geval voldoende.

Onder de knop “Additional Settings” kan vervolgens gekozen worden of aan computer authenticatie of user authenticatie gedaan moet worden. Voor computers in het domein, kan deze op computer authenticatie gezet worden.



Figuur 15: Windows 802.1x Authentication



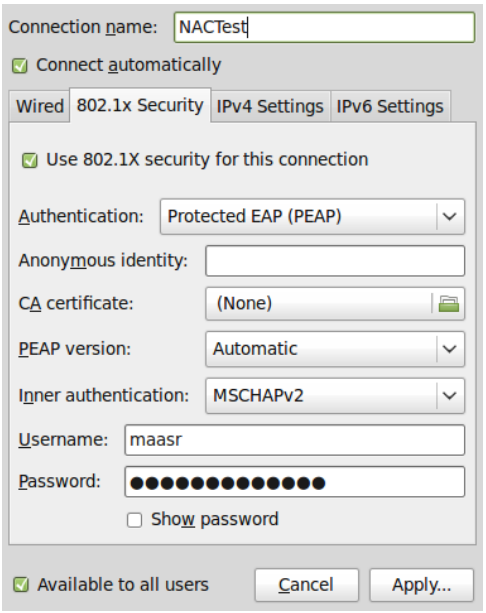
Figuur 16: Windows 802.1x settings

Voor user authentication zijn er echter wat uitzonderingen. Als de computer in het domein hangt is het belangrijk dat een netwerkverbinding voor handen is, alvorens getracht wordt in te loggen.

Om hiervoor te zorgen wordt het vinkje “Enable single sign on for this network” aangezet. Vervolgens is het belangrijk om “Perform immediately before user logon” te selecteren. Nu wordt met de Windows credentials een 802.1x authenticatie uitgevoerd, alvorens de domeincontroller wordt benaderd.

Voor computers die niet in het domein zijn geplaatst is dit niet van toepassing en is user authentication voldoende. Wel is het belangrijk om in dit geval onder “settings” op het tabblad authenticatie “Validate server certificate” uit te zetten.

In Linux kan alleen voor user authenticatie worden gekozen. Dit is eenvoudig te doen, door een nieuw netwerkprofiel aan te maken en de gegevens op het tabblad 802.1x in te vullen.



Figuur 17: Linux 802.1x security

5.2.5.3 MAB

Als 802.1x authenticatie niet ondersteund wordt door het apparaat, moet er naar een ander authenticatiemechanisme overgeschakeld worden. Apparaten die veelal geen 802.1x ondersteunen zijn printers, scanners, pinpads en weegschalen. Het kan natuurlijk niet zo zijn dat deze apparaten niet meer kunnen werken.

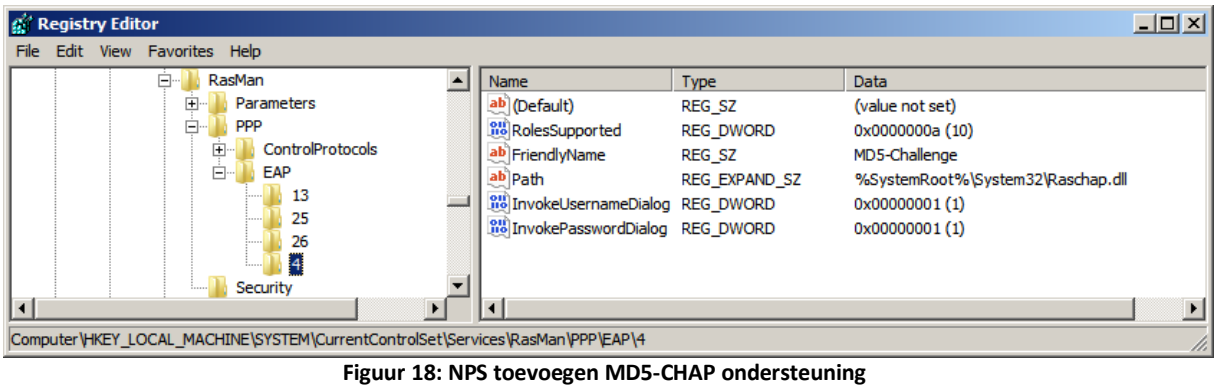
Voor de HP switches is een workaround bedacht, om toch beide protocollen, 802.1x en MAB gelijktijdig aan te kunnen bieden. Hierdoor kan overal met RADIUS gewerkt worden en worden de voordelen van het AAA protocol benut.

Voor de HP MAC Authenticatie via RADIUS dienen er een aantal zaken aangepast te worden aan de NPS server. HP gebruikt namelijk voor zijn MAC Authenticatie een protocol die niet meer wordt ondersteund binnen Windows 2008 R2. Dit protocol MD5-Chap wordt niet meer ondersteund, omdat het relatief makkelijk te kraken is middels een zogenaamde “dictionary attack”. Echter voor MAC-Authenticatie is dit niet erg, want het MAC adres is immers op veel eenvoudigere wijzen te achterhalen.

Dit protocol MD5-Chap is nog wel in te schakelen, maar hiervoor moeten er wat wijzigingen gemaakt worden aan het register[7].

Zo moet er een “sleutel” met de waarde 4 aangemaakt worden onder “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\PPP\EAP\”.
In deze nieuwe “sleutel” dienen een aantal variabelen geplaatst te worden;

RolesSupported	REG_DWORD	0x0000000a
FriendlyName	REG_SZ	MD5-Challenge
Path	REG_EXPAND_SZ	%SystemRoot%\System32\Raschap.dll
InvokeUsernameDialog	REG_DWORD	0x00000001
InvokePasswordDialog	REG_DWORD	0x00000001



Figuur 18: NPS toevoegen MD5-CHAP ondersteuning

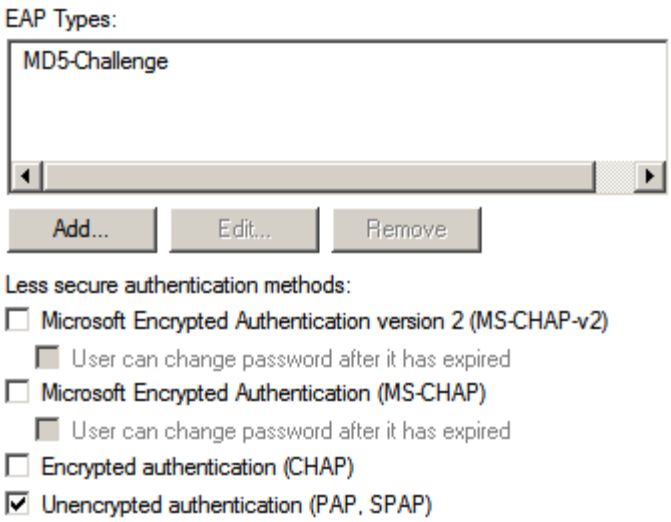
[7] http://support.microsoft.com/kb/922574/en-us

Na het toevoegen van de variabelen aan het register bestaat er de mogelijkheid om MD5-chap te gebruiken binnen de network policy. Voor de eenvoud is er gekozen om één policy te maken voor zowel Cisco als HP met betrekking tot de MAC Authenticatie.

Voordat de policy gedefinieerd kan worden, moet er binnen Active Directory een nieuwe groep aangemaakt worden, waar straks alle MAC adressen lid van worden. Deze groep is in de testomgeving “GG_MAB” genoemd.

Vervolgens kan binnen de NPS configuratie een nieuwe regel toevoegt worden aan de “Network Policies”. In deze regel wordt een conditie toegevoegd dat deze regel bedoeld is voor gebruikers, die lid zijn van de groep GG_MAB.

Voor authenticatie methoden moet, het vinkje voor “Unencrypted authentication (PAP, SPAP)” aangevinkt worden. Deze methode wordt gebruikt door de Cisco switches voor MAB. Vervolgens moet onder EAP types de MD5-Challenge toegevoegd worden. Deze zou na de registerwijziging beschikbaar moeten zijn.

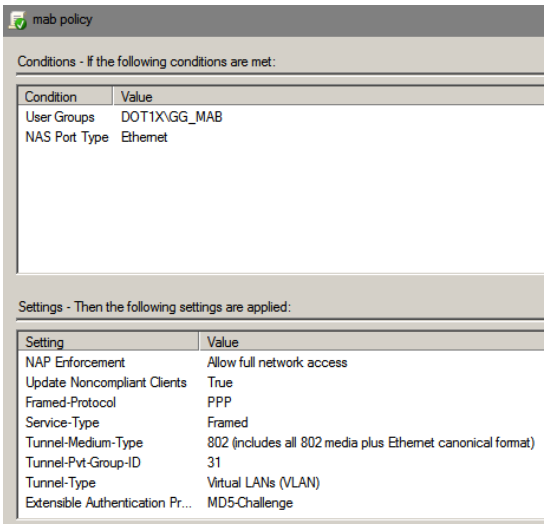


Figuur 19: MAB Authenticatie methoden

Verder moeten apparaten die geauthenticeerd worden middels het MAC adres in een apart VLAN geplaatst worden. Hiervoor worden de volgende drie parameters toegevoegd.

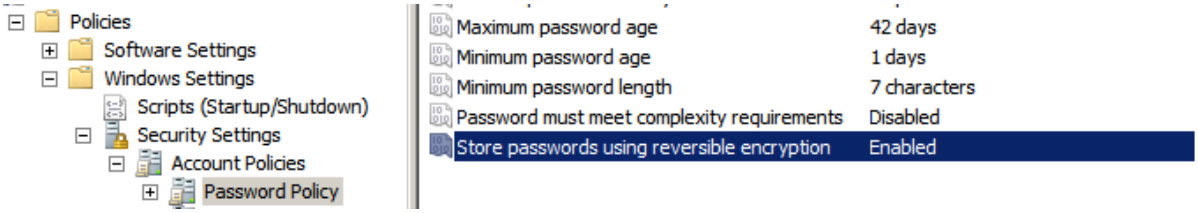
- Tunnel-Medium-Type;
- Tunnel-Pvt-Group-ID;
- Tunnel-Type.

Aan de Tunnel-Pvt-Group-ID word vervolgens VLAN 31 toegevoegd. Hier worden alle apparaten in geplaatst die middels MAC zijn geauthenticeerd.



Figuur 20: MAB Policy

Nu de NPS configuratie klaar is, moet er nog een wijziging gemaakt worden aan de “default domein policy”. Voor de MD5-Chap wordt gebruik gemaakt van “Reversible Encryption”. Deze optie is standaard uitgeschakeld.



Figuur 21: Store passwords using reversible encryption policy

Nu kunnen de apparaten, die middels MAC adres geauthenticeerd mogen worden, toegevoegd worden aan de Active Directory. Hiervoor is in de testopstelling een aparte OU gemaakt, te weten “MAB”. In deze OU worden alle MAC adressen geplaatst. Hiervoor wordt een nieuwe gebruiker gemaakt met als gebruikersnaam en wachtwoord het MAC adres van het betreffende apparaat.

Het is belangrijk om te zorgen dat deze MAC accounts geen lid zijn van de groep “Domain Users”. Dit zou namelijk de mogelijkheid bieden om op het domein in te loggen met het MAC adres als gebruikersnaam en wachtwoord.

Als laatste is voor MD5-Chap protocol van belang, dat er een vinkje gezet wordt voor “Store password using reversible encryption”.

Figuur 22: Store password using reversible encryption, account options

Het aanvinken van deze optie heeft geen invloed op het authenticatie mechanisme dat Cisco gebruikt voor MAB. Beide apparaten kunnen dus zowel op de HP als op de Cisco gekoppeld worden en kunnen door dezelfde policy afgehandeld worden.

Het is belangrijk dat “Reversible Encryption” alleen gebruikt wordt voor MAC authenticatie, omdat bij protocollen die hiervan gebruik maken, het wachtwoord over het netwerk word verstuurd!

Cisco 3750

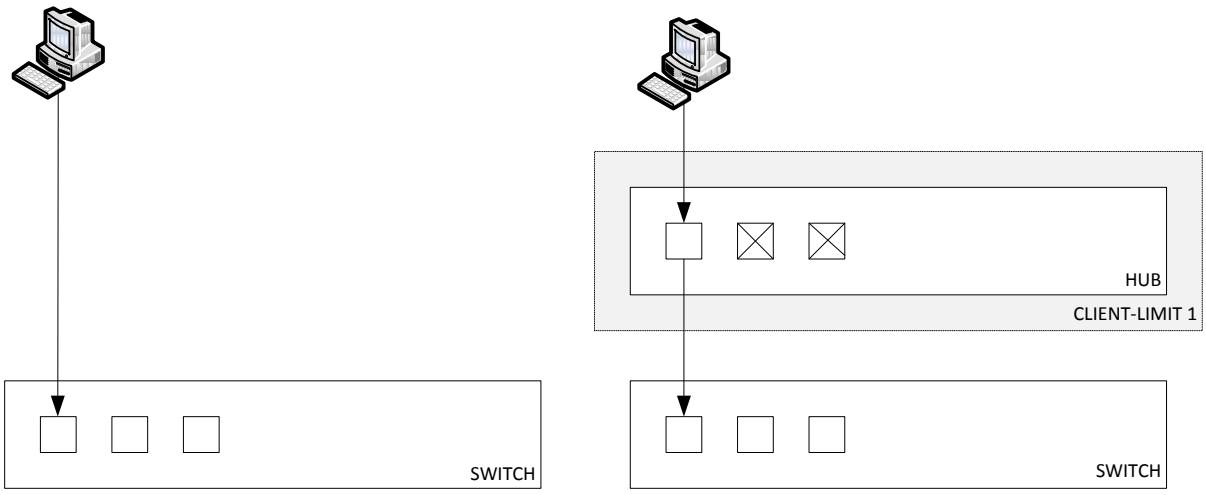
Binnen Cisco is MAB een techniek die relatief eenvoudig kan worden ingeschakeld. Het commando MAB is hiervoor voldoende. Wel is het aan te raden om de time-out aan te passen van de 802.1x authenticatie, zodat apparaten zonder 802.1x ondersteuning, niet 30 seconden hoeven te wachten op de 802.1x time-out. Ook kan er met de volgorde en de prioriteit van de afhandeling worden gespeeld. De standaard volgorde is eerst 802.1x en daarna MAB, toch is het overzichtelijker deze hard te definiëren.

```
interface FastEthernet1/0/5
  switchport access vlan 11
  switchport mode access
  switchport nonegotiate
  authentication order dot1x mab
  authentication priority dot1x mab
  authentication port-control auto
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 2
  spanning-tree portfast
!
interface Vlan31
  description MAC_Authenticated
  ip address 10.10.31.254 255.255.255.0
  ip helper-address 10.2.50.1
end
```

HP Procurve 2650

HP ondersteunt standaard 802.1x en MAC authenticatie. Helaas is het niet mogelijk om, zoals bij de techniek van Cisco, hier een volgorde aan te geven. Dit betekent dus dat het of 802.1x authenticatie is of MAC authenticatie. Om toch voor elkaar te krijgen dat beide technieken gebruikt kunnen worden is een workaround bedacht.

In de HP switches is een mogelijkheid ingebouwd om meerdere apparaten achter één poort te kunnen authenticeren middels 802.1x of MAC authenticatie. Dit zou gewenst kunnen zijn wanneer er een HUB achter een switchpoort wordt geplaatst. Deze techniek wordt ook wel “Cliënt Based Network Access Control” genoemd. Om deze functie in te schakelen moet worden ingesteld wat het maximum aantal cliënts is welke de poort kan verwachten. Nadat deze parameter is ingesteld, zal de switch 802.1x en MAC authenticatie gelijktijdig op de poort uitvoeren. Door het maximum cliënts op 1 te zetten, kan er nog steeds maar met één device geauthenticeerd worden, hiermee ligt deze work around heel dicht tegen “Port Based Network Access Control” aan. Deze techniek wijkt af van de Cisco oplossing, maar voldoet voor deze situatie prima. Er is overigens geen fysieke HUB nodig om deze oplossing te gebruiken.



Figuur 23: Links Port Based Network Access Control, rechts Client Based Network Access Control

```
aaa port-access authenticator 1-48
aaa port-access authenticator 1 client-limit 1
aaa port-access authenticator 2 client-limit 1
aaa port-access authenticator 3 client-limit 1
…
aaa port-access authenticator active
aaa port-access mac-based 1-48
aaa port-access 1-48
vlan 31
   name "MACAuth_Vlan"
   tagged 49,50
   exit
```

5.2.5.4 Captive Portal

Nadat een apparaat de kans heeft gehad zich te authenticeren middels 802.1x of MAC authenticatie (MAB), krijgen de apparaten op het hoofdkantoor en de distributiecentra in Veghel de mogelijkheid om zich alsnog te authenticeren middels een Captive Portal. Op de decentrale vestigingen is dit niet gewenst. Wat gelukkig goed uit komt, want HP ondersteunt geen combinatie van alle drie de technieken. Het is daar 802.1x met MAC Authenticatie of Captive Portal. Apparaten die zich authenticeren middels de Captive Portal zijn niet in beheer van Sligro of niet bekend bij Sligro beheer. Deze apparaten komen dan ook in een gescheiden netwerk (VLAN 666), dat geen verbinding heeft met het Sligro netwerk.

Allereerst moet een groep gemaakt worden binnen Active Directory waar alle gebruikers in geplaatst worden, die netwerktoegang via de Captive Portal mogen aanvragen. Deze groep heet in de testomgeving “GG_WEBAUTH”. Verder is een gebruiker “webuser” aangemaakt, die lid is van de groep “GG_WEBAUTH”.

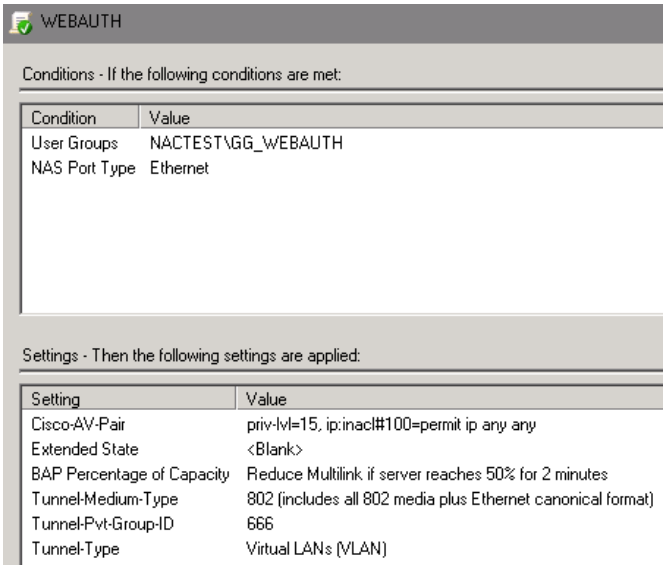
Vervolgens moet er een regel binnen NPS aangemaakt worden. Deze regel is wat complexer als de voorgaande regels. De techniek binnen de Cisco switch maakt gebruik van een Access Control List (ACL) en zal na een succesvolle authenticatie door de NPS server verwijderd moeten worden. Dit kan met Vendor Specific Tags (VST).

Er wordt net als voorheen een nieuwe regel aangemaakt en aan de condities de groep “GG_WEBAUTH” toegevoegd. Vervolgens is er net als in de voorgaande policies, gebruik gemaakt van dynamische VLAN toekenning, maar dit maal met VLAN ID 666.

Als laatste stap moet de ACL, die op de poort actief is, verwijderd worden. Hiervoor worden Vendor Specific Tags toegevoegd. Bij Cisco gebeurt dit door de optie Cisco-Av-Pair toe te voegen en hier 2 parameters aan mee te geven, te weten:

- priv-lvl=15;
- ip:inacl#100=permit ip any any.

De eerste parameter zorgt ervoor, dat de tweede wordt doorgevoerd. De tweede voegt een ACL toe aan de poort, waarbij al het IP verkeer wordt doorgelaten. #100 staat voor de positie binnen de ACL, zodat het mogelijk is eventuele restricties hoger in de ACL te plaatsten.



Figuur 24: NPS regel Captive Portal

Als laatste moet de Cisco 3750 ingesteld worden. Ook hier geldt dat de configuratie wat complexer is als de voorgaande configuraties. Dit wordt met name door de ACL veroorzaakt.

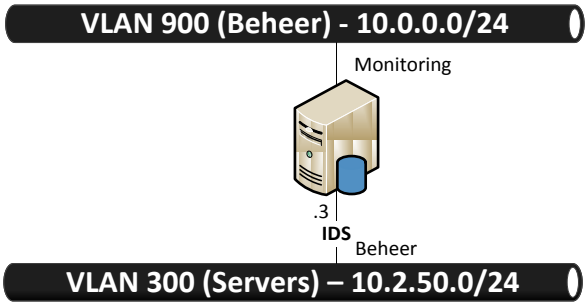
```
aaa authorization auth-proxy default group radius
ip admission name IP_ADMIN_RULE proxy http inactivity-time 60
!
fallback profile WEB_AUTH_PROFILE
  ip access-group PRE_WEBAUTH_POLICY in
  ip admission IP_ADMIN_RULE
!
interface FastEthernet1/0/2
  description MAB-Test
  switchport access vlan 11
  switchport mode access
  switchport nonegotiate
  authentication order dot1x mab webauth
  authentication priority dot1x mab webauth
  authentication port-control auto
  authentication fallback WEB_AUTH_PROFILE
  mab
  dot1x pae authenticator
  dot1x timeout tx-period 3
  spanning-tree portfast
!
ip http server
ip http secure-server
!
ip access-list extended PRE_WEBAUTH_POLICY
  permit udp any any eq bootps
  permit udp any any eq domain
```

5.2.5.5 IDS

Nadat de testomgeving volledig is opgezet met betrekking tot de toegangscontrole en de daarbij horende classificatie, is begonnen met het inrichten van een Intrusion Detection Systeem. Voor de test is gekozen om deze al het verkeer binnen VLAN 900 (Beheer) te laten monitoren. Binnen dit VLAN is het gemakkelijker om diverse alarmen te testen. In de uiteindelijke situatie zal VLAN 31 (MAC Authenticatie) een hogere prioriteit krijgen om met behulp van een IDS te monitoren.

Verder werd gekozen voor een “Out-Of-Band” opstelling, zodat de IDS geen problemen binnen het netwerk kan veroorzaken met betrekking tot doorvoersnelheden. Ook vormt de IDS op deze manier geen kritisch punt binnen het netwerk, als deze uitvalt heeft dit immers geen verdere consequenties voor de connectiviteit van de overige apparaten. Het systeem is uitgerust met 2 netwerkkaarten, waarvan er eentje gekoppeld is aan VLAN 300 (servers) voor het beheer en de andere interface aan VLAN 900 (Beheer) voor de monitoring.

Er is gekozen voor het monitoren van VLAN 900, omdat in de testomgeving hier het vaakst ongecontroleerd verkeer overheen gaat. In dit netwerk bevinden zich namelijk nog diverse andere apparaten, zoals printers en laptops.



Figuur 25: IDS koppeling binnen de testomgeving

Als IDS wordt er gebruik gemaakt van Snort die geïnstalleerd wordt op Ubuntu 10.04 LTS. De configuratie wordt vrij standaard gehouden. Wel is de laatste “ruleset” gedownload en geïnstalleerd. Dit zijn de regels waaraan het verkeer getoetst wordt. Naast Snort is ook Snort Report geïnstalleerd en BASE. Beiden geven een grafische schil voor Snort alarmen.

< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
[snort] snort_decoder: WARNING: IPV6 truncated header	non-standard-protocol	9(30%)	1	1	1	2010-03-17 14:54:30	2010-03-17 14:55:17
[snort] portscan: TCP Portscan	*unclassified*	1(3%)	1	1	1	2010-03-17 13:46:01	2010-03-17 13:46:01
[snort] snort_decoder: TCP Window Scale Option Scale Invalid (> 14)	non-standard-protocol	5(17%)	1	1	1	2010-03-17 13:46:11	2010-03-17 13:46:21
[snort] DNS SPOOF query response with TTL of 1 min. and no authority	bad-unknown	2(7%)	1	2	1	2010-03-17 14:37:08	2010-03-17 14:38:07
[snort] Snort Alert [1:16202:0]	attempted-dos	10(33%)	1	1	1	2010-03-17 14:02:20	2010-03-17 15:16:03
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [snort] SNMP AgentX/tcp request	attempted-recon	1(3%)	1	1	1	2010-03-17 13:46:02	2010-03-17 13:46:02
[cve] [icat] [cve] [icat] [bugtraq] [bugtraq] [bugtraq] [snort] SNMP request tcp	attempted-recon	1(3%)	1	1	1	2010-03-17 13:46:02	2010-03-17 13:46:02
[nessus] [snort] WEB-MISC robots.txt access	web-application-activity	1(3%)	1	1	1	2010-03-17 13:46:21	2010-03-17 13:46:21

ACTION
{ action } Selected ALL on Screen

Figuur 26: Voorbeeld grafische schil Snort alarmen BASE

5.3 Testresultaten

Doordat de testomgeving iteratief werd opgebouwd, is elk onderdeel tijdens de opbouw net zolang bijgeschaafd, tot deze naar behoren werkte. In de testopstelling is duidelijk geworden dat met zeer beperkte middelen toch een groot resultaat gehaald kan worden. Alle apparaten kunnen middels de HP en Cisco switches in samenwerking met de Microsoft NPS server gecontroleerd toegang verkrijgen tot het netwerk. Apparaten die minder of niet vertrouwd zijn, kunnen dynamisch in een ander netwerk worden geplaatst. Dit betekent tevens dat het niet noodzakelijk is om extra hardware aan te schaffen voor de pilot omgeving. Hieronder staan de belangrijkste aandachtspunten nog eens benoemd die in de testsituatie getackeld zijn.

5.3.1 Domain login (802.1x)

Computers die lid zijn van het domein, moeten een verbinding hebben, om op het domein in te loggen. Gebruikers die al eerder op de desbetreffende machine hebben ingelogd en geen wachtwoord hebben welke langer is als 14 tekens (deze worden niet lokaal opgeslagen), ondervinden hier geen hinder van. Dit wachtwoord word gecontroleerd wordt aan de hand van een opgeslagen hash. Het is mogelijk om middels user authenticatie een “pre domain logon” optie aan te vinken. Hierdoor wordt eerst de netwerkverbinding tot stand gebracht alvorens in het domein ingelogd wordt. Dit is voor beheerders welke dynamisch het juiste VLAN toegewezen moeten krijgen de oplossing. Voor gebruikers welke in het standaard VLAN van de switch moeten werken is er gekozen om met behulp van het computeraccount te authenticeren.

5.3.2 Cisco 30 seconden

De Cisco switches doen er na authenticatie erg lang over om de desbetreffende poort actief te maken. Door de switchpoort de parameter “spanning-tree portfast” mee te geven, gaat de poort onmiddellijk in forwarding binnen het spanning-tree protocol. Hierdoor werd de tijd gereduceerd naar zo’n 6 seconden. Als vervolgens ook de parameter “switchport nonegotiate” wordt meegeven, gaat de poort ook niet meer onderhandelen over wel of geen trunking (meerdere VLANs over 1 poort aanbieden). Hierdoor wordt de tijd verkort naar 1 á 2 seconden, dat acceptabel is. HP switches doen er ongeveer 1 seconde over, zonder extra parameters.

5.3.3 HP Mac Authentication Bypass

HP switches ondersteunen standaard geen MAC Authentication Bypass, maar ze ondersteunen wel MAC Authenticatie via het AAA protocol. Op een poort kan 802.1x authenticatie of MAC authenticatie gezet worden. Om toch beide protocollen actief te maken kan er geschakeld worden naar Clientbased Network Access Control, door de parameter “client-limit 1” mee te geven. Hierdoor kan er weliswaar maar 1 apparaat authenticeren, maar maakt het niet uit of dit via 802.1x gebeurt of via MAC Authenticatie.

5.3.4 MAC Authenticatie geen domain users

Het is zeer belangrijk dat de accounts die aangemaakt worden voor MAC Authenticatie, geen lid zijn van de groep “Domain users”. Standaard is dit wel het geval. Als deze accounts hier wel lid van zijn, dan geeft deze de mogelijkheid om met behulp van het MAC adres in te loggen op diverse systemen!

5.3.5 Snort beheer

In de testopstelling is gebleken dat het beheren van een IDS een zeer intensieve klus is. In de testomgeving kwamen al enkele honderden alarmen per uur binnen. Om een IDS zo in te richten dat deze ook daadwerkelijk bruikbaar is, is een project op zich. Besloten is dan ook om de IDS opstelling niet mee te nemen in de pilot, maar achteraf als apart project op te starten.

6. Pilot

Om een goed beeld te krijgen hoe netwerktoegangscontrole in de praktijk zal reageren wordt een pilot omgeving opgebouwd. In deze omgeving wordt een gedeelte van het productienetwerk voorzien van netwerktoegangscontrole. Op deze manier kan er gekeken worden hoe dit systeem bevalt en reageert. Tevens kunnen nog eventuele problemen, die zich niet in de testomgeving hebben voorgedaan, opgelost worden zonder dat business processen gevaar lopen.
Voor de pilot omgeving is ervoor gekozen om dit binnen de afdeling beheer te doen.
De redenen hiervoor zijn:

- Dichtbij in het geval van problemen;
- Veel verschillende apparaten, zelfs weegschalen en pinpads voor testdoeleinden;
- Alle drie de beveiligingsmethoden zijn hier van toepassing.

Alvorens de pilot omgeving opgebouwd wordt, is een kleine presentatie gegeven aan collega's van ICT Beheer, zodat deze op de hoogte zijn van wat netwerktoegangscontrole inhoud en wat ze hier mee kunnen. Ook worden zij aangemoedigd hier gebruik van te maken, zodat deze pilot als representatief gezien kan worden voor het overige gedeelte van het netwerk.

6.1 Opbouw pilot omgeving

Voor de opbouw van de pilot, wordt zoveel mogelijk rekening gehouden met de "nieuwe" situatie. Onder de nieuwe situatie wordt verstaan, het complete netwerk voorzien van Cisco apparatuur inclusief de nieuwe netwerkindeling (VLAN- en IP plan).

In de pilot omgeving krijgt elke patchruimte (SER) zijn eigen standaard VLANs. Op dit moment zijn hier twee VLANs voor benoemd en bestaat ruimte om in de toekomst eventueel uit te breiden. Nu zijn dit het "standaard" VLAN en het "printer" VLAN die voor elke ruimte dus anders zijn. In een later stadium kunnen hier extra VLANs aan toegevoegd worden. Deze scheiding wordt gemaakt om apparaten te scheiden van elkaar en de mogelijkheid te hebben om deze netwerken te voorzien van een Access Control List, zodat deze apparaten alleen kunnen communiceren met apparaten, waarmee deze moeten communiceren. Dit is met name belangrijk voor apparaten die niet middels 802.1x verbonden worden, omdat de andere authenticatie mogelijkheden relatief eenvoudig te omzeilen zijn.

De pilot zal in de eerste instantie opgebouwd worden in kast "PKICT0003A". Deze kast, heeft zoals alle kasten, naast een naam nog een nummer. Dit is nummer 7. Hierop is het nieuwe VLAN plan gebaseerd. Hierin is bepaald dat alle "standaard" VLANs beginnen met 11xx en dat alle "printer" VLANs beginnen met 12xx. Eventuele uitbreiding worden 13xx, 14xx, etc. waarbij xx voor het kastnummer staat.

Naast een VLAN ID en naam krijgt elk VLAN ook zijn eigen subnet. Ook elk subnet maakt gebruikt van het kastnummer.Zo zal subnet 10.128.x.0/24 voor het "standaard" VLAN staan en zal subnet 10.127.x.0/24 voor het "printer" VLAN staan. Eventuele uitbreidingen kunnen worden gemaakt door van het tweede octet één af te halen, zodat het subnet 10.126.x.0/24 de eerstvolgende is. De gateway voor deze subnetten eindigen op één. Dit om eventuele uitbreidingen in de toekomst te vergemakkelijken. Met nummer 254 zou met het vergroten van het subnet namelijk een gateway in het midden van het subnet komen te staan.

Voor de kast “PKICT0003A” met nummer 7, zal het VLAN en subnet plan er zo uit komen te zien.

VLAN ID	Naam	Subnet	Gateway
1107	Standaard	10.128.7.0/24	10.128.7.1
1207	Printers	10.127.7.0/24	10.127.7.1

Tabel 8: VLAN en IP plan PKICT0003A

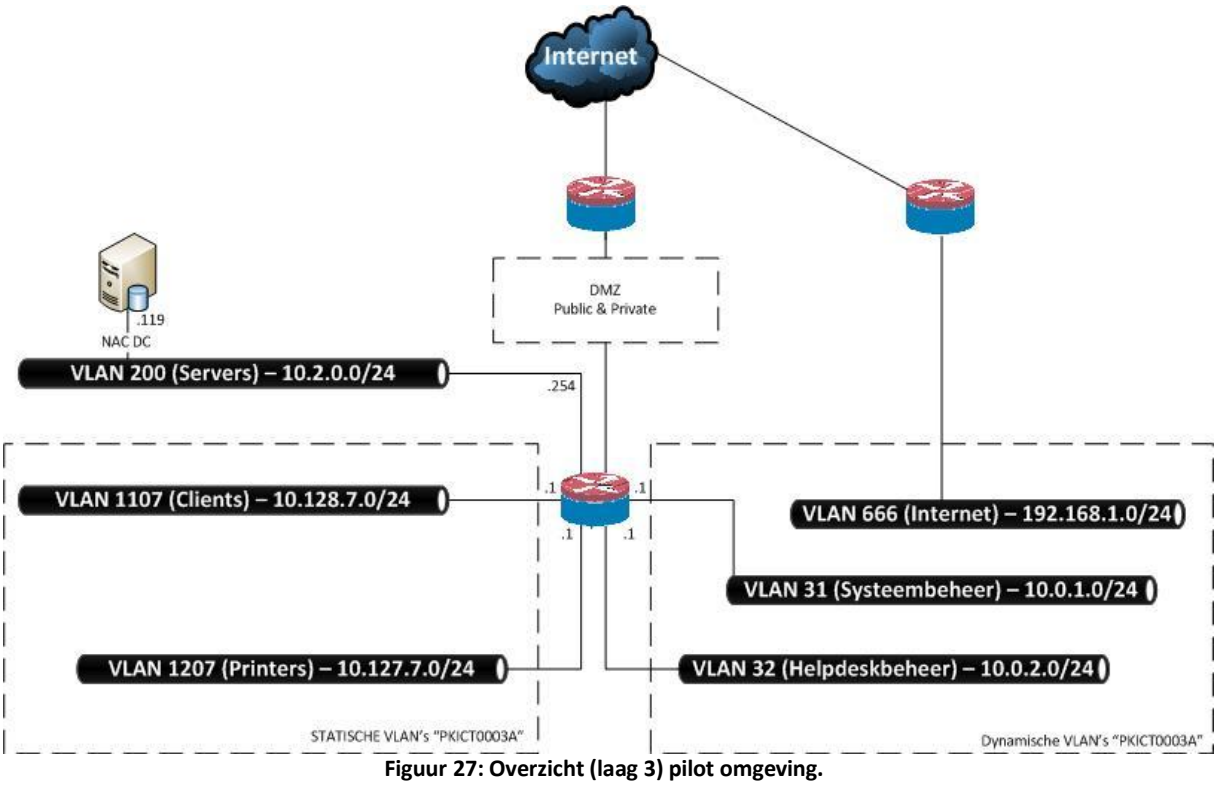
Naast deze “vaste” VLANs per kast, zijn er ook een aantal dynamische VLANs. Deze kunnen in elke kast voorkomen. Denk hierbij aan VLANs voor gebruikers die extra rechten nodig hebben. Bijvoorbeeld systeem- netwerkbeheer, 2e lijns helpdesk, etc. Of de VLANs die een geheel gescheiden netwerk bieden, bijvoorbeeld het Internet VLAN.

Ook deze VLANs en subnetten zijn gedefinieerd en ook hier is rekening gehouden voor eventuele uitbreidingen. Behalve het “Internet” VLAN dat een compleet gescheiden netwerk is.

VLAN ID	Naam	Subnet	Gateway
31	Systeem- en netwerkbeheer	10.0.1.0/24	10.0.1.1
32	2e lijns helpdesk	10.0.2.0/24	10.0.2.1
33	*Uitbreiding*	*10.0.3.0/24*	*10.0.3.1*
666	Internet	192.168.1.0/24	192.168.1.254

Tabel 9: Dynamische VLAN’s en subnetten

Als de bovenstaande gegevens in een overzichtelijke tekening worden gezet, dan ziet deze er als volgt uit.



Figuur 27: Overzicht (laag 3) pilot omgeving.

Nu duidelijk is hoe het netwerk eruit komt te zien moet nog bepaald worden welke server gebruikt gaat worden voor netwerktoegangscontrole. Besloten is om hier één van de drie huidige domeincontrollers voor te nemen, namelijk de “SLGDOM04”. Dit is een virtuele server, dus hiermee is hardwareredundantie gewaarborgd. Er is besloten om IP redundantie nog niet mee te nemen in de pilot, maar dit is wel van belang in een later stadium zie aanbevelingen.

Deze server is gekozen, omdat RADIUS net als Active Directory voor authenticatie zorgt. Ook maakt de RADIUS server in onze opstelling veelvuldig gebruik van de gegevens binnen Active Directory.

6.1.1 Inrichting Active Directory

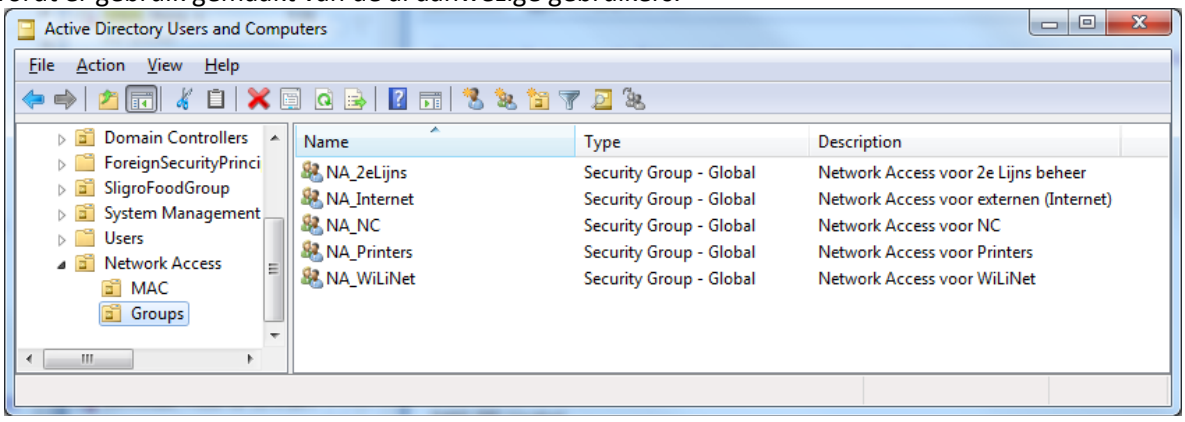
Zoals in de testomgeving is gebleken, is het voor veel apparaten gemakkelijk om te authenticeren middels het domein waar deze lid van zijn. Helaas zijn er apparaten die geen lid zijn van het domein. Vaak omdat ze deze functionaliteit niet ondersteunen. Op het hoofdkantoor zijn dit bijvoorbeeld printers en NC’s.

Nu kunnen deze apparaten authenticeren middels het MAC adres. Alleen is dit niet de meest veilige methode. Om deze methode toch wat veiliger te maken is het verstandig om gebruik te maken van Access Control Lists. Zo kunnen printers bijvoorbeeld na authenticatie alleen met de printserver communiceren. Mocht een apparaat zich dan voordoen als printer, dan kan deze alleen bij de printserver komen.

NC’s ondersteunen wel 802.1x, echter alle NC’s maken gebruik van dezelfde image. Hierdoor zijn deze systemen allemaal gelijk, zodat ze één op één gewisseld kunnen worden. Op het moment dat gekozen wordt om op één locatie netwerk toegangscontrole in te richten en de NC middels 802.1x te laten authenticeren, dan zal de configuratie van deze NC afwijken. Hierdoor kunnen deze systemen niet meer één op één gewisseld worden.

Om ervoor te zorgen dat dit wel kan en de standaard intact blijft, is gekozen om de NC’s te authenticeren middels het MAC adres. Na authenticatie wordt de NC in het “standaard” VLAN geplaatst. Dit is niet de meeste veilige methode, maar hierdoor blijft de standaard in stand en het is beter dan geen beveiliging. Nadat alle locaties zijn voorzien van netwerktoegangscontrole moet gekeken worden na een nieuwe image voor de NC’s zodat deze middels 802.1x gaan authenticeren.

Voor de pilot wordt de Active Directory als volgt ingericht. Er is gekozen om een aparte OU “Network Access” te maken, zodat alles met betrekking tot netwerk toegangscontrole bij elkaar staat. Wel wordt er gebruik gemaakt van de al aanwezige gebruikers.



Figuur 28: Active Directory indeling voor netwerktoegangscontrole

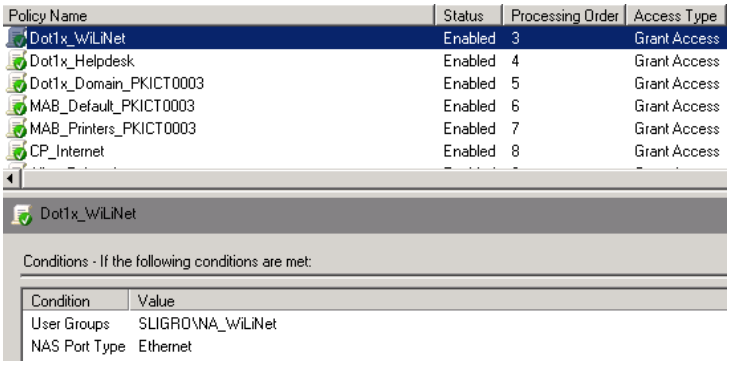
6.1.2 RADIUS instellingen

Nadat de bovenstaande structuur is aangemaakt, kan worden begonnen met het maken van de RADIUS instellingen. In de RADIUS server dienen de volgende regels te worden aangemaakt.

	Methode	Waarde	Resultaat	Naam
1	802.1x	NA_Wilinet	Systeembeheer VLAN (31)	Dot1x_WiLiNet
2	802.1x	NA_2eLijns	Helpdeskbeheer VLAN (32)	Dot1x_Helpdesk
3	802.1x	Domein computer	Standaard VLAN (1107)	Dot1x_Domain_PKICT0003A
4	MAB	NA_NC	Standaard VLAN (1107)	MAB_Default_PKICT0003A
5	MAB	NA_Printers	Printer VLAN (1207)	MAB_Printers_PKICT0003A
6	Captive Portal	NA_Internet	Internet VLAN (666)	CP_Internet

Tabel 10: RADIUS Regels pilot omgeving

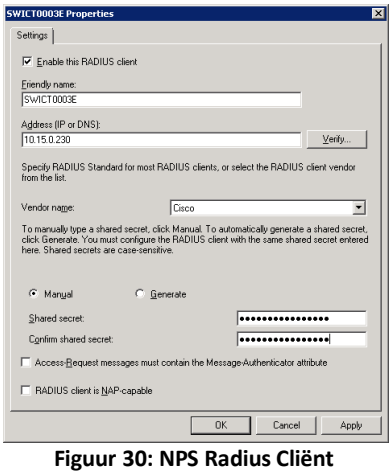
Om dynamisch het juiste printer VLAN voor de desbetreffende kast te kunnen detecteren, wordt gebruik gemaakt van de “Radius-Request” parameter. Deze parameter bevat de locatienaam, bijvoorbeeld “PKICT0003”.



Figuur 29: NPS Regels in de pilotomgeving

De volgorde van de regels is erg belangrijk. Als er eenmaal aan een regel is voldaan, wordt er niet meer naar de onderliggende regels gekeken. Regel 3, 4 en 5 zullen herhaald worden voor elke kast waar netwerktoegangscontrole geïmplementeerd wordt. Uiteraard dient hier dan ook een ander VLAN aan gekoppeld te worden. Voor kast 8 zou dit bijvoorbeeld VLAN 1108 en 1208 zijn.

Aan de NPS (RADIUS) Cliënts is vervolgens de switch toegevoegd. Als key is er gekozen voor de switchnaam in hoofdletters gevolgd door “secret”. De key ziet er dan als volgt uit. “SWICT0003Esecret”.



Figuur 30: NPS Radius Cliënt

6.1.3 Inrichting switch

De switch zal een Cisco 3750 zijn, zodat deze voldoet aan de toekomstige situatie. Deze zal voor de pilot omgeving wel gekoppeld worden aan de bestaande HP omgeving. Alle VLANs, behalve het Internet VLAN zijn bekend op de HP omgeving en worden op laag 2 van het OSI model gekoppeld aan de Cisco switch. Het Internet VLAN zal aangemaakt worden op de Cisco switch en rechtstreeks met de Internet router verbonden worden.

Op poort Gi1/0/1 wordt de koppeling met het bestaande HP netwerk gemaakt. Deze poort zal als trunk poort (Multi-VLAN in HP terminologie) worden ingericht, met de VLANs zoals hierboven benoemd.

```
vlan 666
 name Internet
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 31,32,900,1107,1207
 switchport mode trunk
!
interface FastEthernet1/0/24
 description INTERNET
 switchport access vlan 666
 switchport mode access
```

Nu deze VLANs beschikbaar zijn, kunnen de RADIUS instellingen gemaakt worden, zodat de switch het juiste verzoek doet aan de RADIUS server. Belangrijk hier is de Radius-Request parameter (32). Deze parameter zorgt ervoor dat de NPS weet, welk VLAN het standaard VLAN voor de desbetreffende kast is.

```
aaa new-model
radius-server attribute 32 include-in-access-req format PKICT0003A
radius-server host 10.2.0.119 auth-port 1645 acct-port 1646
radius-server key SWICT0003Esecret
```

Ook belangrijk om niet te onthouden is een lokale gebruikersnaam aan te maken. Als dit niet wordt gedaan, dan bestaat de kans dat je uitgesloten wordt van Telnet of Console toegang, omdat deze probeert te authenticeren middels het AAA protocol en de bijbehorende RADIUS server. Mocht je toch buitengesloten raken, dan is de kans groot, dat je het commando aaa new-model, ongedaan kunt maken met behulp van de web interface. Uiteraard is het ook mogelijk een regel voor Telnet/Console toegang aan de NPS (RADIUS) server toe te voegen.

```
aaa authentication login default local
username nacpilot privilege 15 password nacpilot
```

Nu kan de switch verder ingericht worden met het AAA protocol en de bijbehorende beveiligingsmechanismen. In het voorbeeld hieronder staat één poort als voorbeeld. Het is mogelijk om per poort te specificeren wat gewenst is. In de nieuwe firmware voor de Cisco 3750 is het mogelijk om dit voor meerdere poorten tegelijk te doen met een range commando.

```
int ra fa1/0/1 – 23
```

Er is gekozen om de pilot nog niet naar deze firmware te upgraden, omdat er dan een wezenlijk verschil ontstaat tussen de test- en pilotomgeving. Na het afronden van de pilot kan getest worden met nieuwe firmware.

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
!
ip device tracking
ip admission name IP_ADMIN_RULE proxy http inactivity-time 60
!
dot1x system-auth-control
!
fallback profile WEB_AUTH_PROFILE
 ip access-group PRE_WEBAUTH_POLICY in
 ip admission IP_ADMIN_RULE
!
interface FastEthernet1/0/1
 switchport mode access
 switchport nonegotiate
 authentication order dot1x mab webauth
 authentication priority dot1x mab webauth
 authentication port-control auto
 authentication fallback WEB_AUTH_PROFILE
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 2
 spanning-tree portfast
!
ip http server
ip http secure-server
!
ip access-list extended PRE_WEBAUTH_POLICY
 permit udp any any eq bootps
 permit udp any any eq domain
!
```

7. Conclusie en aanbevelingen

De pilot heeft uitgewezen, dat netwerktoegangscontrole een zeer waardevolle toevoeging kan zijn voor zowel beveiliging als beheersbaarheid. Het geeft de mogelijkheid om ongewenste apparaten van het netwerk af te houden en tevens geeft het inzicht in het gebruik van het netwerk. Toch zijn er ook een aantal nadelen te noemen. Het grootste nadeel is dat het goed inrichten van deze oplossing erg veel tijd kost. Gelukkig kan dit wel geleidelijk opgepakt worden, maar pas na het doorvoeren in het gehele netwerk kan worden gesproken over een “veilig” netwerk, waar apparaten niet “zomaar” toegang kunnen verkrijgen. Ruimten die niet zomaar toegankelijk zijn om een netwerkverbinding te maken en alleen toegankelijk zijn voor ICT, zouden buiten deze oplossing gelaten mogen worden. Denk hierbij aan datacentra.

Mijn advies luidt dan ook om de pilot geleidelijk aan uit te breiden. Alvorens hier mee te beginnen, is het mijn inziens verstandig om eerst te zorgen voor een goede (IP) redundantie. Na deze voorziening kan de pilot uitgebreid worden naar het gehele hoofdkantoor en de bijbehorende distributiecentra. Als deze voltooid zijn, kan er begonnen worden met de decentrale vestigingen. Ook hier moet goed gekeken worden naar de redundantie in de vorm van lijnafhankelijkheid. Nadat de netwerktoegangscontrole volledig is ingericht, zou er indien gewenst gekeken kunnen worden naar Health Checks en Intrusion Detection. Beiden kunnen een waardevolle toevoeging zijn voor controle en beveiliging, maar vragen deze oplossingen wel continue aandacht van de afdeling beheer.

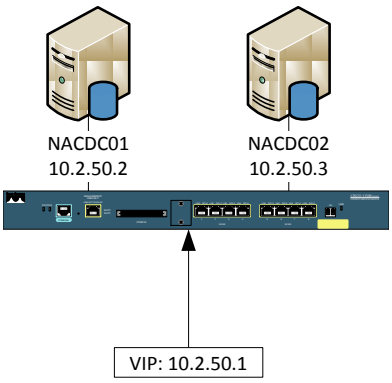
In het volgende gedeelte staan de bovengenoemde punten wat verder uitgewerkt.

7.1 Redundantie

Niet meegenomen in de pilot, maar zeker niet onbelangrijk is het redundant uitvoeren van de RADIUS omgeving. Dit is niet meegenomen in de test- en pilotomgeving, omdat deze beide op een virtuele omgeving draaiden. Zodoende was er al voorzien in hardware redundantie. Mocht deze machine om configuratie technische redenen niet meer werken of herstart moeten worden, dan zou dit betekenen dat niemand op het netwerk zich meer kan authenticeren en dus geen toegang kan verkrijgen.

Helaas is er nog geen perfecte oplossing om een NPS server redundant op te bouwen. Microsoft adviseert zelf gebruik te maken van een RADIUS Proxy en hier minimaal twee NPS/NAP servers achter te plaatsen. De configuratie moet van deze twee servers handmatig gelijk gehouden worden, maar deze oplossing geeft hetzelfde probleem. Wat als de RADIUS Proxy het begeeft? Dit is mijn inziens het probleem verplaatsen.

Het advies is dan ook om gebruik te maken van twee Microsoft NPS servers, die nog wel steeds handmatig via een export, import procedure gelijk van configuratie dienen te worden gehouden, maar vervolgens gebruik maken van loadbalancers. Deze loadbalancers, al redundant aanwezig binnen het Sligro netwerk, zorgen voor een VIP adres. Alle switches die gebruik moeten maken van de NPS server, verwijzen naar dit VIP adres. Vervolgens kunnen de loadbalancers de verzoeken doorzetten naar de daadwerkelijke RADIUS servers. In deze oplossing, mag zowel één van de loadbalancers en één van de NPS servers uitvallen, zonder dat er functionaliteiten verdwijnen.



Figuur 31: IP Redundantie RADIUS servers

De Cisco switches kunnen werken met zogenaamde “RADIUS Groups” hierin kunnen meerdere servers worden opgenomen, zodat bij uitval van een van de servers, gekeken wordt naar de volgende server. Hier wordt de loadbalancing functionaliteit verzorgt door de switch. Dit betekent wel dat dit op alle switches hetzelfde geregeld moet worden. Het voordeel van een losse loadbalancer is dat deze configuratie centraal afgehandeld wordt.

7.2 Decentrale vestigingen en redundantie

Als decentrale vestigingen van netwerktoegangscontrole worden voorzien, betekent dit, dat deze afhankelijk worden van de netwerkverbinding richting het WAN netwerk. Op het moment dat deze verbinding verbroken wordt, zou dit betekenen dat er geen nieuwe apparaten op het netwerk aangemeld kunnen worden. Er bestaan twee oplossingen die dit probleem op kunnen lossen. Enerzijds het aanleggen van een tweede verbinding richting het WAN, die zoveel mogelijk gescheiden is van de huidige verbinding, bijvoorbeeld met behulp van UMTS. Een andere oplossing zou kunnen zijn om de AS400 die op diverse locaties staan, als RADIUS server in te richten en gebruiken. Deze laatste oplossing moet wel verder onderzocht worden. Het is belangrijk om voor ogen te houden, dat bij het verbreken van deze verbinding er geen nieuwe apparaten op het netwerk aangemeld kunnen worden.

7.3 NC's in het domein

Op het moment dat bij de NC's gekozen wordt om deze lid te maken van het domein, moet er rekening gehouden worden met de Preboot Execution Environment (PXE). PXE wordt gebruikt om NC's te kunnen voorzien van een nieuwe image. PXE is een techniek om systemen van het netwerk te laten opstarten. Hiervoor is een netwerkverbinding benodigd. Op het moment dat de switch 802.1x authenticatie vraagt om verbinding te maken met het netwerk, zou PXE niet gebruikt kunnen worden. Om toch PXE te kunnen gebruiken, moet er op de switch "direction-control" ingesteld worden. Het OS wat vervolgens gestart wordt, in het geval van het imaging proces een Linux distributie, moet vervolgens nog wel aanmelden middels het 802.1x protocol.

7.4 NAP en Health checks

Binnen de Microsoft NAP/NPS oplossing bestaat de mogelijkheid om met zogenaamde Health Checks te werken en hier een beleid aan te binden. Hierbij moet je denken aan controle of er een virusscanner op het systeem actief is en of deze wel up-to-date is. Zo kan het zijn dat je wil verplichten dat alle laptops minstens de laatste versie van de virusscanner hebben. Zo niet, kunnen deze in een "quarantaine" VLAN geplaatst worden, waar ze de laatste virusdefinities kunnen downloaden. Dit is een manier om extra veiligheid in te bouwen, maar vergt wel veel tijd om te beheren.

7.5 IDS

Zoals in de testopstelling is gebleken, vergt een IDS oplossing zeer veel tijd om in te richten en te beheren. Wel kan een IDS een waardevolle toevoeging binnen het netwerk zijn, voor de netwerken waar minder controle op is. Na het inrichten van netwerktoegangscontrole is het dan ook interessant om hier een project voor op te starten en hier de juiste oplossing voor te kiezen. Er zijn verschillende leveranciers die een koppeling kunnen leggen met Microsoft NAP. Hierdoor ontstaat er één complete oplossing. Ook biedt Microsoft een NAP API aan, om producten welke standaard geen koppeling hebben, toch te kunnen koppelen.

7.6 Rapportage

De NPS server houdt stipt bij wie en welk systeem er wanneer verbinding maakt. Standaard wordt dit opgeslagen in een op tekst gebaseerd logboek en kan met behulp van de "Event viewer" worden bekeken. Het is echter ook mogelijk om de logging weg te schrijven in een SQL database. Vervolgens zou dan met behulp van SQL Reports een mooie rapportage gemaakt kunnen worden. Denk hierbij aan, wie logt wanneer in, wanneer is het druk, etc.

7.7 Captive Portal

De Cisco switches bieden de mogelijkheid om een “custom” webpagina te tonen als Captive Portal. Nadeel van deze oplossing is, dat op elke switch waar gebruik gemaakt wordt van deze Captive Portal, deze wijziging gemaakt moet worden. Als er iets wijzigt, dan moet dit weer op alle switches. Op het hoofdkantoor zijn dit al snel 20switches. Het is dan ook interessant of dit proces te automatiseren of te centraliseren is.

Figurenlijst

Tabellenlijst

Synoniemen, Acroniemen, Begrippen en Afkortingen

ACL	Access Control List, lijst met regels, om beperkingen op te kunnen leggen wat wel en niet mag op het netwerk.
AD	Active Directory, gebruikers- en computerbeheer binnen een Windows domein.
Captive Portal	Website welke gebruikt wordt om netwerktoegang te verkrijgen.
CHAP	Challenge Handshake Authentication Protocol, protocol voor wachtwoordverificatie, zonder het wachtwoord over het netwerk te verzenden.
DMZ	Demilitarized Zone, netwerk wat zich tussen het Internet en het lokale netwerk bevind.
EAP	Extensible Authentication Protocol. Framework voor authenticatie.
Ethernet	Netwerkprotocol, waarme een local area network kan worden opgezet.
Firmware	Software welke zorgt voor de aansturing van (embedded) apparaten.
HUB	Netwerkapparaat, verkeer wat hier in gestuurd wordt, wordt over alle poorten naar buiten gestuurd.
IDS	Intrusion Detection System, systeem wat controleert op ongewenst gedrag binnen het netwerk.
IEEE	Organisatie, welke technologische standaarden vastlegt.
Image	Een complete software kopie van een systeem welke vaak gebruikt wordt om systemen snel te kunnen voorzien van software. Dit proces wordt imagen genoemd.
LAN	Local Area Netwerk, is een lokaal computernetwerk.
NAC	Network Access Control, opstelling, welke toegang tot het netwerk controlleert.
NAP	Network Access Protection, oplossing van Microsoft om apparaten aan extra eisen (bijv. virusscanners) te laten voldoen, alvorens deze op het netwerk toe te laten.
NPS	Network Policy Server, radius server van Microsoft, opvolger van IAS (windows 2003)
MS	Microsoft, softwareontwikkelaar.
OSI Model	Abstracte weergave van netwerklagen. Functionaliteiten binnen het netwerk worden vaak gespiegeld aan een van deze lagen.
OU	Organizational Unit, afdeling binnen Active Directory.
PAP	Password Authentication Protocol, protocol om paswoorden in platte tekst over het netwerk te versturen.
PEAP	Protected Extensible Authentication Protocol, protocol welke een encryptie laag toevoegd op het EAP protocol.
Policy	Beleid wat gevolgd wordt.
Protocol	Definitie over hoe iets werkt, kan gezien worden als een lijst met afspraken.
PTL	Pick To Light, orderpicking system wat werkt m.b.v. lichten.
RSA	Remote Server Administration, interface van IBM om servers op afstand te kunnen beheren, incl. het aan/uitzetten en biosconfiguratie. Tegenhanger van HP's ILO.
QNX	Realtime operingsysteem, besturingssysteem welke reageert binnen afgesproken tijden.
SBC	Server Based Computer, techniek, waarbij zoveel mogelijk cliëntfunctionaliteiten vanaf de server worden aangeboden.
SER	Secondary Equipment Room, knooppunten binnen het netwerk, vaak de plek waar eindapparaten gekoppeld worden aan het netwerk.
Spanning Tree	Protocol om lussen in het netwerk te voorkomen.
Switch	Netwerkapparaat, welke leert welke apparaten gekoppeld zit aan een poort, zodat deze verkeer, naar de juiste poort kan uitsturen.

Trunk	Meerdere netwerken (VLANs) over één poort meesturen. (Binnen HP heet dit een Multi-VLAN poort).
VIP	Virtual IP address, een virtueel IP adres, vaak met één of meerdere achterliggende IP adressen. Vaak gebruikt voor het redundant maken van functionaliteiten welke middels IP benaderd worden.
VLAN	Virtual LAN, is een virtueel lokaal netwerk. Waar vroeger elk apparaat zijn eigen netwerk vertegenwoordigde is het met VLANS mogelijk om op apparaten meerdere VLANS aan te maken.
VST	Vendor Spacific Tags, instellingen die de RADIUS server meestuurt gericht op een specifiek apparaat.

Bronnen

Algemene Internet encyclopedie:
http://www.wikipedia.com

Configuring IEEE 802.1x Port-Based Authentication (Cisco):
http://www-europe.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_25_se/configuration/guide/sw8021x.html

Inrichting Captive Portal, Web authentication (Cisco):
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/app_note_c27-577494.html#wp9000151

Releasenotes Firmware HP2600 H10.38:
http://cdn.procurve.com/training/Manuals/2600-RelNotes-H1083-59906003.pdf

ProCurve Network Security solutions:
http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm

Configuring Port-Based and User-Based Access Control (802.1X):
http://cdn.procurve.com/training/Manuals/2900-ASG-Jan08-9-8021X.pdf

Planning Redundancy for a NAP Health Policy Server:
http://technet.microsoft.com/en-us/library/dd125340%28WS.10%29.aspx

Snort installatie Ubuntu 10.04 LTS:
http://www.symmetrixtech.com/articles/004-snortinstallguide286.pdf