Scriptie

Network Access Control op de Hogeschool Utrecht

Naam : Danny Verbeek
Studentnummer : 1572282

Datum : 29-05-2012
Klas : SI6B

Opleiding : Systeembeheer Duaal
Docentbegeleider : Leendert van Doesburg

Bedrijf : Hogeschool Utrecht
Bedrijfsbegeleider : Gerard Verwoolde

Voorwoord

Voor u ligt mijn scriptie die ik geschreven heb in kader van het afstuderen voor de opleiding systeembeheer duaal aan de Hogeschool Utrecht. Deze scriptie is gemaakt door Danny Verbeek, netwerkbeheerder van de Hogeschool Utrecht.

Na drie jaar studie ben ik aan het eind van mijn studie gekomen. Het waren drie leerzame jaren, waarin ik veel heb geleerd. Ik ben anders naar mijn werk gaan kijken. Daarnaast heb ik nieuwe inzicht en handvatten gekregen voor het aanpakken van verschillende situatie.

Ik wil in het bijzonder mijn vriendin Mirella van den Burg bedanken, die mij drie jaar lang gesteund en gemotiveerd heeft. Daarnaast wil ik mijn klasgenoten bedanken waarmee ik drie jaar samen heb gestudeerd.

Tevens wil ik de Hogeschool Utrecht Stafdienst Bedrijfsvoering bedanken, die mijn opleiding mogelijk hebben gemaakt. Mijn collega's Max Mudde, Stefan Diedel, Sven de Ridder, Ed de Vries en Gerard Verwoolde en mijn docent begeleider Leendert van Doesburg wil ik bedanken voor hun tijd en feedback tijdens het uitvoeren van mijn afstudeeropdracht.

Danny Verbeek
Utrecht, Mei 2012.

Managementsamenvatting

In dit document wordt het onderzoek naar NAC binnen de Hogeschool Utrecht beschreven. De aanleiding voor dit onderzoek komt voort uit het Strategisch ICT-beleid HU 2010-2015 van de Hogeschool Utrecht. In het Strategisch ICT-beleid HU 2010-2015 staat beschreven wat de ambities zijn van de Hogeschool Utrecht op ICT gebied. Hierin staan ook de doelstellingen van de Hogeschool Utrecht beschreven.

In de analysefase van het onderzoek naar NAC is gekeken hoe de Hogeschool Utrecht er op dit moment voorstaat ten aanzien van NAC. In de huidige situatie wordt geen gebruik gemaakt van NAC op het bekabeld netwerk. Hierdoor is het mogelijk dat iedereen gebruik kan maken van het bekabeld netwerk, zonder te authentiseren. Hierdoor is er geen zicht op wie en wat er gebruik maakt van het bekabeld netwerk van de Hogeschool Utrecht.

Op het huidige draadloos netwerk van de Hogeschool Utrecht wordt wel gebruik gemaakt van NAC. Echter is het niveau van NAC, op het draadloos netwerk, nog niet op het juiste niveau. Thread prevention en het koppelen van gebruikersnamen aan datapakketten wordt dan ook nog niet toegepast.

Om beeld te krijgen van de gewenste situatie, zijn er interviews gehouden met de manager infrabeheer, security officer, netwerk- en serverbeheerders en een aantal gebruikers van het netwerk. Tevens is er gekeken naar het strategisch ICT-beleid van de Hogeschool Utrecht. De resultaten die naar voren zijn gekomen uit de interviews en het strategisch ICT-beleid zijn gevormd tot eisen en wensen. Aan de hand van deze eisen en wensen is er gekeken naar een juiste NAC-oplossing voor de Hogeschool Utrecht.

Voor het nieuwe NAC-ontwerp is er gekozen om gebruik te maken van componenten die al in het bezit zijn van de Hogeschool Utrecht. Er is gekozen om gebruik te maken van de huidige componenten vanwege de volgende redenen:

- Met de huidige componenten is het mogelijk om het zelfde niveau te behalen als met de producten van Juniper of Cisco. Tevens zijn de componenten al reeds in productie, waardoor het implementatietraject korter zal zijn. Dit is tevens een doelstelling uit het beleid.
- In tijden van bezuinigingen moet er goed gekeken worden waar geld aan wordt uitgegeven. In het strategisch ICT-beleid wordt daarom gewezen op het zo efficiënt mogelijk om gaan met aanschaf van de middelen. Het is daarom van belang dat er eerst gekeken wordt of er al middelen aanwezig zijn, voordat er overgegaan wordt tot aanschaf van nieuwe middelen. Een belangrijk punt is dan ook om te kijken of componenten hergebruikt kunnen worden.
- Een ander belangrijk punt is dat het aanschaffen van een NAC-oplossing van Cisco of Juniper ver boven de aanbestedingsgrens van €193.000 zouden uitkomen excl. jaarlijkse support en licentiekosten. Bij Cisco gaat het hier zelfs om bedragen van €300.000 á €350.000. Terwijl bij het hergebruiken van componenten de kosten ver onder de aanbestedingengrens blijven van €193.000. Hierdoor hoeft het NAC-ontwerp niet aanbesteed te worden, waardoor een keuzevrijheid is om de componenten te selecteren.
- Het laatste punt waarom er gekozen is om geen gebruik te maken van de Cisco of Juniper oplossingen, is omdat de componenten die hergebruikt worden als in productie zijn. Hierdoor hoeven alleen de juiste koppelingen gemaakt worden. Dit zal de tijd van de implementatie van NAC verkorten.

Het nieuwe NAC-ontwerp is getest aan de hand van een pilot op de Oudenoord 370. Tevens zijn er op verschillende faculteiten diverse punten getest. Dit is gedaan om alle soorten apparatuur te testen in combinatie met het nieuwe NAC-ontwerp. Tijdens de pilot zijn er een aantal belangrijke en interessante resultaten naar voren gekomen, namelijk:

- Het mechanisme dat apparatuur authentiseert aan de hand van het MAC-adres, is gevoelig voor misbruik. Echter kan dit opgelost worden door dynamic APR inspection te configureren op het netwerk.
- Salto, het sleutelsysteem dat door de Hogeschool Utrecht wordt gebruikt, werkt niet met NAC. Omdat het om +/-20 punten gaat is het mogelijk om dit handmatig te beveiligen.
- Doordat er tijdens de pilot getest is met de thread management module van Palo Alto, kon er gekeken worden hoeveel apparaten er besmet zijn met virus en malware. Uit de test van twee weken zijn er 129 apparaten gedetecteerd die besmet zijn met virus en/of malware. Dit is veel hoger dan de huidige methode. In de huidig methode worden er gemiddeld 2 tot 3 gedetecteerd per week(dit is excl. de virusscanners die op computers van de Hogeschool Utrecht wordt gebruikt). Daarnaast is waargenomen dat hack pogingen gedaan worden op servers en computers van de Hogeschool Utrecht.
- Netwerkverkeer koppelen aan een gebruikersnaam is in het nieuwe ontwerp mogelijk. Tijdens de pilot was er zoveel enthousiasme voor deze functie, dat deze functie reeds geïmplanteerd is op het draadloos netwerk van de Hogeschool Utrecht.
- Authentiseren op het netwerk gaat snel. Gemiddeld wordt een apparaat op het bekabeld netwerk geauthentiseerd binnen 1 á 2 seconden. Op het draadloos netwerk duurt dit langer. Gemiddeld wordt een apparaat op het draadloos netwerk binnen 4 á 5 seconden geauthentiseerd. Dit komt omdat op het draadloos netwerk meer factoren meespelen dan op het bekabeld netwerk. Als alleen naar het authenticatieproces gekeken wordt, is dit net zo snel als op het bekabeld netwerk.
- Doordat gebruikers en apparaten dynamisch een netwerksegment krijgen toegewezen hoeven beheerders en steunpunt medewerkers geen extra handelingen te doen om een apparaat of gebruiker in het juiste netwerksegment te zetten. Tevens is het niet meer mogelijk dat gebruikers of apparatuur in verkeerde netwerksegmenten terecht komen.

Uit deze pilottest is gebleken dat NAC, op het juiste niveau, extra waarde geeft aan de veiligheid en beheersbaarheid van het netwerk. Daarnaast is NAC essentieel voor het bring your own device(BYOD) concept en het flexibele werken dat de Hogeschool Utrecht voor ogen heeft. Want door het toepassen van NAC kan bepaalt worden per apparaat en per gebruiker of gebruikersrol wie wel en wie geen toegang heeft tot de verschillende resources.

De kosten voor het nieuwe NAC-ontwerp worden in tabel hieronder weergegeven. Dit zijn de kosten die het totale NAC-ontwerp op jaarbasis kost. Deze kosten zijn inclusief het onderhoud aan apparatuur, licenties en beheer.

Jaarlijkse kosten		
2 x Windows Server 2008 R2	€	3.000,-
3 x Ubuntu Server 12.04	€	4.500,-
Qnet Appliance	€	8.200,-
Palo Alto Thread Management PA-5050-TP-HA	€	13.500,-
Totaal	€	29.200,-

De initiële kosten die gemaakt worden, voor het inrichten van NAC, zijn gebaseerd op de tijden die gemaakt zijn bij de uitvoering van de pilot. De initiële kosten zijn als volgt:

Initiële kosten		
Implementatie kosten 208 switches (208x3 uur = 624 uur x € 30,- per uur)	€	18.720,-
Implementatie servers (+/- 100 uur x € 30,- per uur)	€	3.000,-
Totaal	€	21.720,-

Inhoudsopgave

1. Inleiding

Dit document bevat het onderzoek naar Network Access Control(NAC) binnen de Hogeschool Utrecht. In dit document wordt onderzocht of NAC volwassen genoeg is om gebruikt te worden binnen de Hogeschool Utrecht. Het document bestaat uit een aantal fases:

- Onderzoek naar NAC;
- Onderzoek naar de huidige situatie en gewenste situatie;
- Functioneel ontwerp;
- Technisch ontwerp;
- Adviesrapport.

In het onderzoek naar NAC wordt beschreven wat NAC inhoudt en welke vormen van NAC er mogelijk zijn. In de huidige situatie is beschreven of NAC al gebruikt wordt en op welke manier dit gedaan is. Aan de handt van interviews en het strategisch ICT-beleid van de Hogeschool Utrecht zullen eisen en wensen geformuleerd worden. Tevens zullen deze eisen en wensen ingedeeld worden volgens de MoSCoW methode.

Aan de hand van de eisen een wensen zullen er ontwerpkeuzes worden gemaakt die bepalend zijn voor het functioneel en technisch ontwerp. In het functioneel ontwerp wordt de functionele werking van het nieuwe NAC-ontwerp beschreven. Aan de hand van het functioneel ontwerp zal het technisch ontwerp worden beschreven. Hierin wordt het functioneel ontwerp naar technisch oplossingen vertaald.

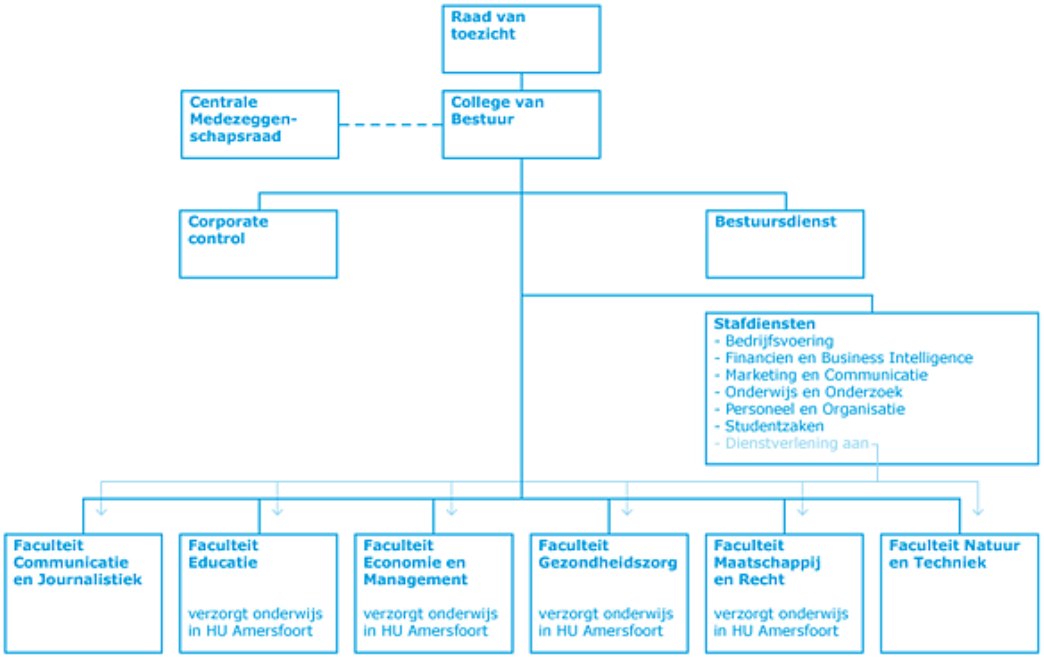
In de laatste fase zal er een advies worden uitgebracht naar het management van de Hogeschool Utrecht. Dit advies zal onderbouwd worden door een pilot die is uitgevoerd op de Oudenoord 370. Aan de handt van deze pilot zullen de resultaten beschreven worden en zal er een advies gegeven worden voor NAC binnen de Hogeschool Utrecht.

2. Hogeschool Utrecht

2.1.De organisatie

Hogeschool Utrecht is een HBO onderwijsinstelling die in 1995 ontstaan is door een fusie van een aantal hogescholen in Utrecht. De fusie is tot stand gekomen vanwege een overheidsmaatregel om landelijk bijna 80 hogescholen te fuseren tot 45 nieuwe hogescholen. Tot 2004 droeg de organisatie de naam: Hogeschool van Utrecht. Maar in 2005 hebben zij deze naam veranderd in Hogeschool Utrecht. Aan de Hogeschool Utrecht studeren bijna 40.000 studenten. Deze studenten zijn verdeelt over 6 faculteiten en 12 vestigingen, die gevestigd zijn in Utrecht en Amersfoort. Naast de studenten werken er ongeveer 3.500 medewerkers. De Hogeschool Utrecht is een plek waar studenten en medewerkers zich kunnen ontplooien, zich thuis voelen en waar we door samen te werken met onze relaties durven te experimenteren en innoveren.

2.2.Organigram Hogeschool Utrecht



afbeelding 1: Organigram Hogeschool Utrecht

2.3.Plaats van afstuderen

Deze opdracht wordt binnen de Hogeschool Utrecht uitgevoerd op de afdeling Infrabeheer. Deze afdeling is onderdeel van stafdiensten bedrijfsvoering(SBV). Dit team is verantwoordelijk voor de basis ICT-infrastructuur van de Hogeschool Utrecht. De afdeling infrabeheer is verantwoordelijk voor het beheren, migreren, implementeren en ontwikkelen van de basis ICT-voorzieningen voor de Hogeschool Utrecht. Afdeling Infrabeheer werken nauw samen met de afdeling applicatiebeheer. Deze afdeling beheerd de applicaties die binnen de Hogeschool Utrecht gebruikt worden.

3. De afstudeeropdracht

3.1.Aanleiding

De Hogeschool Utrecht heeft een koers uitgezet genaamd: Koers 2012. In Koers 2012 wordt de strategische koers ten aanzien van de HU bedrijfsvoering geformuleerd. Vanuit deze koers is er een strategisch ICT-beleid HU 2010-2015 ontwikkeld, die de ambities van de Hogeschool Utrecht op ICT gebied vastlegt. Dit wordt gedaan in de vorm van doelstellingen met de daaraan verbonden kaders.

De manager van de afdeling infrabeheer Ed de Vries heeft gevraagd om te kijken, hoe er vanuit netwerkbeheer een bijdrage geleverd kan worden om de doelstelling van het strategisch ICT-beleid te ondersteunen. In samenspraak met Ed de Vries heb ik er voor gekozen om onderzoek te doen hoe de Hogeschool Utrecht gebruik kan maken van Network Access Control. De doelstellingen waar dit onderzoek een bijdragen aan zal leveren zijn:

- Een omgeving scheppen om te komen tot een open virtuele kennisorganisatie;
- ICT dienstverlening is gebaseerd op anytime, anywhere, any device;
- De ICT dienstverlening ondersteunt in toenemende mate de zelfredzaamheid en zelfservice van gebruikers (studenten, medewerkers en externen);
- Specifieke ICT dienstverlening op basis van standaard bouwstenen (modulair opgebouwde ICT voorzieningen) en standaard gegevensuitwisseling (interoperabiliteit).

3.2.Probleemstelling

De Hogeschool Utrecht heeft een groot data netwerk, dat netwerkconnectiviteit geeft aan een groot aantal apparaten. De diversiteit van deze apparaten loopt uiteen van chipknip oplaadpunten tot privé laptops van studenten, medewerkers en externe partners. Deze apparaten kunnen gebruikmaken van zowel het bekabeld als draadloos netwerk van de Hogeschool Utrecht.

Een groot aantal apparaten van de Hogeschool Utrecht, valt buiten het beheer van de organisatie. Hierdoor is de kans groot dat de apparaten die op het netwerk zijn aangesloten malware, virussen of ander kwaadwillende software met zich mee dragen. Hierdoor Is de kans groot dat malware, virussen of ander kwaadwillende software zich kunnen verspreiden over het data netwerk en voor problemen kunnen zorgen. Daarnaast kan een gebruiker ook kwaadwillende intenties hebben.

Op het bekabeld netwerk is geconstateerd dat er regelmatig apparatuur van studenten, medewerkers of externe partners in verkeerde netwerksegmenten terecht komen. Zo komt het voor dat apparatuur van zowel studenten, medewerkers als externe partners, ook terecht komen in betaal, chipknip en andere bedrijf kritische netwerken.

Naast de mogelijke problemen die hierboven zijn genoemd, neem het werkplek onafhankelijk werken een steeds grotere rol in binnen de Hogeschool Utrecht. Hierdoor gaan gebruikers meer werken op verschillende locaties of werken vanuit huis. Door het statische karakter van het netwerk is dit voor medewerkers met een systeembeheer, financiële of dergelijke bedrijfsinformatie gevoelige applicaties niet mogelijk. Dit omdat per switchpoort en per VLAN rechten worden toegekend.

3.3.Doelstelling

De doelstelling van deze afstudeeropdracht, is om te onderzoeken hoe en of het mogelijk is om Network Access Control(NAC) te gebruiken binnen het netwerk van de Hogeschool Utrecht. Hierbij is het de bedoeling dat medewerkers, cursisten en studenten tijd- en plaats onafhankelijk kunnen

werken . Waarbij ze de keuze vrijheid hebben in de daarvoor benodigde apparatuur. Studenten, cursisten en medewerkers moeten daarbij onafhankelijk van plaats of tijd toegang hebben tot de benodigde informatie. Dit mag echter niet ten kosten gaan van de integriteit, confidentialiteit en authenticiteit. Op het draadloos netwerk van de Hogeschool Utrecht wordt er al aan toegangscontrole gedaan. Echter is dit nog beperkt. Naast het bekabeld netwerk zal dus ook naar het draadloos netwerk gekeken moeten worden. Zodat er één oplossing komt voor het toegang krijgen tot het netwerk van de Hogeschool Utrecht. Door middels van een pilot moet blijken of Network Access Control(NAC) volwassen genoeg is om gebruikt te worden binnen de Hogeschool Utrecht. Concreet zijn de volgende eisen en doelstelling opgesteld:

- Inventariseren welke apparaten er gebruik maakt van het datanetwerknetwerk;
- Inzicht krijgen in welke natuurlijke personen gebruik maken van het netwerk;
- Dynamisch VLAN(logische compartimentering) toewijzen aan de persoon op basis van de functie of rol;
- Het vroegtijdig detecteren van misbruikt en malware;
- De oplossing moet werken volgens een cliënt-less authenticatie en autorisatie mechanisme;
- De oplossing mag geen singlepoint of failure(SPOF) zijn;
- De oplossing moet werken met openstandaard of marktconform geaccepteerde standaarden;
- De oplossing moet mogelijkheid bieden tot een gast netwerk;
- De oplossing moet flexibel uit te breiden zijn naar VPN en draadloos, zodat access control één geheel wordt;
- De oplossing moet mee groeien in de toekomst;
- Dataverkeer moet te herleiden zijn naar een natuurlijk persoon.

3.4.Afbakening

De afstudeeropdracht kent ook zijn afbakening. Om aan te geven wat wel of niet gedaan wordt tijdens deze afstudeeropdracht wordt in dit hoofdstuk aangeven wat binnen of buiten de scope van de opdracht valt.

3.4.1. Binnen de scope

- Onderzoek naar Netwerk Access Control;
- Onderzoek naar de huidige situatie;
- Onderzoek naar de gewenste situatie;
- Opstellen onderzoeksrapport;
- Functioneel ontwerp maken;
- Technisch ontwerp maken;
- Pilot uitvoeren, om te laten zien of NAC wel of geen oplossing is voor de Hogeschool Utrecht;
- Opstellen adviesrapport.

3.4.2. Buiten de scope

- De daadwerkelijke implementatie;
- Onderzoeken naar de functie en rollen die gebruikt worden binnen de HU, denk hierbij aan rollen zoals: onderwijsassistent, bedrijfsbegeleider en p&o medewerker ;
- Ontwerp maken van de netwerksegmenten (logische compartimentering);
- Onderzoek welk product(merk) er gebruikt moet gaan worden, dit i.v.m. de Europese aanbesteding van het netwerk;
- Opstelling implementatieplan.

4. Activiteiten en producten

Om structuur te geven aan het afstuderen is de afstudeeropdracht in verschillende fases opgedeeld. Tevens zullen er uit de verschillende fases verschillende producten worden opgeleverd. De fases en producten die opgeleverd worden zijn:

4.1.Fase 1: Initiatiefase

De initiatiefase is de voorbereiding op de afstudeeropdracht. Na de goedkeuring van het afstudeervoorstel door de afstudeercommissie, zal er in februari gestart worden met deze fase.

Activiteiten:

- Het maken van de Plan van Aanpak
- Het maken van de projectplanning
- Het afsluiten van het afstudeercontract

Producten:

- Plan van aanpak
- Afstudeercontract

4.2.Fase 2: Analysefase

In de analysefase wordt de inventarisatie gedaan van de informatie die nodig is voor het project. Deze resultaten zullen verwerkt worden in een onderzoeksrapport.

Activiteiten:

- Onderzoek: Wat is Network Access Control?
- Onderzoek naar de huidige situatie
  - Huidige situatie netwerk
  - Huidige situatie toegangscontrole
- Onderzoek naar de gewenste situatie
  - Onderzoek gewenste situatie vanuit management perspectief
  - Onderzoek gewenste situatie vanuit security perspectief
  - Onderzoek gewenste situatie vanuit beheer perspectief
  - Onderzoek gewenste situatie vanuit gebruikers perspectief

Producten:

- Onderzoeksrapport

4.3.Fase 3: Ontwerpfase

In deze fase wordt gestart met het maken van een functioneel en technisch ontwerp. In het functioneel ontwerpt wordt gekeken naar de functies die de te bouwen oplossing moet bieden. Dit zal zodanig worden omschreven dat het functioneel ontwerp goed te begrijpen is zonder technisch kennis. In het technisch ontwerp zal omschreven worden hoe het functioneel ontwerp technisch gerealiseerd gaat worden.

Activiteiten:

- Functioneel ontwerp maken
- Technisch ontwerp maken

- Proof of concept ter ondersteuning aan het technisch ontwerp

Producten:

- Functioneel Ontwerp
- Technisch Ontwerp

4.4.Fase 4: Realisatiefase

In de realisatiefase wordt een pilot uitgevoerd op een deel van het netwerk. Daarnaast zal moeten blijken of Network Access Control volwassen is om gebruikt te worden binnen de IT infrastructuur van de Hogeschool Utrecht.

Activiteiten:

- Pilot uitvoeren
- Resultaten analyseren

Producten:

- Adviesrapport

4.5.Fase 5: Afronding

Dit is de laatste fase van het project. In deze fase zal de scriptie opgeleverd worden. Deze scriptie wordt vervolgens aangeboden aan de Hogeschool Utrecht ter beoordeling. Na een goedkeuring zal ik deze scriptie gaan verdedigen in de vorm van een presentatie.

Activiteiten:

- Afronding scriptie
- Verdediging scriptie

Producten:

- Scriptie

5. Onderzoeksrapport

5.1.Inleiding

Dit onderzoeksrapport bevat de resultaten van het vooronderzoek over Network Access Control(NAC) binnen de Hogeschool Utrecht. Dit onderzoeksrapport gaat in op wat NAC is, hoe NAC is vormgegeven in de huidige situatie en wat de gewenste situatie is met betrekking op NAC.

Er wordt beschreven hoe er in de huidige situatie toegang wordt gegeven tot het netwerk. Om in kaart te brengen welke apparatuur er gebruik maken van het netwerk, is er een inventarisatie gemaakt. Dit is gedaan voor zowel de aangesloten apparatuur als de netwerk componenten die de toegang verlenen. Maar ook netwerk mechanismes die van invloed kunnen zijn op de implantatie van NAC komen aan bod.

De eisen en wensen zijn in kaart gebracht door middel van interviews en het strategisch ICT-beleid HU 2010 – 2015 van de Hogeschool Utrecht. De gegevens uit de interviews en het strategisch ICT-beleid zijn vervolgens geanalyseerd en geven weer wat de Hogeschool Utrecht wil bereiken met NAC. Aan de hand van deze gegevens zijn de eisen en wensen opgedeeld volgens de MoSCoW-methode.

5.2.Network Access Control

5.2.1. Wat is Network Access Control

Network Access Control(NAC) is een beveiligingsconcept die de access laag, van het OSI model, voorziet van toegangscontrole. Op de acces laag worden de apparaten aangesloten die gebruiken willen maken van het netwerk.

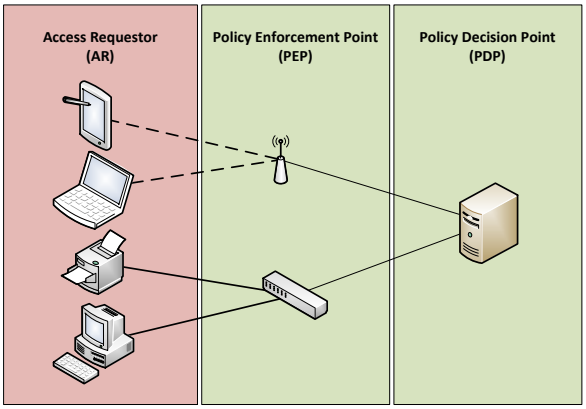
NAC is een concept en niet een opzichzelfstaande oplossing. NAC is een term die verschillende technologieontwikkelingen omschrijft, die er samen voor zorgen dat een gebruiker of apparaat wel, geen of beperkt toegang krijgt tot het netwerk op basis van authenticatie, autorisatie en/of health check.

In het NAC concept wordt de toegang tot het netwerk verleend op basis van een authenticatie mechanisme. In de meeste gevallen wordt een gebruikersnaam en wachtwoord als authenticatie gebruikt, maar ook een certificaat kan een apparaat authentiseren. Aan de hand van een rol die een gebruiker of apparaat heeft binnen een organisatie, wordt er bepaalt hoeveel en welke rechten er gegeven worden op het netwerk. Dit wordt autorisatie genoemd.

Om er voor te zorgen dat gebruikers en apparatuur voldoen aan de aansluitvoorwaarden, kan er een health check uitgevoerd worden. Deze health checks controleren of de computers voldoen aan de aansluitvoorwaarden. In deze voorwaarde staan eisen waaraan een gebruiker en computer moeten voldoen, voordat zij gebruik mogen maken van het netwerk. Zo kan een aansluitvoorwaarde zijn dat een computer voorzien moet zijn van antivirus software of dat de computer up-to-date moet zijn.

De health checks kunnen op verschillende manieren worden uitgevoerd. Dit kan door bijvoorbeeld een stukje software, die op de computer geïnstalleerd moet worden. Deze software controleert of de computer voldoet aan de aansluit voorvoorwaarden. Een andere manier om te controleren of een gebruiker en apparaat aan het beleid voldoet, is door het inspecteren van het netwerkverkeer van de gebruiker. Als de computer aan de voorwaarden voldoet zal de computer toegelaten worden tot het netwerk.

Het NAC concept bestaat uit drie onderdelen. Deze drie onderdelen zijn: Access Requestor(AR), Policy Enforcement Point(PEP) en Policy Decision Point(PDP).



afbeelding 2: Overzicht AR,PEP en PDP

Access Requestor

De Access Reguestor(AR) is de cliënt die een verzoek doet om toegang te krijgen tot het netwerk. Dit is de “cliënt-side” van het NAC concept. De AR kan een werkstation of laptop zijn, maar een printer, IP camera, mobiele telefoon of koffieautomaten kunnen ook AR’s zijn.

Policy Enforcement Point

De Policy Enforcement Point(PEP) is de locatie in het netwerk waar de toegang tot het netwerk gegeven wordt. PEP is een netwerk- en/of beveiligingscomponent dat toegang verleend op basis van de beslissing die de Policy Decision Point(PDP) heeft gemaakt. Per implementatie verschilt dit. Vaak wordt dit gedaan op een netwerk switch of wireless access point, maar een firewall, intrusion detection of intrusion prevention system kan ook worden ingezet als PEP.

Policy Decision Point

De locatie waar de beslissing wordt genomen, wanneer een gebruiker of apparaat toegang krijgt tot het netwerk, wordt Policy Decision Point(PDP) genoemd. Bij NAC is dit vaak een radiusserver. Deze PDP heeft drie basis taken.

- De PDP verzamelt gegevens van gebruikers en apparatuur die toegang willen tot het netwerk;
- Aan de hand van de informatie wordt besloten of een gebruiker of apparaat toegang krijgt tot het netwerk en hoeveel rechten deze gebruiker of apparaat krijgt;
- De PDP stuurt zijn beslissing naar de PEP om toegang te geven tot het netwerk.

Het IEEE openstandaard 802.1x is een protocol dat veel toegepast wordt bij het implementeren van NAC. Net als bij het NAC concept is 802.1x bedoeld om gebruikers en apparatuur te authentiseren en autoriseren. Dit wordt gedaan voordat een gebruiker en/of apparaat gebruik mag maken van het netwerk.

802.1x wordt al op grote schaal toepast op draadloos netwerken. Op het bekabeld netwerk wordt het nog weinig toegepast, dit komt vooral door de beperking van apparatuur met ondersteuning voor 802.1x. Dit is in de loop der jaren wel verbeterd, maar de meeste pinapparaten, IP camera’s en gebouwbeheersystemen ondersteunen tot op de dag van vandaag nog steeds geen 802.1x of is erg slecht geïmplementeerd.

Het verschil tussen NAC en 802.1x is dat NAC een concept is en 802.1x een protocol is waarmee je NAC kan realiseren. Er bestaan ook NAC-oplossingen zonder 802.1x, maar deze oplossingen zijn veelal gebaseerd op proprietary protocollen.

5.2.2. Vormen van NAC

802.1x kan dus gebruikt worden als NAC en wordt ook wel gezien als meest simpele vorm van NAC. 802.1x is echter beperkt tot het authentiseren en autoriseren van apparatuur en gebruikers. Wat in sommige situaties voldoende is. Als we een stap verder gaan wordt er veel gebruik gemaakt van een quarantaine netwerk, dit is een netwerk waar alle geïnfecteerde apparatuur met malware of gebruikers die misbruik hebben gemaakt van het netwerk in terecht komen. Het quarantainenetwerk is daarom beperkt in de functionaliteit. In de meeste gevallen is het quarantainenetwerk gescheiden van het bedrijfsnetwerk en hebben de apparaten beperkt toegang tot het internet om zichzelf malware vrij te maken.

De volgende stap in NAC is het tegengaan van malware en misbruik op het netwerk, door het toepassen van thread prevention of inspection. Dit kan gedaan worden door een health check. Door te controleren of het besturing systeem is bijgewerkt en de antivirus software up-to-date is kan er besloten worden of een apparaat of gebruiker toegang mag tot het netwerk. Een andere manier om te controleren of een apparaat malware bevat of dat een gebruiker misbruik maakt van het netwerk, is door gebruik te maken van een intrusion detection en/of prevention system(IDS/IPS). Het IDS/IPS systeem inspecteert het netwerk, zodra het IDS/IPS systeem vreemde activiteiten ziet of malware herkent kan het IDS/IPS systeem een melding genereren. Aan de hand van deze melding kan de gebruiker of apparaat in quarantaine worden gezet. Natuurlijk kan dit proces ook geautomatiseerd worden.

Fingerprinting is een manier om verkeer te koppelen aan een gebruiker. Door netwerk verkeer te voorzien van de naam van de gebruiker wordt het inzichtelijk wie verantwoordelijk is voor welk netwerk verkeer.

De laatste stap in NAC is device profiling. Dit is een mechanisme die kan bepalen wat voor een apparaat aangesloten wordt op het netwerk. De device profile engine kan onderscheid maken tussen iPhone, laptops, webcam, Android smartphone ‘s enz. Maar ook kan de device profile engine bepalen welke versie van het besturing systeem op het apparaat staat geïnstalleerd. Aan de hand van deze profielen kunnen policies worden gemaakt.

Er bestaan dus verschillende manieren voor het toepassen van NAC. Hieronder zijn de manieren, hoe NAC toegepast kan worden, opgedeeld in vijf verschillende niveaus.

- **Niveau 1 NAC:** authenticatie en autorisatie;
- **Niveau 2 NAC:** authenticatie, autorisatie en quarantaine;
- **Niveau 3 NAC:** authenticatie, autorisatie, quarantaine en thread prevention;
- **Niveau 4 NAC:** authenticatie, autorisatie, quarantaine, thread prevention en fingerprinting;
- **Niveau 5 NAC:** authenticatie, autorisatie, quarantaine, thread prevention, fingerprinting en profiling.

5.3.Huidige situatie

5.3.1. Netwerk toegang

De Hogeschool Utrecht biedt voor grote diversiteit aan apparatuur netwerk toegang. Deze apparaten kunnen op twee manieren toegang krijgen tot het netwerk. De eerste manier is om het apparaat met een netwerkkabel te verbinden aan het bekabeld netwerk. De tweede manier om te verbinding met het netwerk is via het draadloos netwerk. Maar hoe wordt de toegang verleend op deze netwerken? In de volgende twee paragrafen zal beschreven worden hoe deze apparaten, in de huidige situatie, toegang krijgen tot het netwerk van de Hogeschool Utrecht. Dit zal beschreven worden vanuit het bekabeld en draadloos.

5.3.1.1. Bekabeld netwerk

Wanneer een apparaat, met een bekabeld netwerkaansluiting, gebruik wil maken van het bekabeld netwerk van de Hogeschool Utrecht, dan kan het apparaat aangesloten worden op een access switch in één van de faculteiten. Per locatie verschilt het of de access/patch poorten beschikbaar worden gesteld aan studenten, medewerkers en/of netwerk apparatuur zoals printers, pinapparaten of IP camera's. Op de access switch wordt een netwerkpoort in het juiste Virtual Local Area Network (VLAN) gezet. Een VLAN wordt gebruikt om netwerk segmenten te kunnen scheiden. Door middel van VLANS wordt het netwerk verkeer van elkaar gescheiden, zodat VLAN "studenten" niet zomaar bij VLAN "financiële administratie" kan komen. De firewall is het netwerk component dat er voor zorgt dat deze VLANS elkaar niet kunnen bereiken. Door policies toe te voegen aan de firewall kunnen netwerk wel of niet met elkaar communiceren. NAC wordt nu dus niet gebruikt op het bekabeld netwerk. Iedereen kan namelijk zijn apparaat aansluiten op het netwerk, zonder dat de gebruiker of het apparaat zich hoeft te authentiseren. Het gevolg hiervan is dat er veel apparaten zoals beveiligingscamera's in verkeerde VLANS terecht komen. Doordat beveiligingscamera's zomaar worden aangesloten, zonder toestemming, kan de ICT afdeling niet garanderen dat beveiligingscamera's goed afgesloten zijn voor student, medewerkers of andere onbevoegde. Dit is echter maar één voorbeeld. In de praktijk zijn er meer vergelijkbare situatie waar onbevoegden toch toegang kunnen krijgen tot systemen waar zij eigenlijk geen toegang toe hebben.

5.3.1.2. Draadloos netwerk

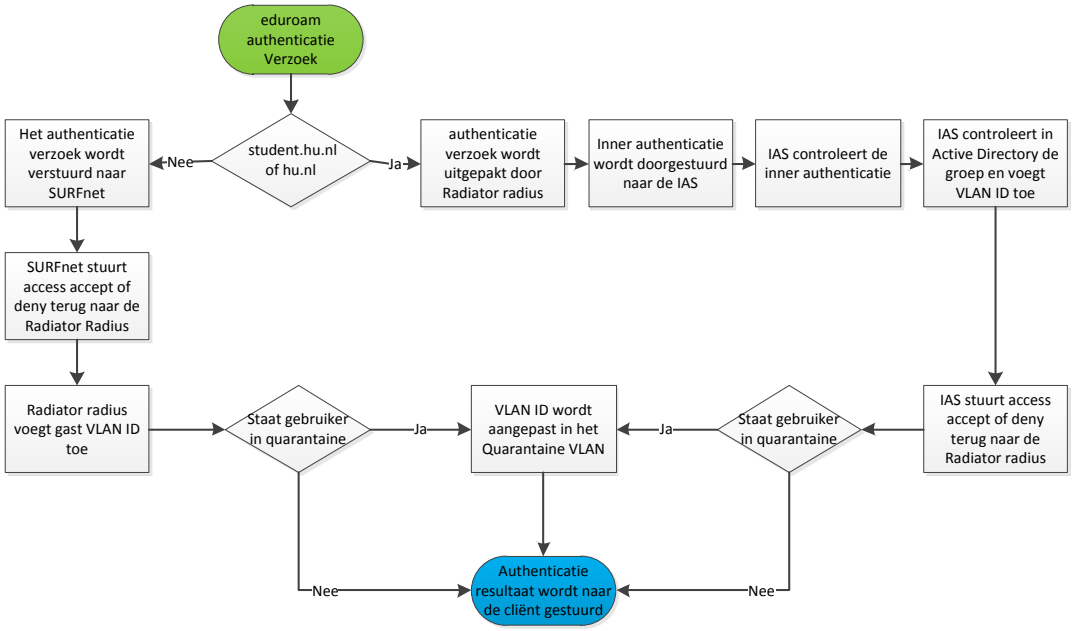
Op het draadloos netwerk van de Hogeschool Utrecht wordt al enige tijd gebruik gemaakt van 802.1x. Dit wordt gebruikt om medewerkers en studenten te authentiseren, voordat er toegang gegeven wordt tot het draadloos netwerk. Maar ook laptops, die in beheer zijn van de Hogeschool Utrecht, worden geauthentiseerd door middel van het computeraccount. Het computeraccount wordt gebruikt om de computer te authentiseren aan het Active Directory domain van de Hogeschool Utrecht, maar kan dus ook gebruikt worden om laptops te authentiseren op het draadloos netwerk. Op het draadloos netwerk van de Hogeschool Utrecht wordt dus al NAC toegepast. Echter kunnen we dit classificeren als een Niveau 2 NAC implementatie.

Op het draadloos netwerk wordt gebruik gemaakt van twee SSID's. Dit zijn netwerknamen waarmee verbinding gemaakt kan worden, om toegang te krijgen tot het netwerk. Op de Hogeschool Utrecht wordt gebruik gemaakt van twee van dit soorten SSID's. Dit zijn eduroam en hu-mdw.

eduroam

eduroam kan gebruikt worden door studenten en medewerkers van de Hogeschool Utrecht. Zij kunnen zich op dit netwerk authentiseren door gebruik te maken van hun inloggegevens. eduroam wordt niet alleen binnen de Hogeschool Utrecht gebruikt. Dit is een netwerknaam die wereldwijd gebruikt wordt door hogescholen, universiteiten en onderzoeksinstellingen die aangesloten zijn bij het eduroam

netwerk. Hierdoor is het mogelijk dat gebruiker van andere instellingen gebruik kunnen maken van het netwerk van de Hogeschool Utrecht. Voor het verbinding maken met het draadloos netwerk van Hogeschool Utrecht kunnen zij gebruik van de inloggegevens van hun eigen instelling.



afbeelding 3: Functioneel proces eduroam netwerk Hogeschool Utrecht

Op afbeelding 3 wordt het functioneel proces weergeven van het authentiseren op het eduroam netwerk. In deze afbeelding is te zien hoe het authenticatie proces verloopt. Dit proces verloopt als volgt: Ten eerste komt een authenticatie verzoek binnen van een apparaat, die gebruik wil maken het eduroam netwerk. In dit authenticatie verzoek staat de inlognaam en het wachtwoord van de gebruiker. Om onderscheid te kunnen maken tussen de verschillende instellingen, die gebruik maken van het eduroam netwerk, wordt het emailadres gebruikt als inlognaam. Aan de domeinnaam van het emailadres kan herleidt worden tot welke instellingen de gebruiker behoort. In een authenticatie verzoek wordt deze domeinnaam ook wel het realm genoemd.

In het authenticatie verzoek wordt gekeken wat de realm is waarmee de gebruiker inlogt. Is de realm student.hu.nl of hu.nl, dan zal het authenticatieverzoek worden afgehandeld door de radiusserver van de Hogeschool Utrecht. Is de realm anders, dan zal het authenticatieverzoek doorgestuurd worden naar de radiusserver van SURFnet. Daarnaast slaat de radius de accounting gegevens op in een accounting database. Zodat er achteraf gekeken kan worden op welk tijdstip een gebruiker of apparaat ingelogd heeft op het netwerk. Verder worden ook de sessies bijgehouden door de radiusserver. In deze sessies wordt de hoeveel geüpload en/of gedownload verkeer bijgehouden.

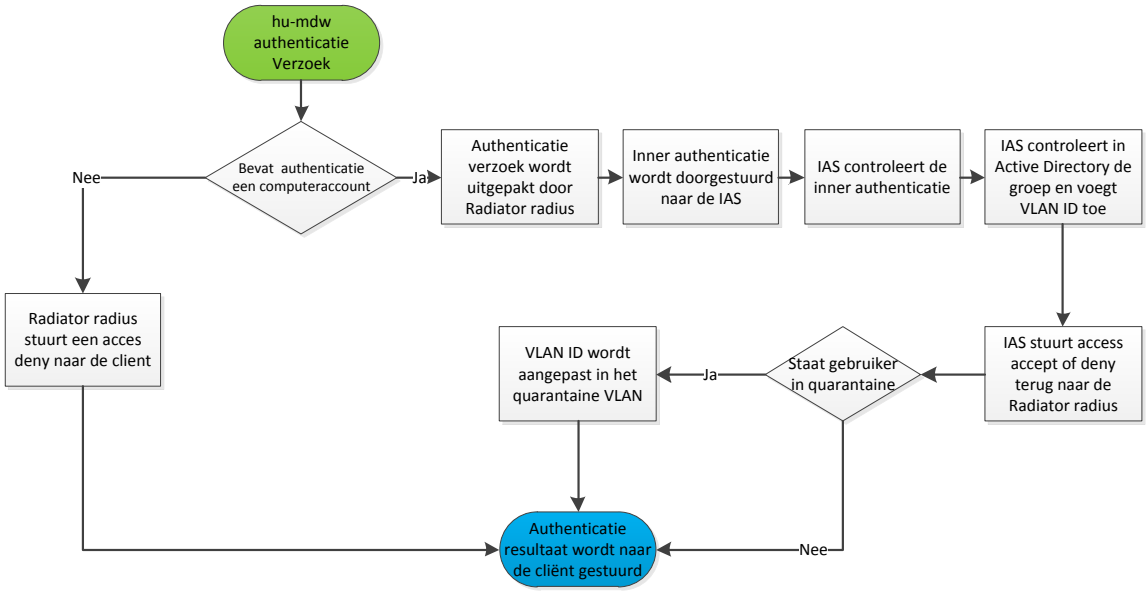
Wanneer er een authenticatie verzoek binnen komt op Radiator radius, dit is de radius die gebruikt wordt door de Hogeschool Utrecht, wordt het authenticatieverzoek uitgepakt. De authenticatie wordt doorgestuurd naar de Internet Authentication Service(IAS), de radiusserver van Active Directory(AD). De IAS controleert de inner authenticatie en kijkt in AD tot welke groep de gebruiker behoort. Aan de hand van de groep, waar de gebruiker lid van is, wordt er een VLAN ID toegevoegd in het responsbericht. Het responsbericht bevat naast het VLAN ID ook een access accept of deny, die terug gestuurd wordt naar de Radiator. Vervolgens wordt er een controle gedaan door de radiusserver of het apparaat of gebruiker in quarantaine gezet moet worden. Quarantaine is een netwerksegment dat gebruikt wordt om computers die malware bevatten of misbruik maken van het netwerk beperkt toegang te geven tot het internet. Als de computer of gebruikersnaam bekend is in bij het

quarantainenetwerk, zal Radiator het VLAN ID aanpassen in het quarantaine VLAN. En als laatst zal het responsbericht met het resultaat teruggestuurd worden naar het apparaat dat het authenticatie verzoek heeft gedaan.

Als SURFnet het authenticatieverzoek afhandelt, zal SURFnet een access accept of deny responsbericht terugsturen naar de Radiator, de radiusserver van de Hogeschool Utrecht. Radiator zal een VLAN ID toekennen die speciaal bedoeld is voor studenten of medewerkers van andere hogescholen, universiteiten en onderzoeksinstellingen. Net zoals bij de verzoeken die door de Hogeschool Utrecht zelf worden afgehandeld, zullen ook de authenticatie verzoeken die vanuit SURFnet komen gecontroleerd worden of zij in quarantaine gezet moeten worden.

Hu-mdw

Het hu-mdw netwerk wordt alleen gebruikt om laptops, die in het beheer zijn van de Hogeschool Utrecht, te laten authentiseren met het draadloos netwerk. Dit wordt gedaan om Active Directory(AD) policies toe te passen op laptops die draadloos verbonden zijn. Een groot deel van de AD policys worden toegepast voordat een gebruiker kan inloggen op de computer. Maar omdat er pas draadloos verbinding kan worden gemaakt wanneer een gebruiker is ingelogd. Zouden er nooit AD policys toegepast kunnen worden op laptops. Daarom wordt de laptop, doormiddel van het computeraccount geauthentiseerd aan het netwerk. Dit gebeurd voordat AD policys worden toegepast. Omdat hu-mdw alleen bedoeld is om te authentiseren met het computeraccount, worden alle andere manieren van authentiseren geweigerd.



afbeelding 4: Functioneel proces hu-mdw netwerk Hogeschool Utrecht

Op afbeelding 4 wordt het functioneel proces weergegeven van het authentiseren op het hu-mdw netwerk. In deze afbeelding is te zien hoe het authenticatie proces verloopt. Het hu-mdw verschilt op twee punten te opzicht van het eduroam netwerk. Het eerste verschil is dat de authenticatie gebeurt op basis van het computeraccount. Het computeraccount is het account dat wordt gebruikt binnen AD om te controleren of de computer lid is van het Active Directory domain. Het tweede verschil is dat het er alleen maar ingelogd kan worden met dit computeraccount. Alle overige authenticatie verzoeken krijgen een access deny. De overige stappen zijn precies hetzelfde als bij het aanloggen op het eduroam netwerk.

5.3.2. Huidig technisch ontwerp

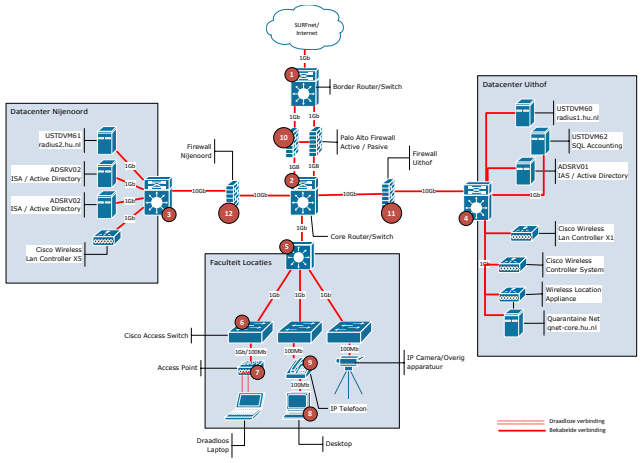
In de hiervoor beschreven hoofdstukken is beschreven hoe er functioneel toegang wordt verleend tot het bekabeld en draadloos netwerk. In deze paragraaf wordt beschreven hoe dit technisch geregeld is.

5.3.2.1. Bekabeld netwerk

Toegangscontrole of een gebruiker of apparaat gebruik mag maken van het netwerk van de Hogeschool Utrecht is er niet. Wel wordt er op het netwerk gebruik gemaakt van firewalls om het verkeer te scheiden en/of te blokkeren. Op afbeelding 5 (een grote weergave van afbeelding 5 is te vinden in bijlage 3) is het technisch ontwerp van de bekabeld infrastructuur schematisch weergegeven. Het netwerk van de Hogeschool Utrecht is opgebouwd uit een core, distributie en een access netwerk laag. Het core netwerk kent een borderrouter/switch(1), core router/switch(2) en twee datacenter routers/swiches(3 en 4). Zowel de border als de core router/switch staan in het datacenter op de Uithof. De distributie laag bestaat uit zes distributie switches(5). Deze staan verspreid over de locaties, die verbinding geven aan de access switches(6). Alleen de Hogeschool Utrecht locatie in de binnenstad is anders ingericht. Op de locatie worden de access switches direct aangesloten op de core router/switch in het datacenter. Deze router/switch functioneert hier ook als distributie switch.

De faculteiten zijn op een standaard wijze ingericht. Elk faculteit heeft zijn eigen distributie switch, dit op de binnenstad locatie na. Op alle faculteiten wordt apparaten die gebruik willen maken van het bekabeld netwerk worden aangesloten op een 100Mb verbinding. De access points(7) worden aangesloten op 100Mb poorten en 802.11n access points worden aangesloten op een 1Gb verbinding. Bekabeld werkstations(8) worden aangesloten via een IP telefoon(9) op de access switch. Dit wordt gedaan om netwerk poorten te besparen.

De Hogeschool Utrecht maakt op dit moment nog gebruik van vier firewalls. Dit zijn de twee Palo Alto firewalls(10) die tussen de internet verbinding en het interne netwerk staan. Deze firewalls controleren en filteren al het in- en uitgaande netwerk verkeer. Dit zijn 'next generation' firewalls. Een next generation firewall controleert de inhoud van de netwerk pakketten en werkt niet op basis van source- en destination poort(statefull firewall). Zo is het mogelijk om tunnelverkeer tegen te houden die gebruik maken van poort 80 en internetverkeer wel toe te laten op dezelfde poort. De 2 Cisco firewalls(11 en 12) die tussen de twee datacenters staan zijn nog wel firewalls die het verkeer controleren op basis van source- en destination poort, maar zullen binnenkort ook vervangen worden voor virtuele Palo Alto firewalls.



afbeelding 5: Infrastructuur Hogeschool Utrecht

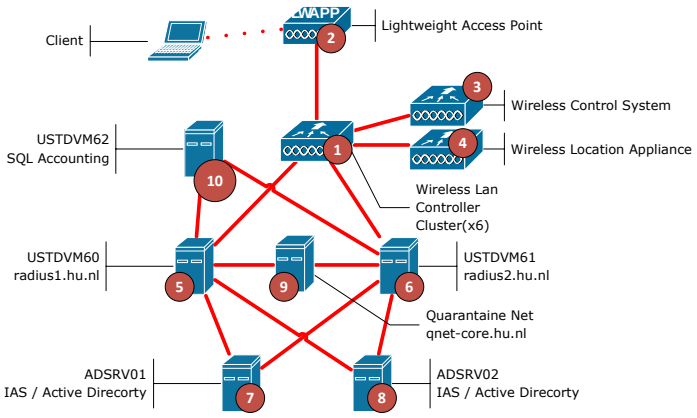
5.3.2.2. Draadloos netwerk

Het draadloos netwerk van de Hogeschool Utrecht bestaat uit een cluster van vijf Cisco 4404 Wireless Lan Controllers en één 5508 Wireless Lan Controller(1). Deze controllers beheren de lightweight access points(2) die verdeeld zijn over de faculteiten. Het verschil tussen een lightweight access point en een normale access point is dat een lightweight access point zich gedraagt als antenne van de Wireless Lan Controller(WLC). De communicatie tussen de access points en de WLC's wordt gedaan via en beveiligde tunnel.

De WLC cluster worden beheerd vanuit het Cisco Wireless Control System(3), dit om het beheer makkelijk te maken en de configuraties gelijk te houden. De Wireless Location Appliance(4) wordt gebruikt om de fysieke locatie van gebruikers of apparatuur te bepalen die gebruik maken van het draadloos netwerk. In de Wireless Control System (WCS) is het mogelijk om te zien waar de gebruikers of apparatuur, die gebruik maakt van het draadloos netwerk, zich bevindt.

Om gebruikers te authentiseren voor het draadloos netwerk, wordt de WLC cluster gekoppeld aan de twee Radiator radiusservers(5 en 6). Die op hun beurt weer gekoppeld zijn aan de twee Internet Authentication Service(7 en 8), de radiusservers van het Active Directory domain. De Radiator radiusservers zitten ook gekoppeld aan de quarantaine server(9), om gebruikers in quarantaine te zetten. En aan een SQL Accounting server(10), die alle radius accountingpakketten registreren.

Het is ook mogelijk om de WLC cluster direct te koppelen aan de Internet Authentication Service(IAS). Echter is er voor gekozen om dit niet te doen. De reden waarom de WLC cluster niet gekoppeld is aan de ISA maar aan de Radiator radiusserver is omdat de IAS niet flexibel genoeg is. Om quarantaine te kunnen gebruiken zijn zelf gemaakte scripts nodig, IAS biedt deze optie niet. Daarom is er voor gekozen om Radiator radius te gebruiken.



afbeelding 6: Technisch Ontwerp Wireless

5.3.3. Inventarisatie hardware

Om inzicht te krijgen in de aangesloten apparatuur is er een inventarisatie gedaan van het apparatuur dat gebruik maakt van het netwerk. Daarnaast is er een inventarisatie gemaakt van de huidige netwerk componenten die binnen de hogeschool Utrecht gebruikt worden. Omdat de meeste NAC-oplossingen gebaseerd zijn op 802.1x zal er ook gekeken worden of de aangesloten apparatuur en de netwerk componenten ondersteuning bieden voor 802.1x.

5.3.3.1. Aangesloten hardware

In onderstaande tabel zijn de resultaten verwerk van de onderzoek naar inventarisatie van de aangesloten hardware. Deze resultaten zijn tot stand gekomen door netwerkscans, interviews met ICT en facilitaire medewerkers. Binnen de Hogeschool Utrecht zijn er ook netwerk en bouwtechniek labs, deze labs hebben een eigen netwerk voorziening en zijn niet meegenomen in de inventarisatie. Er is tevens gekken naar 802.1x, omdat dit het meeste gebruikte protocol is voor NAC.

Naam	802.1x Ondersteuning	bekabeld of draadloos
Salto oplaat punt	Nee	bekabeld
XEROX WorkCentre 7556	Ja	bekabeld
XEROX WorkCentre 5765	Ja	bekabeld
Computer met Windows XP SP2	Ja	bekabeld en draadloos
Computer met Windows Vista	Ja	bekabeld en draadloos
Computer met Windows 7	Ja	bekabeld en draadloos
Computer met Windows 8	Ja	bekabeld en draadloos
Computer met Linux Debian/Mint/Ubuntu	Ja	bekabeld en draadloos
Computer met Linux Fedora	Ja	bekabeld en draadloos
Computer met Linux OpenSuse	Ja	bekabeld en draadloos
Computer met MAC OSX 10.4	Ja	bekabeld en draadloos
Computer met MAC OSX 10.5	Ja	bekabeld en draadloos
Computer met MAC OSX 10.6	Ja	bekabeld en draadloos
Computer met MAC OSX 10.7	Ja	bekabeld en draadloos
iPhone	Ja	draadloos
iPad	Ja	draadloos
Android Phone	Ja	draadloos
Windows Phone / Mobile 6.x	Ja	draadloos
Cisco 7940 IP Phone	Nee	bekabeld
Cisco 7960 IP Phone	Nee	bekabeld
Cisco 7941 IP Phone	Ja	bekabeld
Cisco 7961 IP Phone	Ja	bekabeld
Cisco 7911 IP Phone	Ja	bekabeld
Cisco 7912 IP Phone	Nee	bekabeld
Cisco ATA 186	Nee	bekabeld
Cisco 7920 IP Phone	Ja	draadloos
Cisco 7921 IP Phone	Ja	draadloos
Chipknip/Pin betaal punten	Nee	bekabeld
VIVOTEK IP Camera	Nee	bekabeld
netPAGE BHV systeem	Nee	bekabeld
MOBOTIS IP Camera	Nee	bekabeld
GBS Gebouw beheer systeem	Nee	bekabeld
Moxa Nport	Nee	bekabeld
ADAM-6000	Nee	bekabeld
ECS Kassa	Ja	bekabeld
NetGear Switches	Nee	bekabeld
XBOX 360	Nee	bekabeld en draadloos
PS3	Nee	bekabeld en draadloos
AXIS IP camera	Nee	bekabeld
Indigo Vision IP Camera (doventolk)	Nee	bekabeld
APC UPS	Nee	bekabeld
Panasonic WV-SF332 IP Camera	Nee	bekabeld
Polycom CX 5000	Ja	bekabeld
Polycom HDX 8000	Ja	bekabeld

5.3.3.2. Netwerk componenten

In tabel hieronder zijn de resultaten verwerkt van het onderzoek naar inventarisatie van de netwerk componenten. Dit zijn de componenten die gebruikt worden om de aangesloten hardware(tabel in

paragraaf 5.3.3.1) te voorzien van netwerk. Deze resultaten zijn tot stand gekomen door het raadplegen van de interne documentatie. Netwerk componenten die niet gebruikt worden op de access laag van het netwerk, zijn niet meegenomen in de inventarisatie.

Naam	802.1x Ondersteuning	soort
Cisco 2950	ja	switch
Cisco 2960	ja	switch
Cisco 3550	ja	switch
Cisco 3560	ja	switch
Cisco 3560X	ja	switch
Cisco 3560E	ja	switch
Cisco 3560G	ja	switch
Cisco 4404	ja	wireless lan controller
Cisco 5508	ja	wireless lan controller
Cisco 1900	ja	Integrated Services Routers
Cisco 870	ja	Integrated Services Routers
Cisco 3602	ja	wireless access point
Cisco 3502	ja	wireless access point
Cisco 1152	ja	wireless access point
Cisco 1142	ja	wireless access point
Cisco 1231	ja	wireless access point
Cisco 1210	ja	wireless access point

5.3.4. Netwerk functionaliteiten

Naast het inventariseren van de hardware is er ook gekeken naar netwerk functionaliteiten, die mogelijk voor problemen kunnen zorgen bij het implementeren van NAC. De drie functionaliteiten die tijdens het onderzoek naar voren zijn gekomen zijn:

- Preboot Execution Envirenment(PXE);
- Waken-on-Lan(WOL);
- Het voice VLAN.

In de volgende drie paragrafen zal beschreven worden wat deze functionaliteiten doen en waarom het voor problemen kan zorgen.

5.3.4.1. Preboot Execution Environment

Preboot execution environment(PXE) wordt binnen de Hogeschool Utrecht gebruikt om werkstations en laptops te installeren met Windows XP en binnenkort Windows 7. Omdat PXE opstart voordat er een NAC(802.1x) authenticatie plaatsvindt, is het niet mogelijk om de computer te authentiseren voordat PXE gestart wordt. Er moet een oplossing gezocht worden om PXE mogelijk te maken.

5.3.4.2. Wake-on-Lan

Wake-on-Lan is een manier, om computers die uit staan, vanaf afstand op te kunnen starten. Door het sturen van een WOL bericht is het mogelijk om een computer die uit staat aan te zetten. Binnen de Hogeschool Utrecht wordt WOL gebruikt om ’s avonds computers op te starten. Hierdoor kan in de avonduren software geïnstalleerd en updates uitgevoerd worden, zodat gebruikers overdag geen last hebben van wijzigingen op de computer. Net zoals bij PXE kan er nog geen NAC(802.1x) authenticatie plaatsvinden. Dit omdat de computer uitstaat.

5.3.4.3. Voice VLAN

Het voice VLAN wordt gebruikt om de IP telefoons te scheiden van het computerverkeer, zodat gesprekken niet afgeluisterd kunnen worden. Om er voor te zorgen dat er op de access switches niet

te veel netwerk poorten worden gebruikt, kan een computer via de IP telefoon aangesloten worden op het netwerk. Hierdoor is er maar één fysieke netwerk poort nodig voor de computer en IP telefoon. Het probleem hierbij is dat NAC(802.1x) er vanuit gaat dat er maar een apparaat achter de netwerk poort zit aangesloten. Zodra de IP telefoon geauthentiseerd is, krijgt de computer die aan de telefoon is verbonden de zelfde netwerkrechten als de telefoon. En dit wil je juist voorkomen door gebruik te maken van een voice VLAN.

5.4.Gewenste situatie

In dit hoofdstuk wordt de gewenste situatie in kaart gebracht. Dit is gedaan door middel van interviews met de manager infrabeheer, security officer, netwerk- en serverbeheerders en een aantal gebruikers van het netwerk. Daarnaast is er gekeken naar het strategisch ICT-beleid. De gegevens uit de interviews en de punten uit het strategisch ICT-beleid zijn geanalyseerd en verwerkt tot een lijst met eisen en wensen. Daarna zijn de eisen en wensen ingedeeld volgens de MoSCoW methode.

5.4.1. Eisen en wensen

Om de eisen en wensen in kaart te brengen is er als eerst gekeken naar het ICT-beleid van de Hogeschool Utrecht. Het beleid genaamd “Strategisch ICT-beleid HU 2010 – 2015” is geschreven door P. Hillman, CEO van de Hogeschool Utrecht. In het strategisch ICT-beleid van de Hogeschool Utrecht is de ambitie beschreven op het gebied van ICT van de Hogeschool Utrecht. Hierin staat het ICT-beleid op strategisch niveau beschreven. Uit dit ICT-beleid zijn een aantal punten omgezet naar concrete eisen die bij kunnen dragen aan deze beleidspunten die beschreven staan in het “Strategisch ICT-beleid HU 2010 – 2015”. Deze eisen zijn tevens goedgekeurd door de opdracht gever E. de Vries en de geïnterviewde. De eisen die gevormd zijn van uit het beleid zijn:

- **Hergebruiken van componenten**
  In het strategisch ICT-beleid van de Hogeschool Utrecht is opgenomen dat er gewerkt wordt met standaard bouwstenen en hergebruiken van componenten. Hiermee wordt bedoeld dat de componenten, die al gebruikt worden zo veel mogelijk hergebruikt worden. Voordat er overgegaan wordt tot aanschaf van nieuw componenten. Een eis is dan ook om zo veel mogelijk componenten te hergebruiken. Wanneer componenten te oud zijn of niet slecht functioneren kan er gekeken worden naar een andere oplossing.
- **Open standaard of marktconform geaccepteerde standaarden**
  In het strategisch ICT-beleid van de Hogeschool Utrecht is opgenomen dat er gewerkt wordt met open standaarden en/of marktconform geaccepteerde standaarden. Dit beleid is opgesteld om de interoperabiliteit tussen systemen te bevorderen.
- **Detecteren van misbruik en malware**
  Omdat het netwerk van de Hogeschool Utrecht voor het grootste deel gebruikt wordt door studenten, bestaat de kans dat computers van studenten malware met zich meedragen. Daarbij komt het feit dat er een toename is van malware (G-Data, 2011). Een eis is dan ook om misbruik en malware op tijd te kunnen detecteren.
- **Dataverkeer Herleiden naar natuurlijk persoon**
  Er komen incidenten voor waarbij de vraag is door wie en van welk apparaat het dataverkeer afkomstig is. Dit kan gaan van misbruik op het netwerk tot het opsporen van problemen. In de huidige situatie is dit op het bekabeld netwerk niet mogelijk en op het draadloos netwerk beperkt mogelijk. Hierdoor is er een wens om dataverkeer te kunnen herleiden naar een natuurlijk persoon. Tevens is dit een eis van onze internet provider SURFnet.

Naast de eisen die zijn voortgekomen uit de strategisch ICT-beleid stukken, zijn er ook eisen en wensen naar voren gekomen tijdens de interviews met de manager infrabeheer, security officer, netwerk- en serverbeheerders en een aantal gebruikers van het netwerk. De eisen en wensen die voorgekomen zijn uit deze interviews zijn vergeleken met de strategisch ICT-beleid stukken. In de vergelijking is er gekeken of er eisen en wensen in strijd zijn met de strategisch ICT-beleid stukken en zijn waar nodig aangepast. De eisen en wensen die uit de interviews naar voren zijn gekomen zijn:

- **Quarantaine**
  Wanneer een computer malware bevat of een gebruiker misbruik maakt van het netwerk moet een gebruiker geïsoleerd kunnen worden. Daarom moet er een quarantainenetwerk komen die verspreiding voorkomt. De wens is om quarantaine in eerste instantie handmatig te vullen, dit om false positives meldingen te voorkomen. Wanneer er meer zekerheid en stabiliteit is moet het wel mogelijk zijn om dit proces te automatiseren.
- **Dynamisch VLAN toewijzen**
  Om het beheer makkelijker te maken, maar ook om menselijke fouten te voorkomen is er de wens om het dynamisch toewijzen van VLANS groot. Daarnaast hoeven er geen VLAN wijzigingen meer aangevraagd worden, wat de oplostijd van meldingen ten goede komt. Ook wordt de kans verkleind dat apparatuur in het verkeerde VLAN terecht komt, wat de beveiliging van het netwerk ten goede komt.
- **Cliënt-less authenticatie en autorisatie**
  Het grootste deel van de gebruiker die gebruik maken van het netwerk zijn studenten. Omdat studenten allemaal hun eigen laptop of apparaat meenemen, is het moeilijk te eisen dat gebruikers software gaan installeren voordat ze op het netwerk kunnen. Dit is gebleken uit eerdere ervaringen met de SecureW2 client. Voor computers die in beheer zijn van de Hogeschool Utrecht kan dit well een optie zijn, alleen wanneer dit een meerwaarde biedt. Het is dan ook een eis dat de NAC-oplossing cliënt-less werkt, hiermee wordt bedoelt dat er geen extra software geïnstalleerd hoeft te worden door de gebruiker.
- **Single point of failure**
  Wanneer NAC wordt geïmplementeerd moet iedereen zich eerst authentiseren, voordat er gebruik kan worden gemaakt van het netwerk. Wanneer een NAC systeem niet zou werken kan niemand zich authentiseren en dus geen toegang kunnen krijgen tot het netwerk De gevolgen die dit heeft voor de bedrijfsvoering zullen niet te overzien zijn. Daarom is het een must dat de NAC-oplossing geen single point of failure is.
- **Bekabeld en draadloos netwerk één NAC-oplossing**
  Om het beheer te versimpelen moet er voor het bekabeld en draadloos netwerk één oplossing komen. Meerder oplossingen zullen uiteindelijk leiden tot meer beheer en het maakt het oplossen van problemen ingewikkeld.
- **Schaalbaar**
  Omdat het netwerk explosief is gegroeid in het afgelopen jaar van gemiddeld 3000 actieve draadloze sessie naar 6000, moet het NAC systeem ook mee kunnen schalen met dit soort explosieve toenamen in netwerk gebruikers.
- **Rekening houden met de EU aanbesteding**
  Dit jaar zal het netwerk van de Hogeschool Utrecht Europees aanbesteed worden. Om er voor te zorgen dat de NAC-oplossing ook toepasbaar is na de EU aanbesteding, zullen de resultaten, van het ondezoek naar NAC, meegenomen worden in het EU aanbestedingstraject.
- **Gast netwerk**
  Vanuit de faculteit en de gebruikers is een wens om gasten toegang te bieden tot het netwerk

van de Hogeschool Utrecht. Echter is uit gesprekken naar voren gekomen dat het toelaten van gasten op het netwerk meegenomen wordt in het provisioning project. Het provisioning project gaat er voor zorgt dat netwerkaccounten worden aangemaakt en verwijderd wanneer er een nieuw medewerker in of uit dienst gaat. Dit proces zal tevens ingericht worden voor studenten en gasten.

- **NAC op VPN**
  Uit de gesprekken met de manager van afdeling infrabeheer en de security office is er naar voren gekomen dat er geen specifieke wens is voor het toepassen van dynamisch VLAN op het VPN netwerk. Echter is er wel een wens om te kijken of het in de toekomst wel mogelijk is om het VPN netwerk te koppelen aan het NAC systeem voor malware en misbruik te detectie.

5.4.2. MoSCoW

De eisen en wensen die zijn voortgekomen uit het strategisch ICT-beleid en de interviews, zijn hieronder aan de hand van hun prioriteit ingedeeld volgens het MoSCoW-indelingsprincipe.

Must Have
De eisen die hier genoemd worden moeten in het eindresultaat terugkomen

- Quarantaine;
- Detecteren van misbruik en malware;
- Dataverkeer Herleiden naar natuurlijk persoon ;
- Rekening houden met de EU aanbesteding;
- Geen single point of failure;
- Dynamisch VLAN toewijzen;
- Hergebruiken van componenten;
- Cliënt-less authenticatie en autorisatie;
- Schaalbaar;
- Bekabeld en draadloos netwerk één NAC-oplossing.

Should Have
De eisen die hier genoemd worden zijn zeer gewenst, maar een vergelijkbare eigenschap is ook goed genoeg.

- Open standaard of marktconform geaccepteerde standaarden.

Could Have
De eisen die hier genoemd worden mogen alleen aan bod komen als er tijd genoeg is.

- NAC op VPN.

Won’t Have
De eisen die hier genoemd worden zullen in het eindresultaat niet aan bod komen maar kunnen in de toekomst, bij een vervolgproject, interessant zijn.

- Gast netwerk.

6. Ontwerp

6.1.Inleiding

In dit hoofdstuk wordt het nieuwe NAC-ontwerp beschreven. Allereerst wordt beschreven welke keuzes er zijn gemaakt voor het nieuwe NAC-ontwerp. Aan de hand van deze keuzes zal het functioneel ontwerp beschreven worden. Daarna zal het technisch ontwerp aan bod komen en wordt er gekeken naar de kosten van het nieuwe NAC-ontwerp.

6.2.Ontwerpkeuze

In de voorgaande hoofdstukken is beschreven hoe de Hogeschool Utrecht ervoor staat, ten aanzien van NAC. Uit het onderzoek naar de huidige situatie, kan geconcludeerd worden, dat op het bekabeld netwerk van de Hogeschool Utrecht nog geen toegangscontrole wordt toegepast. Iedereen kan zijn laptop of apparatuur, met netwerk aansluiting, koppelen aan het netwerk van de Hogeschool Utrecht. Dit kan allemaal zonder dat de gebruiker zich hoeft te authentiseren. Op het draadloos netwerk van de Hogeschool Utrecht wordt al wel gebruik gemaakt van NAC. Dit wordt gedaan met het 802.1x protocol. Daarnaast wordt er een quarantainenetwerk gebruikt. Dit om apparatuur, die besmet is met malware of gebruikers die misbruik maken van het netwerk, de toegang tot het netwerk te ontzeggen. Dit kan ook gezien worden als een niveau 2 implementatie van NAC.

Voor het realiseren van NAC op het gewenste niveau zijn er verschillende leveranciers. Die totaaloplossingen bieden om access control toe te kunnen passen op het netwerk. De grootste spelers in Nederland, op het gebied van NAC, zijn Cisco en Juniper (Gartner, 2011). Beide leveren uitgebreide NAC-oplossingen met functionaliteiten, die voldoen aan de eisen en wensen van de Hogeschool Utrecht. Er is echter voor gekozen om geen gebruik te maken van de NAC-oplossingen van Cisco of Juniper.

In het nieuwe ontwerp zal er gebruik worden gemaakt van de componenten die al beschikbaar zijn binnen de Hogeschool Utrecht. De NAC componenten die gebruikt worden voor access control op het draadloos netwerk, kunnen als basis functioneren voor een totaaloplossing voor access control op het bekabeld en draadloos netwerk van de Hogeschool Utrecht. Omdat de huidige situatie op het draadloos netwerk niet het juiste niveau heeft, is gekeken welke componenten er binnen de Hogeschool Utrecht aanwezig zijn om toch tot het gewenste niveau te komen. Daarnaast is er gekeken of deze componenten niet het NAC systeem beperken, zodat eventuele uitbreidingen in de toekomst, niet mogelijk zijn.

Om tot het juiste NAC niveau te komen zal tevens gebruik worden gemaakt van de Palo Alto firewall. De Palo Alto firewall wordt ook wel een “Next generation firewall” genoemd. Dit houdt in dat de firewall de netwerkpakketen inspecteert op inhoud en niet op poortnummer. Tevens is het mogelijk om intrusion detection en inspection toe te passen en het is mogelijk om een gebruikersnaam te gekoppeld aan een IP-adres.

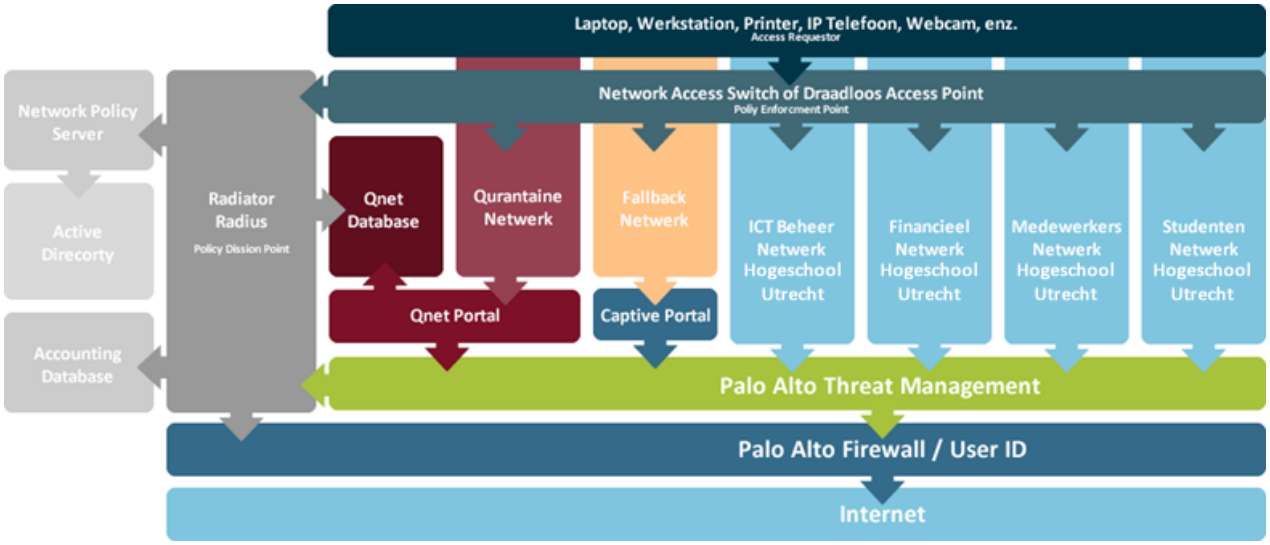
Om NAC toe te passen op de Hogeschool Utrecht zal gebruik worden gemaakt van 802.1x. Dit wordt gedaan, omdat het een bewezen en openstandaard is. Daarnaast wordt dit protocol gebruikt, omdat de huidige componenten alleen 802.1x ondersteunen om NAC toe te kunnen passen.

Natuurlijk is er niet zomaar voor deze oplossing gekozen. Er zijn een aantal belangrijk punten waarom er gekozen is om juist geen gebruik te maken van een NAC-oplossing van Cisco of Juniper.

- Met de huidige componenten is het mogelijk om het zelfde niveau te behalen als met de producten van Juniper of Cisco. Tevens zijn de componenten al in productie, waardoor het implementatietraject korter zal zijn. Dit is tevens een doelstelling uit het beleid.
- In tijden van bezuinigingen moet er goed gekeken worden waar geld aan wordt uitgegeven. In het strategisch ICT-beleid wordt daarom gewezen op het zo efficiënt mogelijk om gaan met aanschaf van de middelen. Het is daarom van belang dat er eerst gekeken wordt of er al middelen aanwezig zijn, voordat er overgegaan wordt tot aanschaf van nieuwe middelen. Een belangrijk punt is dan ook om te kijken of componenten hergebruikt kunnen worden.
- Een ander belangrijk punt is dat het aanschaffen van een NAC-oplossing van Cisco of Juniper ver boven de aanbestedingsgrens van €193.000 zouden uitkomen excl. jaarlijkse support en licentiekosten. Bij Cisco gaat het hier zelfs om bedragen van €300.000 á €350.000. Terwijl bij het hergebruiken van componenten de kosten ver onder de aanbestedingengrens blijven van €193.000. Hierdoor hoeft het NAC-ontwerp niet aanbesteed te worden, waardoor een keuzevrijheid is om de componenten te selecteren.
- Het laatste punt waarom er gekozen is om geen gebruik te maken van de Cisco of Juniper oplossingen, is omdat de componenten die hergebruikt worden als in productie zijn. Hierdoor hoeven alleen de juiste koppelingen gemaakt worden. Dit zal de tijd van de implementatie van NAC verkorten.

6.3.Functioneel ontwerp

In de voorgaande hoofdstukken is beschreven welke globale keuzen er zijn gemaakt en waarom deze keuzes zijn genomen. In dit hoofdstuk zal beschreven worden hoe het nieuwe functioneel ontwerp voor NAC er uit komt te zien, aan de hand van de keuzes die zijn gemaakt. Op afbeelding 7 is te zien hoe het functioneel ontwerp er schematisch uitziet. Aan de hand van afbeelding 7 zal beschreven worden welke functionaliteiten het nieuwe ontwerp biedt. Verder laat het zien hoe deze functies gebruikt worden. Daarnaast zal beschreven worden op welke wijze de toegang tot het netwerk gegeven/verkregen wordt. Het ontwerp op afbeelding 7 is voor zowel het bekabeld als draadloos netwerk van de Hogeschool Utrecht en er zit geen verschil in functionaliteit. Het ontwerp zal in de volgende paragrafen beschreven worden en is voor zowel het bekabeld als draadloos netwerk.



afbeelding 7: Functioneel ontwerp

6.3.1. Client-less authentiseren

In het ontwerp is er rekening mee gehouden, dat het authenticatieproces zo gebruiksvriendelijk moet zijn. Daarom is er voor gezorgd dat gebruikers geen extra client software hoeven te installeren, voordat de gebruikers, gebruik kunnen maken van het netwerk. De besturingssystemen die tegenwoordig gebruikt worden, zoals Max OS x, Windows XP, Windows Vista, Windows 7, Ubuntu, Fedora, openSuse leveren standaard ondersteuning voor 802.1x. Hierbij wordt er vanuit gegaan dat de besturingssystemen up-to-date zijn. Echter 802.1x zal eenmalig moeten worden ingesteld, voordat er gebruik kan worden gemaakt van het netwerk

Voor werkstations en laptops, die in het beheer zijn van de Hogeschool Utrecht, zal deze instelling standaard meegenomen worden in het installatieproces. Voor de werkstations en laptops, die al voorzien zijn van een installatie, zullen de instellingen aangepast worden via een Active Directory Policy. De overige computers die niet in het beheer zijn van de Hogeschool Utrecht zullen deze instellingen zelf moeten aanpassen.

802.1x wordt gezien als client-less, omdat de functionaliteit van 802.1x in iedere besturingssysteem is geïmplementeerd. Echter om volledig client-less authenticatie mogelijk te maken, wordt gebruik gemaakt van een captive portal. Via deze captive portal kan, via een inlogformulier, toegang verkregen worden tot het netwerk. De werking van de captive portal wordt in paragraaf 6.3.6 beschreven.

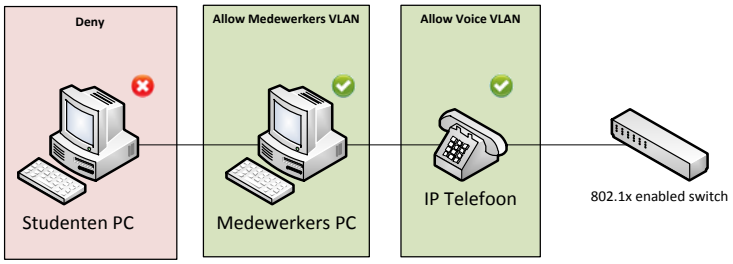
6.3.2. MAC Authentication bypass

Voor de apparatuur die geen ondersteuning bieden voor 802.1x, zal er gebruik worden gemaakt van de functie MAC authentication bypass(MAB). Het betreft apparatuur zoals: IP camera's, faxen, gebouwbeheer systemen en het grootste deel van de IP telefoons. Deze functie is alleen beschikbaar voor het bekabeld netwerk. Dit komt omdat de apparatuur die geen ondersteuning bieden voor 802.1x, allemaal gebruik maken van een bekabeld netwerkaansluiting. Tevens moet erbij vermeld worden dat MAB een naam is die Cisco gebruikt. Juniper, HP, Brocade, enz. bieden dezelfde functionaliteit, alleen onder een andere naam.

MAB zorgt ervoor dat een apparaat, die geen ondersteuning biedt voor 802.1x, geauthentiseerd wordt aan de hand van het MAC-adres van het apparaat. Hierbij zal de switch, de policy enforcement point(PEP), ook functioneren als access requester(AR). De switch zal in dit geval het MAC-adres als gebruikersnaam en wachtwoord als 802.1x authenticatieverzoek versturen aan de policy decision point(PDP). Zo is het mogelijk om apparatuur, die geen ondersteuning biedt voor 802.1x, wel te authentiseren aan de hand van het MAC-adres.

6.3.3. Multi-Domain authenticatie

Om ervoor te zorgen dat er twee verschilden apparaten geauthentiseerd kunnen worden op één netwerkpoort, wordt er gebruik gemaakt van Multi-Domain authenticatie(MDA). MDA is een mechanisme dat ervoor zorgt, dat zowel een IP telefoon als een computer of ander apparaat geauthentiseerd wordt op één netwerkpoort. De IP telefoon zal in het voice VLAN worden geplaatst en het apparaat, dat aangesloten zit aan de IP telefoon, zal geplaatst worden in het netwerk waar hij geautoriseerd voor is. Het zal dus niet mogelijk zijn om meerdere apparaten te koppelen aan een IP telefoon.



afbeelding 8: Multi-Domain authenticatie

6.3.4. Role based netwerken

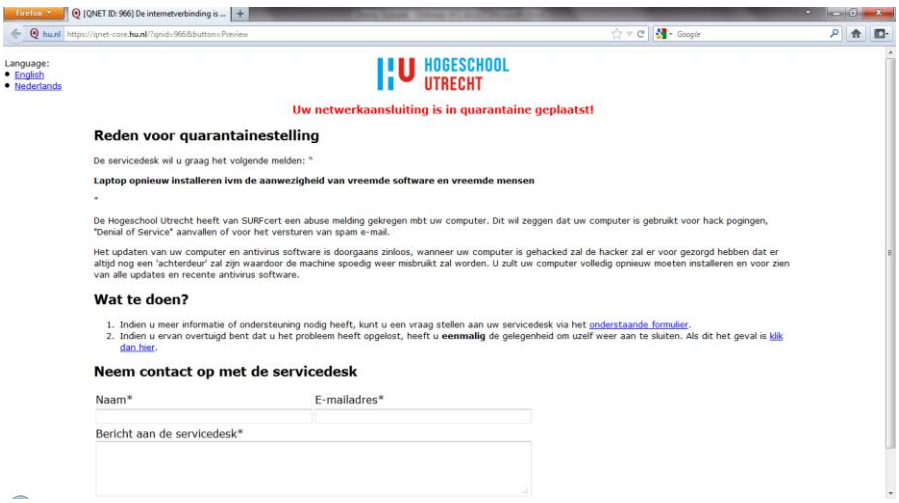
Het ontwerp kent verschillende soorten netwerken. In het ontwerp is er een verdeling gemaakt in vier verschillende productie netwerken. Dit zijn de ICT-beheer, financieel, medewerkers en studenten netwerken. Aan de hand van de rol, die een gebruiker heeft binnen de Hogeschool Utrecht, wordt bepaald in welk netwerk de gebruiker wordt geplaatst. Wanneer er in de toekomst een specifiekere rolverdeling gewenst is, kan dit op ieder moment worden aangepast. Naast de vier productie netwerk zijn er nog twee netwerken. De eerste is het quarantainenetwerk en de tweede is het fallbacknetwerk. Deze zullen in de volgende paragraven beschreven worden.

6.3.5. Quarantaine netwerk

Apparaten die besmet zijn met malware of gebruikers die misbruik van het netwerk maken, worden in eerste instantie handmatig in quarantaine geplaatst, dit om false positive meldingen te voorkomen. Wanneer er meer zekerheid en stabiliteit is kan dit proces te geautomatiseerd worden.

In het nieuwe NAC-ontwerp zal de quarantaine omgeving van het draadloos netwerk hergebruikt worden en ingezet worden voor zowel het draadloos als bekabeld netwerk. Het doel van het quarantainenetwerk is het tegengaan van het verspreiden van malware. Tevens moet het quarantainenetwerk er voor zorgen, dat gebruikers die misbruik maken van het netwerk geen schade meer aan kunnen richten.

Het quarantainenetwerk bestaat uit drie onderdelen. Het eerste onderdeel is het netwerk zelf. Dit netwerk is een apart netwerksegment, waarbij het verkeer afgescheiden wordt van de rest van het netwerk. Het tweede onderdeel is de quarantaineportal. Wanneer gebruikers, waarvan het apparaat in quarantaine staat, een internet pagina bezoeken, zal de gebruiker doorgestuurd worden naar de quarantaineportal. Op deze portal krijgt de gebruiker te zien waarom hij of zij in quarantaine is gezet. Een voorbeeld van de quarantaineportal is te zien op afbeelding 9.



afbeelding 9: Quarantaine portal

Het laatste onderdeel van het quarantainenetwerk is de database. In deze database staan alle gebruikersnamen, IP-adressen en de MAC-adressen van de gebruikers die in quarantaine geplaatst zijn. Voordat een gebruiker toegang krijgt tot het netwerk, zal de PDP eerst kijken of de gebruikersnaam of MAC-adres in de quarantaine database staat. Als dit het geval is zal de PDP het verzoek naar de PEP sturen om het apparaat in quarantaine te plaatsen.

6.3.6. Fallbacknetwerk

Het quarantainenetwerk en de vier productie netwerken die hierboven beschreven zijn, worden gebruikt voor zowel het bekabeld als draadloos netwerk van de Hogeschool Utrecht. Het laatste netwerk in het ontwerp is het fallbacknetwerk. Het fallbacknetwerk zal echter alleen toegepast worden op het bekabeld netwerk, omdat anders het draadloos netwerk onbeveiligd is. Waardoor iedereen gebruik kan maken van het draadloos netwerk, zonder te authentiseren. Het fallbacknetwerk zal gebruikt worden als de authenticatie mislukt of wanneer 802.1x nog niet is ingesteld op het apparaat.

Wanneer een apparaat in het fallbacknetwerk is terecht gekomen of wanneer geen gebruik kan worden gemaakt van 802,1x, zal de gebruiker eerst moeten inloggen op de captive portal voordat er gebruik kan worden gemaakt van het netwerk. De captive portal is een techniek waarmee een gebruiker zich kan authentiseren via een webpagina. Wanneer een gebruiker zijn webbrowser opent en wil verbinden met een webpagina, zal al het verkeer onderschept worden door de captive portal. De gebruiker krijgt dan een pagina te zien, waar hij kan inloggen met zijn gebruikersnaam en wachtwoord. Een voorbeeld van deze captive portal is te zien op afbeelding 10.

afbeelding 10: Captive portal

Op de captive portal worden tevens handleidingen geplaats. In de handleidingen wordt uitgelegd hoe je 802.1x kan instellen op de diverse besturingssystemen. Wanneer hier geen gebruik van wordt gemaakt, bestaat de mogelijkheid om in te loggen via het inlogformulier op de captive portal. De functionaliteiten zullen echter beperkt worden. Dit wordt gedaan om het gebruik van 802.1x te bevorderen. Het nadeel van de capive portel is dat deze techniek geen ondersteuning biedt voor dynamich VLAN. Dit houdt in dat de PEP niet kan bepalen tot welk netwerk het apparaat of de gebruiker behoort.

Naast de functionaliteiten die hierboven zijn beschreven, zal het fallbacknetwerk ook gebruikt worden om computers te installeren. Omdat ieder apparaat standaard terecht komt in het fallbacknetwerk, na een time-out en zich niet eerst hoeft te authentiseren, kan er toch gebruik worden gemaakt van PXE.

Dit is ook de beste manier om PXE en 802.1x samen toe te passen, zonder dat er wijzigingen hoeven plaats te vinden op de netwerkswitch.

6.3.7. Radiator radius

Een belangrijk onderdeel van het nieuwe NAC-ontwerp is de Radiator radiusserver. Dit is de plek waar alle beslissingen worden genomen. Dit punt wordt ook wel het policy dessicion point(PDP) genoemd.

De radiusserver is als eerst verantwoordelijk voor het authentiseren van de 802.1x authenticatie verzoek dat de radiusserver ontvangt van het policy enforcement point(PEP). Dit doet de radiusserver door het authenticatie verzoek door te sturen naar de network policy server(NPS). Aan de hand van het antwoord zal de radiusserver een access-accept of access-deny terug sturen naar het PEP. Daarnaast zal de radiusserver aangeven in welk netwerk het apparaat gezet moet worden.

Wanneer er een verzoek binnen komt via het MAB mechanisme, zal de radiusserver het apparaat authentiseren aan de hand van een lokale database. Als het MAC-adres van dit apparaat niet bekend is, zal er een access-deny terug worden gestuurd. Voordat er een antwoord wordt terug gestuurd, zal er nog gekeken worden of het apparaat in quarantaine gezet moet worden. De radiusserver zal in de quarantaine database kijken of het MAC-adres bekend is. Als dit het geval is zal de radiusserver het quarantainenetwerk ID meegeven in het antwoord op het authenticatie verzoek.

Nadat het apparaat geauthentiseerd is via 802.1x of MAB, zal een accounting verzoek gestuurd worden door het apparaat dat het authenticatie verzoek heeft gedaan. Dit accountingproces is onderdeel van het 802.1x protocol. Aan de hand van dit accounting verzoek zullen er een tweetal acties worden uitgevoerd. Ten eerste zal het accounting verzoek worden opgeslagen in een accounting database. Hierdoor kan achteraf gekeken worden wie en wat er allemaal toegang heeft gekregen tot het netwerk. Daarna wordt een verzoek gestuurd naar de Palo Alto Firewall User-ID Engine om de gebruikersnaam en het IP-adres te koppelen. Later in dit hoofdstuk zal uitgelegd worden wat de Palo Alto Firewall User-ID engine precies doet.

6.3.8. Network policy server

De netwerk policy server(NPS), is het de nieuwe radiusserver van Microsoft. De NPS is de vervanger van de oude IAS. In het nieuwe ontwerp is ervoor gekozen om de oude IAS te vervangen door de nieuwe NPS. Dit is niet gedaan omdat de NPS meer functies heeft, maar omdat de support op Windows server 2003, waar IAS een onderdeel van is, op korte termijn niet meer ondersteund zal worden door Microsoft. NPS is in het nieuwe ontwerp verantwoordelijk voor de communicatie met Active Directory. Dit is gedaan omdat de Radiator radiusserver niet direct kan communiceren met Active Directory. Daarnaast wordt NPS niet direct gekoppeld met het PEP. Dit omdat NPS geen ondersteuning biedt voor zelfgemaakte functies, die wel nodig zijn om te kunnen communiceren met de database van Qnet en de Palo Alto firewall user-ID engine.

6.3.9. Accounting database

In een eerdere paragraaf is er al beschreven dat de accounting database gebruikt wordt om accountingpakketten op te slaan. Zodat er op een later tijdstip gekeken kan worden, wie er allemaal heeft ingelogd op het netwerk van de Hogeschool Utrecht. In het nieuwe ontwerp zal deze database gebruikt worden voor zowel het bekabeld als draadloos netwerk van de Hogeschool Utrecht.

6.3.10. Palo Alto thread management

Een van de belangrijkste wijziging in het nieuwe ontwerp, is het gebruik van een intrusion prevention system(IPS). In het ontwerp wordt gebruik gemaakt van de Palo Alto firewall, die reeds in het bezit is van de Hogeschool Utrecht. Echter de thead prevention module wordt nog niet gebruikt. Deze firewall

kan dus naast het tegenhouden van verkeer ook het verkeer inspecteren op malware, kwetsbaarheden en kan misbruik herkennen.

De Palo Alto firewall is een “Next-Generation Firewall” dit houdt in de firewall niet alleen het verkeer controleert op souce ip/poortnummer en destination ip/poortnummer, maar ook op applicatie niveau. Hierdoor kan de firewall precies zien welke applicatie er gebruikt wordt, ongeacht het poort nummer. Zo kan de firewall ook onderscheid maken in bijvoorbeeld facebook-browsing of facebook-posting. Doordat de firewall het netwerk al inspecteert kan er ook gelijktijdig geïnspecteerd worden op malware, vunrebilitys en spyware.

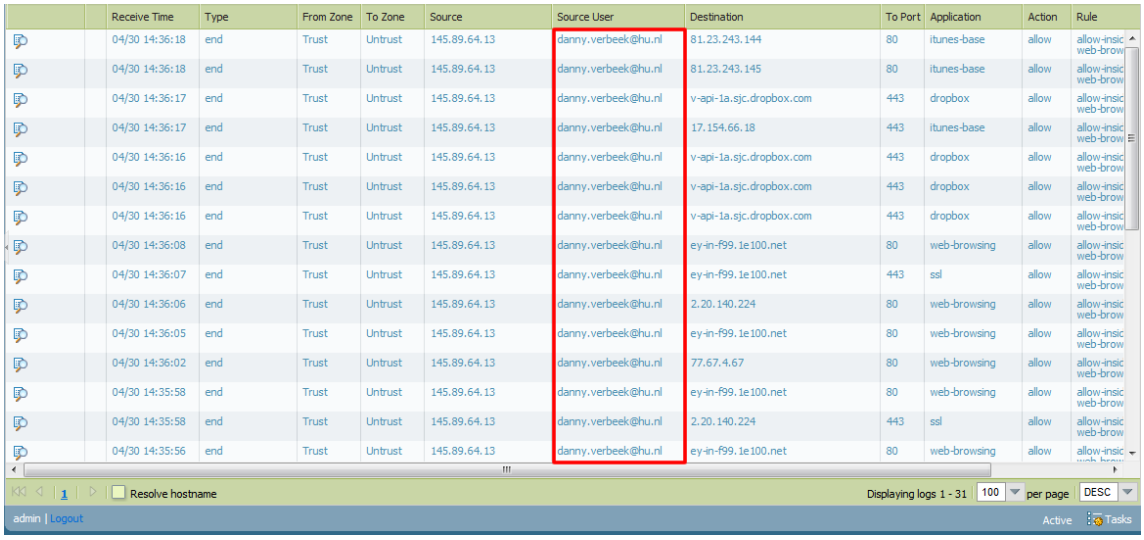
In het ontwerp wordt de Palo Alto firewall gebruikt om ongewenst verkeer van gebruikers direct te blokkeren. Naast het blokkeren van malware, vunrebilitys en spyware zal de Palo Alto thread management module ook een melding doorgeven aan de PDP, die op zijn beurt de gegevens doorgeeft aan de quarantaine database. Dit wordt gedaan om te zorgen dat de gebruikers, die een virus of malware op hun computers hebben ook in het quarantaine wordt geplaatst. In het ontwerp is er rekening mee gehouden dat er een handmatige bewerking moet plaatsvinden voordat een gebruiker in quarantaine wordt geplaatst. Dit wordt gedaan om ervoor te zorgen dat gebruikers niet door foutieve meldingen in quarantaine worden geplaatst. In de toekomst kan dit geautomatiseerd worden.

6.3.11. Palo Alto User-ID Engine

Een andere belangrijke functie die de Palo Alto firewall in het nieuw ontwerp zal krijgen, is het koppelen van de gebruikersnaam aan een IP-adres. Hierdoor kan al het verkeer, dat door de firewall heen gaat, herleid worden naar een natuurlijk persoon.

In de Palo Alto firewall, kan door deze koppeling, gekeken worden welke gebruiker verantwoordelijk is voor welk verkeer dat door de Palo Alto firewall heen gaat. Daarnaast kunnen er ook firewall rules worden aangemaakt op basis van gebruikersnaam.

Aan de manier van inloggen op het netwerk wordt bepaald of de gebruikers of apparaat naam wordt weergegeven in de Palo Alto firewall. Als MAB gebruikt wordt zal het MAC-adres worden weergegeven als gebruikersnaam. En bij een computer, die ingelogd is met het computeraccount van Active Directory, is dit de computernaam. Op afbeelding 11 is een voorbeeld gegeven van een gebruiker die met zijn gebruikersnaam en wachtwoord, via 802.1x is ingelogd op het netwerk.



afbeelding 11: Palo Alto User-ID

6.3.12. Toegangscontrole proces

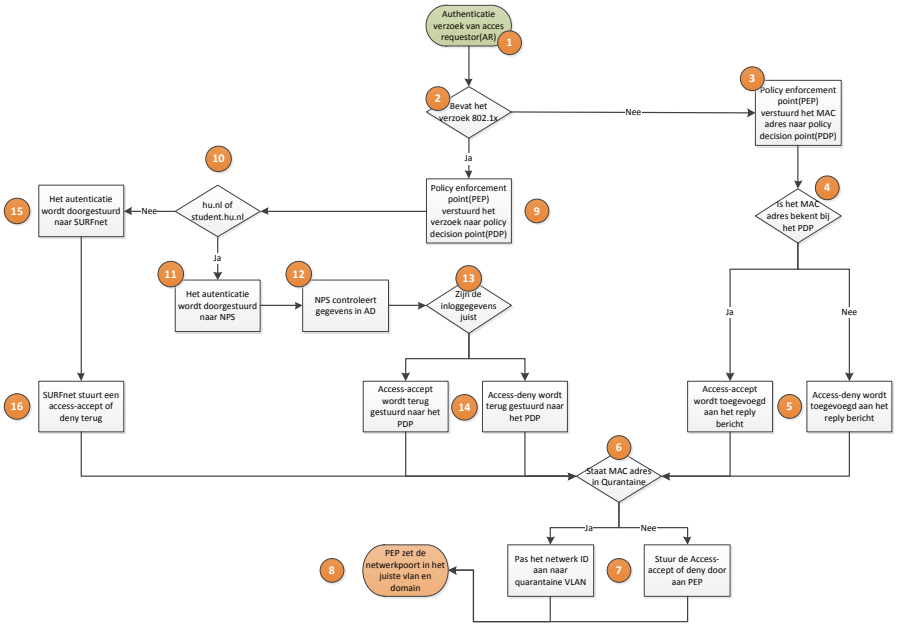
In de voorgaande hoofdstukken is beschreven welke functies het nieuwe ontwerp moet kunnen, wat ze doen en hoe ze werken. In deze paragraaf zal beschreven worden hoe een gebruiker of apparaat toegang krijgt tot het netwerk. Hierbij wordt tevens beschreven hoe de functionaliteiten samen werken en in welke volgorde deze functies worden gebruikt. Aan de hand van afbeelding 12(een grote weergave van afbeelding 12 is te vinden in bijlage 4) zal het proces om toegang te krijgen tot het netwerk van de Hogeschool Utrecht beschreven worden.

De eerste stap in het proces(1), om toegang te krijgen tot het netwerk, is dat de access requester(AR) De AR doet een verzoek om toegang te krijgen tot het netwerk. De AR kan verschillen van laptop tot IP webcam. Het maakt ook niet uit of het verzoek gedaan wordt vanaf het bekabeld of draadloos netwerk. In het authenticatie verzoek wordt gekeken of er geautoriseerd wordt met 802.1x (2). Wanneer het authenticatie verzoek geen 802.1x bevat zal het MAC-adres, die op de netwerkpoort van de access switch geregistreerd staat, doorgestuurd worden naar het policy desicion point(3). In het nieuwe ontwerp is de primaire policy desicion point(PDP) de Radiator radiusserver.

De MAC-adressen die op de poorten van de access switches geregistreerd staan, zullen alleen op het bekabeld netwerk worden doorgestuurd. Dit komt omdat er op het draadloos netwerk alleen 802.1x verzoeken worden toegestaan. Het PDP controleert in de lokale database of het MAC-adres bekend is(4). Wanneer dit het geval is, zal de PDP een access-accept en een VLAN-ID toevoegen aan het reply bericht naar het policy enforcement point (5). Wanneer het een MAC-adres van een IP telefoon is, zal tevens een variabel meegestuurd worden waaraan de PEP kan herkennen dat het om een IP telefoon gaat. Hierdoor wordt de IP telefoon in het voice VLAN geplaatst. Wanneer het MAC-adres niet bekend is, wordt er een access-deny toegevoegd aan het reply bericht die aan het PEP wordt gestuurd.

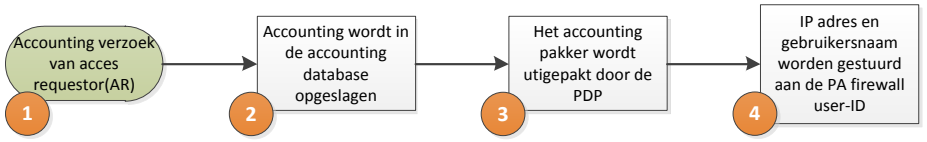
Wanneer het authenticatie verzoek wel 802.1x bevat, zal het verzoek doorgestuurd worden naar het Radiator radiusserver (9). Het PDP controller of het authenticatie verzoek hu.nl of student.hu.nl als realm bevat(10). Wanneer dit het geval is wordt het authenticatie verzoek doorgestuurd naar de network policy server(11). Anders wordt het authenticatie verzoek doorgestuurd en afgehandeld door SURFnet. SURFnet zal vervolgens en access-accept of deny terugsturen als reply bericht(15 en 16). Wanneer de network policy server(NPS) het authenticatie verzoek ontvangt, zal de NPS in Active Directory(AD) controleren of de juiste gebruikersnaam en wachtwoord zijn in gevuld(13). Tevens wordt er een VLAN ID aan de gebruiker gekoppeld. Dit doet de NPS aan de hand van de groep waarvan de gebruiker lid is. De NPS stuurt aan de hand van het resultaat een access-accept of deny plus VLAN-ID terug naar het PDP(14)

Voordat alle authenticatie verzoeken terug worden gestuurd naar de PEP, wordt er gekeken of het MAC-adres, van de AR, bekend is in de quarantaine database(6). Als het MAC-adres bekend is wordt de VLAN-ID aangepast in het VLAN-ID van het quarantaine netwerk(7). Wanneer het MAC-adres niet bekend is wordt het reply bericht zonder aanpassing teruggestuurd aan het PEP. Wanneer een access-accept terug komt zal het PEP de AR toewijzen aan het VLAN dat in het replay bericht staat. Wanneer er een access-deny terug komt wordt de gebruiker of apparaat niet toegelaten op het draadloos netwerk. Op het bekabeld netwerk wordt de netwerkpoort aangepast in het fallback VLAN.



afbeelding 12: Toegangscontrole Flow

Nadat de AR geauthentiseerd is stuurt de AR een accountingverzoek naar het PDP. Dit accountingsproces wordt weergegeven op afbeelding 13. Wanneer de PDP het accounting verzoek ontvangt, wordt het account verzoek als eerste weggeschreven in de accounting database(2). In de tweede stap wordt het accountingpakket uitgepakt door de PDP(3) en wordt het IP-adres en de gebruikersnaam, waarvan het accountingpakket afkomstig is, doorgestuurd aan de Palo Alto User-ID Engine(4).

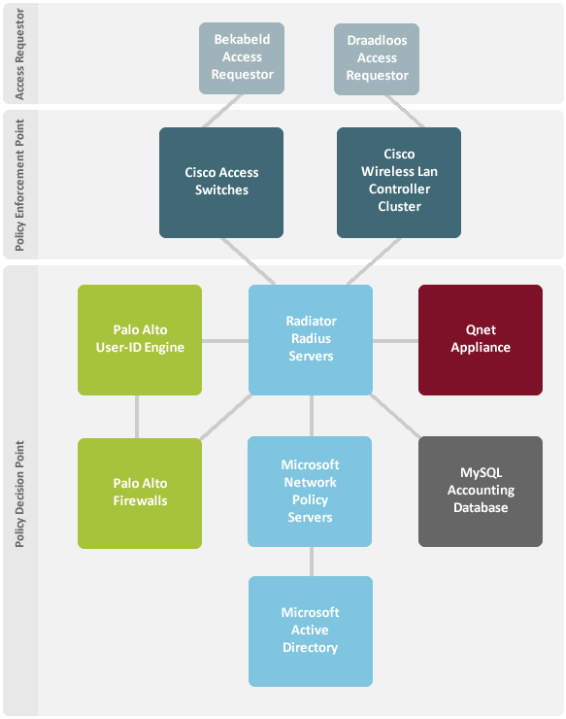


afbeelding 13: Accounting Flow

6.4.Technisch ontwerp

In de voorgaande hoofdstuk is beschreven welke functie het nieuwe ontwerp biedt en welke doelen de functies hebben. In dit hoofdstuk wordt beschreven, hoe deze functionaliteiten technisch worden opgelost. Op afbeelding 14 wordt het technisch ontwerp versimpeld weergegeven. Deze afbeelding zal in de volgende paragrafen gedetailleerder worden beschreven.

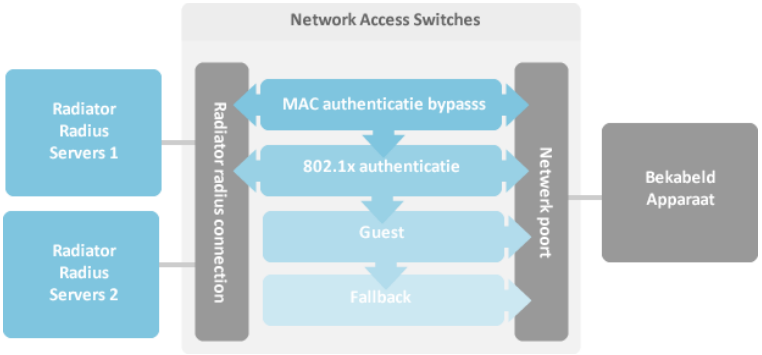
In het technisch ontwerp is er rekening mee gehouden, dat er geen single point of failure mag zijn. Daarom zijn de Radiator radius en de Microsoft Network Policy Servers(NPS) dubbel uitgevoerd. Zowel de radiusserver als de NPS zijn geconfigureerd als een active-active configuratie. Active Directory en de Palo Alto Firewalls zijn ook dubbel uitgevoerd. De Palo Alto User-ID Engine wordt tevens geïnstalleerd op twee verschillende servers, en niet direct op de firewall zelf. De Qnet Appliance en de MySQL database zijn niet dubbel uitgevoerd, dit is gedaan omdat de werking van het authentiseren niet afhankelijk is van deze twee componenten. Wanneer deze componenten zullen uitvallen zal NAC nog steeds werken, Er zal echter dan geen Quarantaine controle en accounting naar de MySQL database plaatsvinden.



afbeelding 14: NAC technisch ontwerp

6.4.1. Network access switches

Als een apparaat verbinding wil maken met het netwerk, zijn er twee mogelijkheden. De eerste mogelijkheid is om het apparaat aan te sluiten op het bekabeld netwerk van de Hogeschool Utrecht. Wanneer een apparaat wordt aangesloten op het bekabeld netwerk, zal het apparaat een verzoek doen om toegang te krijgen tot het bekabeld netwerk. De netwerk access switch zal als eerst proberen te authentiseren met het MAC authenticatie bypass(MAB) mechanisme. Wanneer het MAC-adres niet in de database staat of als de netwerk access switch een 802.1x authenticatie verzoek ontvangt van het bekabeld apparaat, zal geprobeerd worden om het apparaat te authentiseren via het 802.1x mechanisme.



afbeelding 15: Werking netwerk access switch

Op de netwerk access switch is het mogelijk om de volgorde van authentiseren aan te passen. Dit geldt echter alleen voor MAB en 802.1x. De guest en fallback volgorde kunnen niet aangepast worden. Wanneer een apparaat met 802.1x authentiseert zal de 802.1x functionaliteit direct aangeroepen worden, hierdoor hoeft 802.1x niet te wachten op de MAB functionaliteit. Wanneer 802.1x als eerst plaatsvindt moet de MAB functionaliteit wel wachten totdat 802.1x een time-out geeft. Daarom is gekozen om MAB voor 802.1x te laten plaatsvinden.

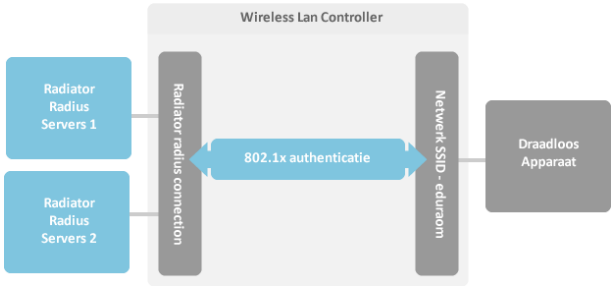
Wanneer een apparaat niet authentiseert of als de authenticatie foutieve gegevens bevat zal de access switch het apparaat in het fallback VLAN zetten. Hiervoor wordt de guest of fallback functionaliteit gebruikt. Voor beide functionaliteiten wordt het apparaat in het fallback VLAN gezet. Er zit wel een verschil in de twee functies. De guest functionaliteit wordt gebruikt wanneer een authenticatie verkeerd gaat. Terwijl de fallback functionaliteit alleen wordt gebruikt, wanneer de radiusservers niet bereikbaar zijn. Hierdoor kunnen we garanderen, dat bij een uitval van beide radiusservers of beide NPS servers, er nog steeds gebruik kan gemaakt worden van het netwerk. Per faculteit is de fallback VLAN anders, op deze wijze wordt er geen groot broadcast domain gecreëerd.

Om een single point of failure te voorkomen, worden de access switches aangesloten op beide radiusserver. Per faculteit wordt de prioriteit van de radiusservers aangepast, om de load over de radiusservers te verdelen.

Een switch verstuurt netwerk verkeer naar de apparaten op basis van MAC-adressen. Hierdoor weet de switch niet welk IP-adres het apparaat heeft, dat is aangesloten op de netwerk switch. Voor het koppelen van een gebruikersnaam aan een IP-adres moet dit wel meegestuurd worden naar de radiusserver. Om toch het IP-adres voor de access switch zichtbaar te maken, zal DHCP snooping geconfigureerd worden op de switches. DHCP snooping zorgt er voor dat de switcht weet welk IP-adres het apparaat heeft gekregen. Om static IP-adressen te blokkeren zal DHCP snooping gebruikt moeten worden in combinatie met dynamic arp inspection(DAI).

6.4.2. Wireless Lan Controller

De tweede mogelijkheid om een apparaat aan het netwerk te koppelen, is via het draadloos netwerk. Het draadloos netwerk is in vergelijking met het bekabeld netwerk minder gecompliceerd ingericht. Dit omdat er op het draadloos netwerk alleen gebruik wordt gemaakt van 802.1x. Het is wel mogelijk om gebruik te maken van andere authenticatie mechanismes, echter deze zijn minder veilig en zijn complexer in beheer. Tevens is het gebruik van 802.1x nodig om gebruik te kunnen maken van eduroam. Wel zullen de verschillende netwerken voor studenten, medewerkers, beheerders en financiële toepassingen, dynamische worden toegewezen. Net zoals bij netwerk access switches wordt de Wireless Lan Controller(WLC) cluster verbonden met beide de radiusservers, wat reeds het geval is in de huidige situatie. Per WLC zal dit op een ander wijze ingesteld worden, dit om de load over de radiusservers te verdelen.



afbeelding 16: Werking Wireless Lan Controller

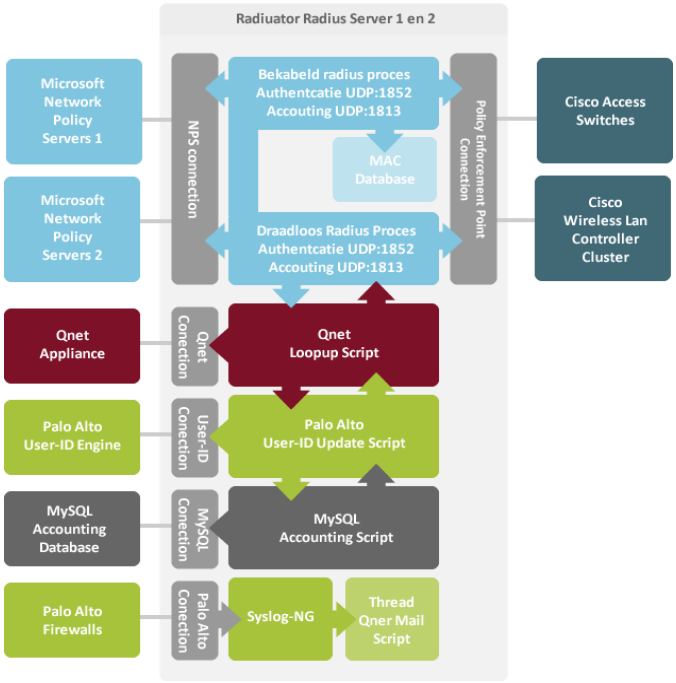
6.4.3. Radiator radiusserver

De Radiator radiusserver is het middelpunt van het nieuwe NAC-ontwerp en kent verschillende processen. Op afbeelding 17 is weergegeven hoe de radiusservers zijn ingericht. Aan de hand van deze afbeelding zal de werking van de radiusserver beschreven worden.

Op afbeelding 17 is niet te zien dat de radiusserver dubbel is uitgevoerd. Dit is in het nieuwe ontwerp wel meegenomen. Eén server zal in het datacenter op de Uithof worden geplaatst. De tweede

radiusserver zal geplaatst worden in het datacenter op de Nijenoord. Beide servers worden geïnstalleerd op de virtuele server omgeving van de Hogeschool Utrecht, in twee verschillende clusters. Beide servers zijn identiek, zo ook de configuraties. Door middel van een r-sync proces zullen de configuratie van beide servers gelijk worden gehouden.

Het eerste proces dat beschreven wordt zijn de radius accounting en authenticatie processen van het bekabeld en draadloos netwerk. Voor zowel het bekabeld als draadloos netwerk wordt er een eigen radiusproces gebruikt. Dit heeft als voordeel dat de load beter verdeeld wordt op de server. Beide processen zijn bijna identiek. Het bekabeld netwerk heeft een extra functie. Op het bekabeld netwerk wordt ook gebruik gemaakt van MAB authenticatie. Daarom is er een extra functie ingebouwd die het authenticatie verzoek van de MAB authenticatie afhandelt. Wanneer er een authenticatie verzoek binnenkomt van een netwerk access switch, zal het radiusproces een query doen in de MAC database. In deze database staan alle MAC-adressen die toegang mogen tot het netwerk. In de database is aangegeven tot welk VLAN het apparaat toegang heeft. Wanneer er een authenticatieverzoek gedaan wordt door een IP telefoon, zal de radiusserver tevens een “Cisco-AV-Pair” terugsturen zodat de switch weet dat hij de IP telefoon in het voice VLAN moet zetten. Deze voice VLAN wordt geconfigureerd op de netwerk switch en wordt niet meegestuurd door de radiusserver.



afbeelding 17: Werking Radiator radius

Zowel het 802.1x authenticatieproces voor het bekabeld als draadloos netwerk is gelijk. Wanneer er een 802.1x authenticatieverzoek binnen komt op één van de radiusprocessen sturen de radius processen het authenticatie verzoek door naar één van de NPS servers. De primaire NPS server is bij de twee radius processen omgedraaid om de load over de twee NPS servers te verdelen.

Wanneer een authenticatie reply terugkomt van de NPS server of wanneer een look-up is gedaan is, in de MAC database, wordt het authenticatie bericht doorgestuurd naar het Qnet lookup script. Dit script controleert of de gebruikersnaam en/of het MAC-adres van het apparaat bekkend is in de database van Qnet. Wanner de gebruiker of apparaat bekend is, wordt het VLAN ID aangepast in het VLAN nummer van het quarantainenetwerk. Het radiusproces zal vervolgens het resultaat terug sturen naad de access switch of de WLC, die op hun beurt de gebruiker of apparaat toelaten of de toegang weigeren tot het netwerk.

Wanneer een apparaat of gebruiker toegang krijgt tot het netwerk, zal er een accountingverzoek worden verstuurd naar de radiusprocessen. Dit accountingverzoek is onderdeel van het 802.1x protocol. Wanneer toegang is gekregen door de MAB-functionaliteit zal de switch het accountingverzoek initiëren en versturen aan het radiusproces. Als het accounting verzoek binnenkomt op één van de radiusprocessen zal het accounting verzoek doorgestuurd worden naar het Palo Alto User-ID script. Dit script is gemaakt om het IP-adres te koppelen aan de gebruikersnaam en om de radiusserver te laten communiceren met de Palo Alto User-ID Engine. Het Palo Alto User-ID script haalt het IP-adres en de gebruikersnaam uit het accountingverzoek en stuurt dit naar de API van de Palo Alto User-ID engine. Als laatst zal het MySQL accounting script aangeroepen worden. Dit script zal alle gegevens uit het accountingverzoek in een MySQL database plaatsen.

Naast de processen en scripts die verantwoordelijk zijn voor de authenticatie en accountingproces, draait er ook nog een syslogproces. Die syslogberichten ontvangt van de Palo Alto thread management module. Het thread Qnet mail script kijkt in de syslogberichten of er een melding binnenkomt met als source adres “145.89.xxx.xxx”. Wanneer dit het geval is, wordt er een email gestuurd aan de Qnet appliance. In de Qnet applicance wordt vervolgens zichtbaar dat er een gebruiker of apparaat is gedetecteerd met malware, virus of vulnerability . De Qnet beheerder kan vervolgens het apparaat, via één knop in quarantaine zetten. Dit proces kan ook geautomatiseerd worden, Echter om false positives te voorkomen wordt het op deze manier opgelost.

6.4.4. Palo Alto User-ID Engine

De Palo Alto User-ID Engine is een stukje software dat geïnstalleerde wordt op beide NPS servers. De User-ID Engine zorgt voor gegevens uitwisseling met de Palo Alto firewall. Het is een opzichzelfstaand onderdeel en is niet geïntegreerd in de Palo Alto firewall.

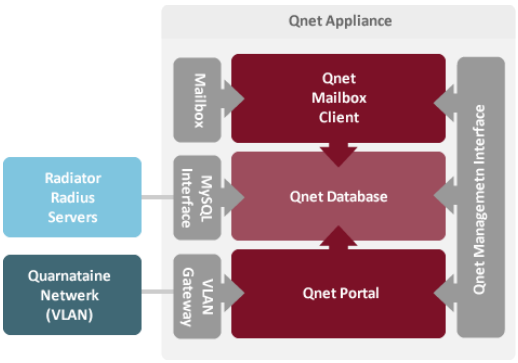
De Palo Alto User-ID Engine kan gebruikersnaam en IP-adressen koppelen en deze zichtbaar maken in de firewall. Hierdoor worden alle sessies getagd met een gebruikersnaam. Zo kan al het verkeer, dat door de firewall heen gaat, herleid worden naar een natuurlijk persoon. Het IP-adres en de gebruikersnaam kunnen op twee verschillende manieren verzameld worden. De Palo Alto User-ID Engine kan de securitylogs uitlezen van Active Directory. Uit deze logs kan de Palo Alto User-ID Engine zien welke gebruiker welk IP-adres heeft gekregen. Een groot nadeel van deze manier, is dat er alleen wordt gekeken wanneer een gebruiker inlogt op een computer van de Hogeschool Utrecht. Hierdoor zijn de gegevens niet betrouwbaar, omdat de gebruikersnaam gekoppeld blijft aan het IP-adres terwijl het niet zeker is of de gebruiker nog ingelogd is.

De tweede manier om deze gegevens te verzamelen, is door gebruik te maken van de Palo Alto API. Deze optie zal gebruikt worden in het nieuwe ontwerp, omdat er in de radiusserver altijd een start, alive en stopbericht binnenkomt, kan er aan de hand van die status geupdate worden naar de Palo Alto firewall. Bij het startbericht zal een verzoek worden gedaan om de gebruikersnaam te koppelen aan het IP-adres en bij een stopbericht zal de gebruikersnaam ontkoppeld worden. Hierdoor kun je er vanuit gaan, dat de gegevens die naar de Palo Alto firewall verstuurd worden, altijd correct zijn.

6.4.5. Qnet Appliance

De Qnet appliance bestaat uit drie processen. Het belangrijkste proces is de Qnet Database. In deze database staan alle gebruikers die in quarantaine gezet worden. Daarnaast staan hier ook alle apparaten en gebruikers in die ooit in quarantaine hebben gestaan. Deze database wordt door de radiusservers geraadpleegd om te kijken of een apparaat of gebruiker in quarantaine gezet moet worden. Naast de database heeft de Qnet ook een mailboxclient. Het is mogelijk om een email te sturen naar de Qnet Appliance. Aan de hand van deze email kunnen gegevens geïmporteerd worden in de Qnet appliance. Natuurlijk kan niet iedereen zomaar een mail sturen. Voordat een email

geaccepteerd wordt, moet het email bekend zijn in de Qnet appliance. Wanneer de Qnet appliance een email ontvangt, zal dit zichtbaar worden in het dashboard van de Qnet appliance. Waarop de beheerder van Qnet actie kan ondernemen. Deze actie kan ook geautomatiseerd worden, maar dit is op dit moment nog niet wenselijk.



afbeelding 18: Werking Qnet

Het laatste onderdeel van de Qnet Appliance is de Qnet Protal. Dit is de webpagina die de gebruikers krijgen te zien als ze in quarantaine zijn gezet. De interface van de portal is tevens de gateway van het quarantaine VLAN.

6.4.6. Network policy server

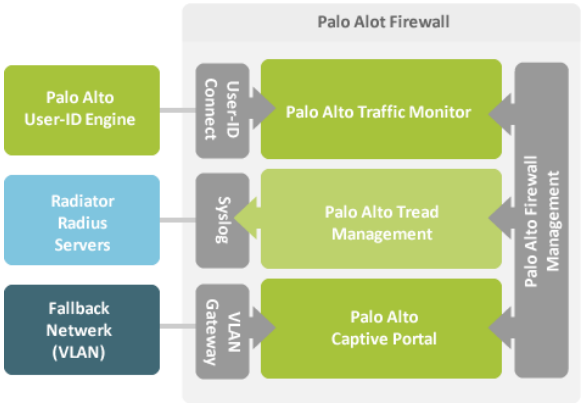
De Netwerk Policy Server(NPS) is verantwoordelijk voor het afhandelen van de authenticatie verzoeken, die de NPS ontvangt van de radiusserver. Aan de hand van policy die gedefinieerd zijn in de NPS wordt er toegang verleend tot het netwerk van de Hogeschool Utrecht. Dit doet NPS door de gegevens te controleren in Active Directory. Aan de hand van een Acitve Directory groep wordt bepaald of iemand toegang krijgt tot het netwerk. Tevens wordt er bepaald tot welk netwerk de gebruiker rechten heeft. In de volgende tabel wordt weergegeven hoe de policys zijn opgebouwd. Het VLAN ID kan verschillen per faculteit. De keuzen voor het VLAN nummer wordt gedaan aan de hand van de naam van het PEP.

Policy naam	Port-Type	AD Groep	VLAN	Action
Wireless 802.1x Access Studenten	Wireless	STD\HvU Studenten	Studenten VLAN ID	Allow
Wireless 802.1x Access Medewerkers	Wireless	MDW\Domain Users	Medewerkers VLAN ID	Allow
Wireless 802.1x Access Beheerders	Wireless	BIS\HU BIS SSC-ICT Netwerkbeheerders	Beheerders VLAN ID	Allow
		BIS\HU BIS SSC-ICT Applicatiebeheerders		
		BIS\HU BIS SSC-ICT Netwerkbeheerders		
Wireless 802.1x Access Administratie	Wireless	MDW\Administratie\Financiële Administratie	Financiële Adm. VLAN ID	Allow
Bekabeld 802.1x Access Studeten	Ethernet	STD\HvU Studenten	Studenten VLAN ID	Allow
Bekabeld 802.1x Access Medewerkers	Ethernet	MDW\Domain Users	Medewerkers VLAN ID	Allow
Bekabeld 802.1x Access Beheerders	Ethernet	BIS\HU BIS SSC-ICT Netwerkbeheerders	Beheerders VLAN ID	Allow
		BIS\HU BIS SSC-ICT Applicatiebeheerders		
		BIS\HU BIS SSC-ICT Netwerkbeheerders		
Bekabeld 802.1x Access Administratie	Ethernet	MDW\Administratie\Financiële Administratie	Financiële Adm. VLAN ID	Allow

Deze policys zijn globaal opgezet en kunnen specifieker worden ingericht. Echter het onderzoeken van de rollen die gebruikers kunnen hebben, valt buiten de scoop van dit onderzoek.

6.4.7. Palo Alto firewall

De Palo Alto firewall is de firewall die gebruikt wordt tussen de internet verbinding met SURFnet en het interne netwerk van de Hogeschool Utrecht. Deze firewall is dubbel uitgevoerd en geconfigureerd als active-passive firewall. Dit houdt in dat er één firewall actief is. Wanneer de primaire firewall niet meer werkt, zal de secundaire firewall de functie van de primaire firewall overnemen.

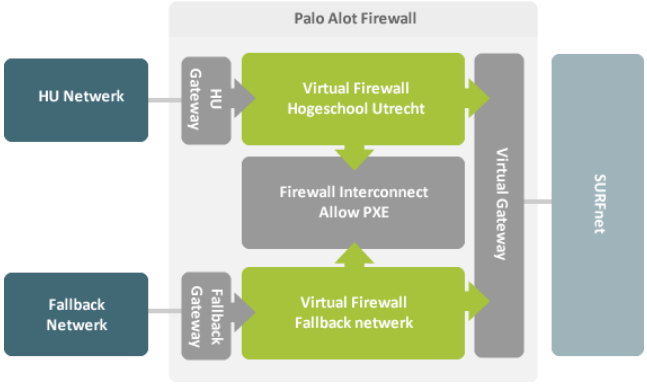


afbeelding 19: Werking Palo Alto firewall

De firewall biedt naast de functie als firewall ook een aantal andere functies. Zo kan de firewall ook ingezet worden als IDS of IPS en kan er gebruik worden gemaakt van een captive protal.

In het nieuwe NAC-ontwerp zal de IDS en IPS functie, die in de Palo Alto firewall “Thread Management” wordt genoemd, gebruikt worden om malware, vulnerability en misbruik te detecteren. Wanneer de thread management malware, vulnerability of misbruik detecteert zal de thread management module een syslog bericht genereren. Deze syslog melding wordt verstuurd naar het syslogproces dat op de radiusserver draait. De werking van dit syslogporces is al beschreven in paragraaf 6.4.3.

Voor de captive portal functie zal er een virtual firewall aangemaakt worden, die de gateway is voor het fallbacknetwerk. Door gebruik te maken van een extra virtual firewall kan het fallbacknetwerk helemaal gescheiden worden van het interne netwerk van de Hogeschool Utrecht. Op afbeelding 20 wordt dit weergegeven. Om PXE toe te staan op het fallbacknetwerk, zal alleen PXE verkeer tussen het fallback en het interne netwerk van de Hogeschool Utrecht toegelaten worden.



afbeelding 20: Werking Palo Alto virtual firewall

Het User-ID script, dat op de radiusserver draait is verantwoordelijk voor het koppelen van de gebruikersnaam en het IP-adres. De Palo Alto firewall is verantwoordelijk voor het koppelen van de gebruikersnaam aan de sessie in de firewall. Dit wordt gedaan in de traffic monitoring module van de firewall. In deze module is the zien welke sessies er verbonden zijn en welke sessies door de firewall zijn doorgelaten of zijn geblokkeerd. Wanneer de Palo Alto User-ID engine een accountingverzoek ontvangt van de radiusserver, zal de Palo Alto User-ID engine de gebruikersnaam koppelen aan de sessie. Dit wordt gedaan op basis van het IP-adres. Hierdoor is het zichtbaar welke gebruiker er bij welke sessie hoort in de firewall.

6.4.8. MySQL Accounting Database

De MySQL database is het laatste component in het nieuwe NAC-ontwerp. De MySQL database server wordt niet dubbel uitgevoerd. Dit is gedaan omdat de MySQL database niet een single point of failure is. Wanneer de database server niet bereikbaar is, heeft dit geen invloed op de werking van het NAC authenticatieproces. Gebruikers zullen hier ook geen hinder van ondervinden.

De database is ingericht om alle accounting berichten op te slaan die op de radiusserver binnen komen. De radiusserver zal een verbinding initiëren naar de MySQL database en zal de database vullen met de gegevens uit het accounting bericht.

6.4.9. Wake-on-Lan

Wake-on-Lan(WOL) is een toepassing die computers opstart via een netwerkbericht. Om dit toe te kunnen passen in combinatie met 802.x. Is er een kleine aanpassing nodig op de switch. Om WOL toe te kunnen passen op het netwerk moet “dot1x control-direction in” ingesteld worden op iedere netwerkpoort. Door deze instelling kan er vanaf de switch wel gecommuniceerd worden met de computer, zonder dat de computer geauthentiseerd is op het netwerk.

6.5.Kosten

Voor het nieuwe NAC-ontwerp, van de Hogeschool Utrecht, is er voor het grootste deel gebruik gemaakt van componenten die inmiddels in bezit zijn van de Hogeschool Utrecht. Hierdoor hoeft er geen grote investering plaats te vinden. Als we kijken naar het nieuwe ontwerp, is er alleen een extra licentie nodig voor de Palo Alto firewall. Het gaat hier om de Palo Alto thread management licentie. Dit is een licentie die per jaar afgesloten wordt. Daarom is ervoor gekozen om de totale kosten in kaart te brengen. Zo wordt duidelijk wat het nieuwe NAC-ontwerp per jaar gaat kosten. In deze kostenberekening, zijn de kosten meegenomen die de Hogeschool Utrecht kwijt zal zijn per jaar aan het nieuwe NAC-ontwerp.

De onderhoudskosten van de netwerk componenten, de Palo Alto firewall en Active Directory, zijn hierin niet opgenomen. Dit is gedaan omdat de onderhoudskosten van deze componenten ondergebracht zijn in een raamwerk overeenkomst met Microsoft, Dimension Data en Secure Link. De kosten voor het nieuwe NAC-ontwerp worden in tabel hieronder weergegeven. Dit zijn de kosten die het totale NAC-ontwerp op jaarbasis gaat kosten. Deze kosten zijn inclusief het onderhoud aan apparatuur, licenties en beheer.

Jaarlijkse kosten		
2 x Windows Server 2008 R2	€	3.000,-
3 x Ubuntu Server 12.04	€	4.500,-
Qnet Appliance	€	8.200,-
Palo Alto Thread Management PA-5050-TP-HA	€	13.500,-
Totaal	€	29.200,-

De initiële kosten die gemaakt worden, voor het inrichten van NAC, zijn gebaseerd op de tijden die gemaakt zijn bij de uitvoering van de pilot. De initiële kosten zijn als volgt:

Initiële kosten		
Implementatie kosten 208 switches (208x3 uur = 624 uur x € 30,- per uur)	€	18.720,-
Implementatie servers (+/- 100 uur x € 30,- per uur)	€	3.000,-
Totaal	€	21.720,-

6.6.Proof of concept

Om tot een goed ontwerp te komen, is er gebruik gemaakt van een proof of concept. In dit proof of concept zijn de functionaliteiten en de technische werking getest. Daarnaast is de proof of concept opstelling gebruikt om ervaring op te doen met het nieuwe NAC-ontwerp. Voor de realisatie van het proof of concept is er gebruik gemaakt van de volgende componenten:

- Cisco 3560 Switch;
- Cisco Wireless Lan Controller;
- Cisco Access Point;
- Radiator radiusserver;
- Windows Network Policy Server;
- Windows Active Directory;
- Qnet Appliance;
- Palo Alto firewall met thread management.

Het proof of concept is opgebouwd in de testomgeving van de Hogeschool Utrecht. Echter voor de Qnet Appliance, Palo Alto firewall en Cisco Wireless Lan Controller is gebruik gemaakt van de productieomgeving. Dit is gedaan omdat er voor deze componenten, binnen de Hogeschool Utrecht, geen test apparatuur beschikbaar is. Wel zijn deze componenten op zodanige manier gebruikt dat het proof of concept geen invloed heeft op de productiecomponenten. Voor het testen van de werking van NAC is er gebruik gemaakt van diverse client apparaten.

Omdat er een pilottest uitgevoerd wordt, voor het testen van het nieuwe NAC-ontwerp, is ervoor gekozen alleen de authenticatie methodes te testen in het proof of concept. Dit om er zeker van te zijn, dat alle apparaten werken in het nieuwe ontwerp. Uit de pilotfase moet blijken of dit ook echt het geval is.

7. Adviesrapport

7.1.Inleiding

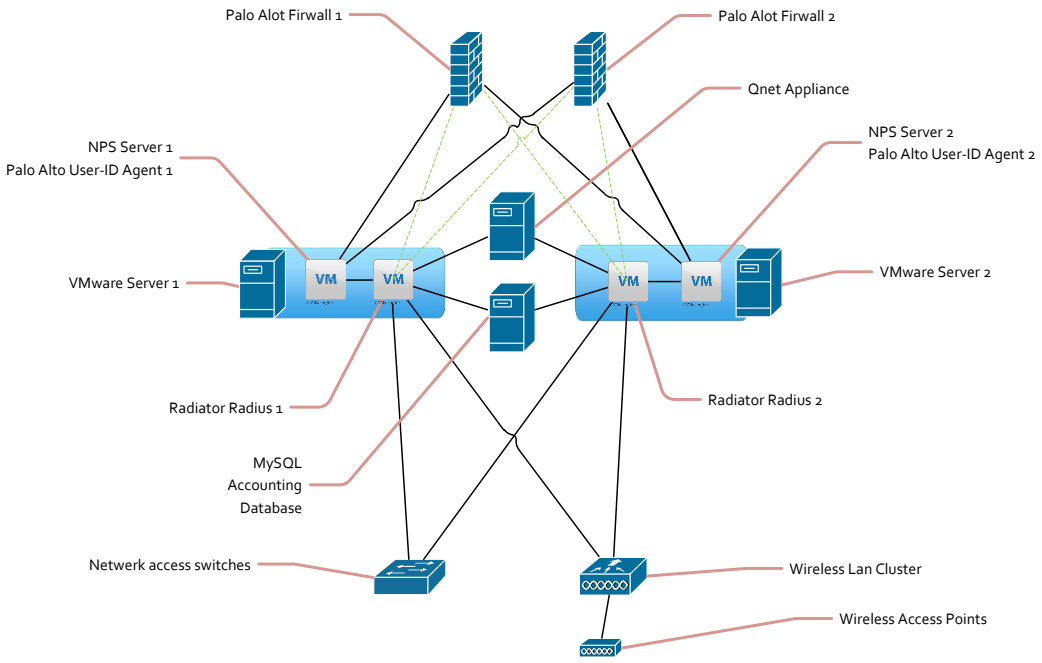
In dit adviesrapport wordt advies gegeven aan de hand van de pilot die is uitgevoerd op de Oudenoord 370. Allereerst zal de uitvoering van de pilot beschreven worden en daarna zullen de resultaten behandeld worden. Aan de hand van de resultaten zal er advies uitgebracht worden over NAC binnen de Hogeschool Utrecht.

7.2.Pilot

In de proof of concept is alleen de werking getest van het nieuwe NAC-ontwerp. Daarom is een pilot uitgevoerd om te onderzoeken of het nieuwe NAC-ontwerp functioneert binnen de ICT infrastructuur van de Hogeschool Utrecht. In deze pilot is het nieuwe NAC-ontwerp getest op de functionele werking, maar er is ook gekeken naar de technisch prestaties. De pilot is uitgevoerd op de locatie Oudenoord 370. Daarnaast zijn er op verschillende faculteiten punten getest, dit is gedaan om zo alle soorten apparaten te testen in combinatie met het nieuwe NAC-ontwerp. De apparaten die getest zijn in de pilot, zijn terug te vinden in het onderzoeksrapport.

7.2.1. Pilot opstelling

Op afbeelding 21 is te zien hoe de pilot opstelling is opgezet. Om ook in de pilot te garanderen dat NAC geen singlepoint of failure is, wordt gebruik gemaakt van twee VMware servers. Op beide VMware servers is een Radiator radius en NPS servers geïnstalleerd. Dit is gedaan om te zorgen. Dat bij een uitval van één van de twee servers, de gebruikers niet zonder netwerkverbinding komen te zitten.



afbeelding 21: Pilot opstelling

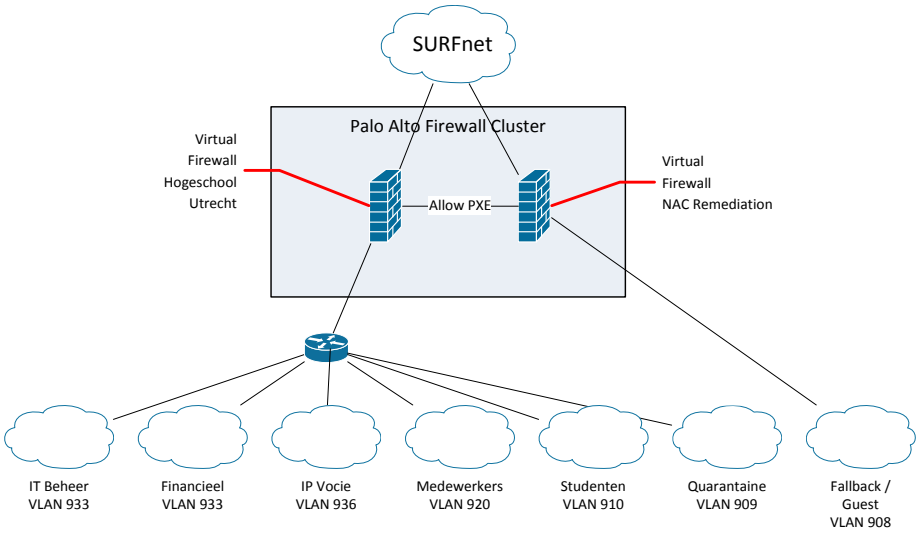
Op de twee NPS servers zijn ook twee Palo Alto User-ID agent's geïnstalleerd. Deze User-ID agent's verzorgen de communicatie tussen de Radiator radiusserver en de Palo Alto firewall.

De Radiator radiusservers zijn vervolgens verbonden met de Qnet Appliance en de MySQL database. Daarnaast is de testomgeving zo ingericht dat de radiusservers ook de syslogberichten ontvangt van de Palo Alto firewalls. Deze syslogberichten worden gebruiker om thread management informatie beschikbaar te maken in de Qnet Appliance.

Voor het draadloos netwerk is er een extra SSID aangemaakt genaamd “HU-NAC”. Deze is alleen beschikbaar op de Oudenoord 370. Daarnaast is de SSID verbonden met beide radiusservers.

Als laatste zijn alle switches op de locatie Oudenoord 370 verbonden met de twee radiusservers en zijn alle netwerkpoorten geconfigureerd, zodat 802.1x beschikbaar is. Om de overgang soepel te laten verlopen is het fallback VLAN tijdelijk anders ingesteld. Hierdoor hebben de gebruiker geen last van de wijziging. Nadat alle apparaten op de juiste manieren zijn ingesteld, is het fallback VLAN op de juiste wijze geconfigureerd.

Voor de pilot is ook een virtual firewall aangemaakt op de Palo Alto firewall cluster. Deze firewall is aangemaakt om het fallback VLAN te scheiden van het Hogeschool Utrecht netwerk. Daarnaast dient deze firewall ook als captive portal voor het fallbacknetwerk. Om netwerk installaties, via PXE, op het fallbacknetwerk toe te laten, is er een interconnect aangemaakt tussen de firewall van de Hogeschool Utrecht en de firewall die voor het fallbacknetwerk gebruikt wordt. Dit is te zien op afbeelding 22. In het nieuwe NAC-ontwerp is het ook de bedoeling om het Quarantainenetwerk achter de firewall van het fallbacknetwerk te plaatsen. In de pilot is dit echter niet gedaan. Dit is niet gebeurd, omdat de quarantainenetwerk ook gebruikt wordt op de productie omgeving.



afbeelding 22: Pilot opstelling netwerk

7.2.2. Pilot resultaten

Na de inrichting van de pilotomgeving, is er twee weken getest met het nieuwe NAC-ontwerp. Deze testen zijn hoofdzakelijk uitgevoerd op de Oudenoord 370. Er zijn ook andere locaties getest om te kijken of alle soorten apparaten werken in combinatie met het nieuwe NAC-ontwerp. In dit hoofdstuk worden de resultaten van de pilot beschreven. Tijdens de pilot is gekeken naar de functionele werking van het nieuwe NAC-ontwerp, maar ook naar de performance van het ontwerp. Uit de pilot is gebleken dat het nieuwe NAC-ontwerp goed functioneert. Alle functies functioneren in het nieuwe NAC-ontwerp zoals deze bedoeld zijn. Er zijn echter een paar belangrijke en interessante punten naar voren gekomen die hieronder beschreven worden.

7.2.2.1. MAB en MAC spoofing

Een belangrijk punt is de zwakheid van MAB. Met het MAB-mechanisme is het mogelijk om apparaten te authentiseren aan de hand van het MAC-adres. Uit de pilot is gebleken dat een MAC-adres gespoofed kan worden. Dit houdt in dat bijvoorbeeld een computer het MAC-adres van een IP telefoon kan instellen als het MAC-adres van de computer. Hierdoor kan iemand zonder toestemming toch toegang krijgen tot het voice VLAN. Dit kan opgelost worden door dynamic arp inspection.

7.2.2.2. Salto en NAC

Tijdens de pilot zijn alle soorten apparaten getest die genoemd zijn in het onderzoeksrapport. Alle apparaten die ondersteuning bieden aan 802.1x, werken naar behoren. De apparaten die geen ondersteuning bieden aan 802.1x, zijn ingesteld om te authentiseren via MAB. In bijna alle gevallen werd er gebruik gemaakt van MAB. Echter de Salto apparatuur, het sleutelsysteem van de Hogeschool Utrecht, werkt niet met MAB. Er is niet achterhaald waarom Salto apparatuur niet werkt met MAB of andere vorm van netwerkbeveiliging zoals ACL's. Ook de leverancier van Salto kon hier geen antwoord op geven. Om toch NAC toe te kunnen passen, kan er op het de netwerkpoort een vast MAC-adres ingevuld worden. Hierdoor kan alleen het aangesloten Salto apparaat gebruik maken van het de netwerkpoort. Omdat het hier om ongeveer 20 Salto apparaten gaat, is dit nog te overzien.

7.2.2.3. Palo Alto thread management

Tijdens de pilot is de evaluatie versie van de Palo Alto thread management module geactiveerd voor al het netwerkverkeer dat door de Palo Alto firewall heen gaat. Niet alleen voor de pilot. Door het activeren van de thread management module, kon er waargenomen worden welke virussen, vulnerabilities en malware actief zijn op het netwerk van de Hogeschool Utrecht. In de twee weken dat deze module actief is, zijn er 3820 virussen, vulnerabilities en malware pakketten waargenomen. Daarnaast zij er 129 apparaten gedetecteerd die besmet zijn met virussen of malware. Als we kijken naar de huidige situatie, zien we dat er gemiddeld maar 2 tot 3 computers per week in quarantaine worden gezet. Als we kijken naar het verkeer dat van buiten de Hogeschool Utrecht naar binnen komt, is het aantal groter. Het gaat hierbij om 198,186 vulnerabilities pakketten en 25,750 malware en virus pakketten, die doorgelaten worden door de firewall. Hierbij gaat het om ongeveer 1000 IP-adressen waarvan pakketten afkomstig zijn. De meeste pakketten komen uit Rusland, China, Italië en Brazilië.

7.2.2.4. Netwerk verkeer koppelen aan een persoon

Het koppelen van netwerkverkeer aan de gebruiker is een belangrijk onderdeel van het nieuwe NAC-ontwerp. Door netwerkpakketten te koppelen, kan er gekeken worden wie er verantwoordelijk is voor welk netwerkverkeer. Omdat de gebruikersnaam in de Palo Alto firewall gekoppeld is aan het IP-adres, is het mogelijk om firewall rules aan te maken op basis van gebruikersnaam. Hierdoor is het mogelijk om alleen personen toe te laten tot financiële netwerksegmenten in plaats van IP-adressen. Tijdens de pilot was er zoveel enthousiasme voor deze functie, dat deze functie reeds geïmplementeerd is op het draadloos netwerk van de Hogeschool Utrecht.

7.2.2.5. Authenticatie snelheid

De snelheid waarmee een gebruiker of apparaat geauthentiseerd wordt op het netwerk is een belangrijke factor voor het slagen van NAC op de Hogeschool Utrecht. Wanneer het authentiseren te lang duurt, zullen gebruikers hier last van hebben en dit als negatief ervaren. De kans dat een implementatie van NAC hierdoor wordt gecanceld is groot. Daarom is er in de pilot uitvoerig getest, hoe snel het authentiseren gaat met het nieuwe NAC-ontwerp.

Op het bekabeld netwerk gaan de authenticaties erg snel. Bij de eerste keer authentiseren duurt het gemiddeld 1 á 2 seconden. Dit geldt voor zowel MAB als 802.1x authenticaties. Wanneer er een IP telefoon en computer, op dezelfde netwerkpoort, tegelijk geauthentiseerd moeten worden, duurt dit gemiddeld 1 seconde langer. Dit is alleen van toepassing wanneer de IP telefoon nog niet is geauthentiseerd. Wanneer dit wel het geval is, zal het authentiseren net zo snel gaan als zonder IP telefoon. Wanneer er een herauthenticatie plaatsvindt, wordt de verbinding niet onderbroken.

Op het draadloos netwerk duurt een authenticatie gemiddeld 4 á 5 seconden. Dit is twee keer zolang als bij het bekabeld netwerk. Dit komt omdat er op het draadloos netwerk meer factoren meespelen dan alleen de authenticatie. Het authenticatieproces is ook afhankelijk van de dichtheid van het

draadloos spectrum en de hoeveelheid aangesloten computers op één acces point. Als er gekeken wordt naar de Radiator radiusserver, is te zien dat de authenticatie voor zowel het draadloos als bekabeld netwerk even snel gaan. Hieruit kunnen we dan ook opmaken dat de vertraging ontstaat door de infrastructuur van het draadloos netwerk en niet door het authenticatieproces. Voor zowel het bekabeld als draadloos netwerk maakt het niet uit of dit 1, 10, of 50 authenticaties tegelijk zijn. De tijden blijven hetzelfde.

7.2.2.6. *Minder beheer*

Naast alle voordelen die het op beveiligingsniveau heeft, zal de belasting van het beheer ook minder worden. Doordat netwerkpoorten niet meer handmatig ingesteld hoeven te worden, maar dynamic, zijn er minder handelingen nodig. Ook is er minder administratie nodig, omdat het toewijzen van het juiste netwerksegment automatisch gebeurt. Ook neemt de kans op fouten af, waardoor gebruikers van het netwerk niet zomaar in het verkeerde netwerksegment terecht komen.

7.3.Conclusie en aanbevelingen

De pilot geeft een goed inzicht in de werking van NAC binnen de Hogeschool Utrecht. Uit de pilot kunnen we concluderen dat NAC, op het juiste niveau, extra waarde geeft aan de veiligheid van het netwerk. Daarnaast is NAC essentieel voor het bring your own device(BYOD) concept en het flexibele werken dat de Hogeschool Utrecht voor ogen heeft. Want door het toepassing van NAC, kan bepaald worden per apparaat, per gebruiker of gebruikersrol, wie wel en wie geen toegang heeft tot de verschillende resources.

Door thread prevention toe te passen, kan er sneller gereageerd worden op malware of misbruik op het netwerk. Door gebruik te maken van MAB, 802.1x en een captive portal, kan iedereen geauthentiseerd worden zonder dat een gebruiker client software hoeft te installeren. Omdat iedereen zich eerst moet authentiseren is het mogelijk om alle datapakketen te koppelen aan een gebruikersnaam. Ook het beheer van de switches zullen afnemen, omdat de netwerksegmenten dynamic worden aangepast.

Door het hergebruiken van componenten, die al in het bezit zijn van de Hogeschool Utrecht, zijn de kosten laag gebleven. In het nieuwe NAC-ontwerp is gebruik gemaakt van open standaarden, waardoor het nieuwe NAC-ontwerp makkelijk te integreren is in een gemixte netwerkomgeving van diverse merken.

Er kan geconcludeerd worden dat NAC volwassen genoeg is om gebruikt te worden binnen de Hogeschool Utrecht. Er zijn een aantal aandachtpunten voor de invoering van NAC. Daarom zijn hieronder een aantal aanbevelingen beschreven die moeten helpen bij de implementatie van NAC.

- **Thread prevention als eerste implementeren**
  Uit de pilot is gebleken dat er veel computers besmet zijn met virussen en malware, maar er worden ook aanvallen van buiten de Hogeschool Utrecht gedaan. Daarom is het advies om zo snel mogelijk thread management te implementeren. Hiermee kunnen de aanvallen van buitenaf tegengehouden worden.
- **Stapsgewijs implementeren**
  Voor het uitrollen van NAC is het van belang dat alles stapsgewijs geïmplanteerd wordt. Dit is belangrijk omdat het grote gevolgen heeft als het niet goed functioneert. Het advies is dan ook om te beginnen met het implementeren van het nieuwe NAC-ontwerp op het draadloos netwerk. Omdat er al NAC gebruikt wordt op de huidige omgeving zal de impact minder groot

zijn dan op het bekabeld netwerk. Wanneer er begonnen wordt met de implementatie op het bekabeld netwerk, kan dit het beste per patchkast en per switch gedaan worden.

- **Dynamic ARP inspection implementeren**
  Omdat het MAB authenticatie mechanisme makkelijk te misbruiken is, wordt het advies gegeven om dynamic ARP inspection te implementeren. Dit mechanisme kan herkennen of er misbruik wordt gemaakt van het MAB authenticatie mechanisme.
- **NAC op VPN**
  In het nieuwe ontwerp is VPN op NAC niet meegenomen. Er is echter wel rekening gehouden dat op het VPN netwerk thread prevention kan worden toegepast. Dit kan gedaan worden door tussen het VPN netwerk en het interne netwerk van de Hogeschool Utrecht de Palo Alto firewall te plaatsen. Hierdoor kan het netwerk verkeer op het VPN netwerk geïnspecteerd worden.
- **EU aanbesteding**
  Omdat het huidige netwerk EU aanbesteed gaat worden, is het van belang dat er eisen worden meegenomen in het EU aanbestedingstraject, zodat het nieuwe NAC-ontwerp ook samen werkt met het nieuwe netwerkontwerp. De eisen die hiervoor meegenomen moeten worden zijn:

    - De access switch moet ondersteuning bieden voor 802.1x;
    - De access switch moet multi-domain authenticatie ondersteuning;
    - De access switch moet radius ondersteunen;
    - De access switch moet mac authentication bypass functies hebben;
    - De access switch moet een fallback of guest vlan functie aanbieden, wanneer een 802.1x authenticatie mislukt.

8. Evaluatie

Voordat er gestart kon worden met de afstudeeropdracht, is er een plan van aanpak gemaakt. In dit plan van aanpak is inzicht gegeven in de wijze waarop het afstudeer project is uitgevoerd. Er staat in beschreven welke stappen en producten er opgeleverd zijn. Ook de planning was een onderdeel van het plan van aanpak. Het plan van aanpak heeft tijdens het uitvoeren van de afstudeeropdracht een houvast gegeven, waardoor de afstudeeropdracht op tijd is afgerond.

Het eerste product dat is opgeleverd tijdens het uitvoeren van de afstudeeropdracht is het onderzoeksrapport. Dit onderzoeksrapport is opgedeeld in drie delen. In het eerste deel is onderzoek gedaan naar wat NAC precies inhoud. In het tweede deel is gekeken naar de huidige situatie van de Hogeschool Utrecht ten aanzien van NAC. En in het laatste deel zijn de wensen en eisen in kaart gebracht. Voor het inwinnen van informatie zijn er tweetal bijeenkomsten bijgewoond. De eerst bijeenkomst was door Cisco georganiseerd en de tweede bijeenkomst door Juniper georganiseerd. Tijdens beide bijeenkomsten waren NAC en bring your own device(BYOD) de hoofdpunten van de bijeenkomst. Tijdens deze bijeenkomsten is er kennis opgedaan van NAC en wat NAC precies inhoud. De bijeenkomst waren marketing gericht, waardoor er vooral ingegaan werd op de producten die Cisco en Juniper aanbieden. Desondanks was het zeer leerzaam.

Voor het in kaart brengen van de huidige en gewenste situatie is er eerst gekeken naar het beleid van de Hogeschool Utrecht. Vervolgens zijn er interviews afgenomen met de manager infrabeheer, security officer, netwerk- en serverbeheerders en een aantal gebruikers van het netwerk. Omdat de meeste geïnterviewden nog niet bekent waren met het NAC concept, begonnen de interviews erg moeizaam. Maar naarmate ze het concept NAC begrepen, ging het een stuk beter. Dit is een aandachtspunt voor in de toekomst.

Het was snel duidelijk dat er gekozen werd voor een NAC-oplossing met huidige componenten, die al in het bezit zijn Hogeschool Utrecht. De kosten tussen een nieuwe oplossing van Cisco of Juniper en het hergebruiken van componenten was zo groot, dat dit nooit zou geaccepteerd worden door het management.

Om tot de juiste oplossing te komen zijn er zelf scripts gemaakt. Echter de kennis van PERL, waarin de scripts geschreven zijn,was niet aanwezig binnen de afdeling infrabeheer. Om toch het ontwerp te realiseren, is deze kennis opgedaan door online tutorial en screencasts te volgen.

Om het adviesrapport te onderbouwen is er een pilot uitgevoerd op de Hogeschool Utrecht. Deze pilot was erg leerzaam. Zonder het uitvoeren van de pilot, zouden een aantal belangrijke en interessante resultaten nooit ontdekt zijn. Hiervan is geleert dat bij het uitvoeren van een pilot veel ontdekt kan worden. Dit kan helpen om problemen tijdens de implementatie te voorkomen.

Bronvermelding

Cisco. (sd). *Cisco.* Opgeroepen op mei 5, 2012, van www.cisco.com

Cisco. (sd). *Understanding the Cisco ICE Server*. Opgeroepen op April 5, 2012, van http://goo.gl/iKkMf

Gartner. (2011, December 8). *Magic Quadrant for Network Access Control*. Opgeroepen op Maart 2010, 2012, van http://goo.gl/Ms2rC

Gartner. (2011, December 22). *NAC Strategies for Supporting BYOD Environments*. Opgeroepen op Maart 10, 2012, van http://goo.gl/a4HmE

Gartner. (2011, October 11). *Strategic Road Map for Network Access Control*. Opgeroepen op Maart 10, 2012, van http://goo.gl/ak8ZH

G-Data. (2011, Februari 9). *G Data waarschuwt voor toename 'hacktivisme' en malware-aanvallen in 2011*. Opgeroepen op April 2, 2012, van http://goo.gl/nWvWN

Innervate. (2012, Januari). *Whitepaper 802.1x*. Opgeroepen op Maart 13, 2012, van http://goo.gl/HvL3d

Juniper. (sd). *Unified Access Control*. Opgeroepen op April 7, 2012, van http://goo.gl/MB5kC

Juniper. (sd). *WHITE PAPER - 802.1X: Port-Based Authentication Standard for Network Access Control.* Opgeroepen op April 16, 2012

Mudde, M. (2011, December 16). Netwerk Structuur Firewall. Utrecht: Hogeschool Utrecht.

Trusted Computing Groep. (2012, Januari). *Comply-to-connect solution overview.* Opgeroepen op April 10, 2012

Trusted Computing Group. (2007, November). *Controlling Network Access and Endpoints*. Opgeroepen op Maart 10, 2012, van http://goo.gl/e3VV6

Begrippenlijst

- **802.1x:** Protocol om poort gebaseerde authenticatie toe te passen.
- **Access Requestor:** Binnen NAC het onderdeel dat een verzoek doet om toegang te krijgen.
- **Access laag:** Netwerk laag die toegang biedt tot het netwerk**.**
- **Access point:** Een apparaat die het draadloos signaal uitzend.
- **Access poort:** Een netwerkpoort op een switch.
- **Active Directory:** De directory service van Microsoft.
- **Core laag:** Netwerk laag die netwerk voorziet aan de distributie laag.
- **Cliënt:** Een apparaat of stuk software die communiceert met een server.
- **Distributie laag:** Netwerk laag die netwerk voorziet aan de access laag.
- **Domainnaam:** De naam waar een host met wordt aangeduid.
- **Firewall:** Een barrière in het netwerk die netwerk verkeer beschermt tegen misbruik.
- **Lightweight access point:** Een access point die zich gedraagt als antenne van de WLC.
- **Network Access Control:** Concept die beschrijft hoe netwerktoegang kan toepassen worden.
- **Patch poort:** Een poort in een werkruimte waar je een netwerk apparatuur op kan aansluiten.
- **Policy Enforcement Point:** Binnen NAC het onderdeel dat toegang geeft.
- **Policy Decision Point:** Binnen NAC het onderdeel dat beslissing neemt wie er toegang krijgt.
- **Preboot execution environment:** Mechanisme om computers op afstaand te installeren.
- **Quarantaine:** Afgeschermde VLAN waar besmette computers in staan.
- **Realm:** Dit is eendere naam voor een domainnaam.
- **Router:** Apparaat dat netwerken met elkaar verbinden.
- **SSID:** Naam die uitgezonden wordt op een access point.
- **Switch:** Apparaat dat computers verbinden met het netwerk.
- **VLAN:** Een netwerksegment binnen het netwerk.
- **VLAN ID:** Het nummer van de VLAN.
- **Wake-on-Lan:** Mechanisme om computers op te starten op afstand.

Afbeeldinglijst

Plan van Aanpak

“Netwerk Access Control binnen de Hogeschool Utrecht”

Naam : Danny Verbeek
Studentnr : 1572282
Datum : 15-11-2011
Klas : SI6A
Opleiding : Systeembeheer Duaal

Inhoudsopgave

1. Inleiding

Voor u ligt mijn Plan van Aanpak, dat deel uit maakt van het afstudeertraject. In dit Plan van Aanpak maak ik concreet op welke wijze ik mijn afstudeertraject zal uitvoeren. Dit plan van aanpak heeft als doel om de afstudeercommissie zicht te geven in mij afstudeeropdracht. Daarnaast dient het als kader voor het uitvoeren van mijn afstudeeropdracht. In dit plan van aanpak zullen de volgende onderwerpen aan bod komen:

- Aanleiding tot de opdracht;
- Bedrijfssituatie waarbinnen het afstudeerproject wordt uitgevoerd;
- Probleemstelling;
- Doelstellingen;
- Producten en activiteiten;
- Projectgrenzen en randvoorwaarden;
- Methoden en technieken;
- Project organisatie.

2. Bedrijfssituatie

2.1. Hogeschool Utrecht

Hogeschool Utrecht is een HBO, Deze onderwijsinstelling die is ontstaan in 1995 door fusie van een aantal hogescholen in Utrecht. De fusie is tot stand gekomen vanwege een overheidsmaatregel om landelijk bijna 80 hogescholen te fuseren tot 45 nieuw hogescholen. Tot 2004 droeg de organisatie de naam: Hogeschool van Utrecht. Maar in 2005 hebben zij deze naam veranderd in Hogeschool Utrecht. Aan de Hogeschool Utrecht studeren bijna 40.000 studenten. Deze studenten zijn verdeelt over 6 faculteiten en 12 vestigingen, die gevestigd zijn in Utrecht en Amersfoort. Naast de studenten werken er ongeveer 3.500 medewerkers. De Hogeschool Utrecht is een plek waar studenten en medewerkers zich kunnen ontplooien, zich thuis voelen en waar we door samen te werken met onze relaties durven te experimenteren en innoveren.

1.1. Afdeling Infrabeheer

De afdeling Infrabeheer is onderdeel van Informatie Management en ICT die vervolgens weer onderdeel is van stafdienst bedrijfsvoering(SBV). Infrabeheer is verantwoordelijk voor het beheer van de basis ICT infrastructuur van de Hogeschool Utrecht en wordt geleid door Ed de Vries. De afdeling infrabeheer is op te delen in de vier verschillende expertises, genaamd: Netwerk en Telefonie, Basis Infra, Active Directory en Adviseurs. Gezamenlijk is de afdeling infrabeheer verantwoordelijk voor het beheren en continueren van de ICT infrastructuur van de Hogeschool Utrecht. Tevens draagt het team bij aan het innoveren en vernieuwen van de operationele omgeving van de Hogeschool Utrecht.

1.2. Mijn functie

Binnen Informatie Management en ICT ben ik werkzaam in het team infrabeheer. Dit team is verantwoordelijk voor de basis ICT infrastructuur van de Hogeschool Utrecht. Het team basis infrabeheer is verantwoordelijk voor het beheren, migreren, implementeren en ontwikkelen van de basis ICT voorzieningen van de Hogeschool Utrecht. Dit zijn server-, netwerk, storage-, security-, mail-, en telecombeheer. Als team basis infrastructuur werken we nauw samen met de afdeling applicatiebeheer. Deze afdeling beheren de applicaties die binnen de Hogeschool Utrecht gebruikt worden. Mijn rol binnen infrabeheer is netwerk-, en telefoniebeheerder. Ik ben verantwoordelijk voor het beheer van het TCP/IP datanetwerk, de firewall en het IP telefoniesystemen van de Hogeschool Utrecht. Daarnaast heb ik ook een adviserende rol. Mijn adviezen en aanbevelingen geef ik aan het ICT management om systemen binnen de hogeschool Utrecht te optimaliseren en te verbeteren.

2. Formulering afstudeeropdracht

2.1. Aanleiding

De Hogeschool Utrecht heeft een koers uitgezet genaamd: Koers 2012. In Koers 2012 wordt de strategische koers ten aanzien van de HU bedrijfsvoering geformuleerd. Vanuit deze koers is er een Strategisch ICT beleid HU 2010-2015 ontwikkeld, die de ambities van de Hogeschool Utrecht op ICT gebied vastlegt. Dit wordt gedaan in de vorm van doelstellingen met de daaraan verbonden kaders.

Van Ed de Vries heb ik de vraag gekregen om te kijken, hoe er vanuit netwerkbeheer een bijdrage geleverd kan worden om deze doelstelling te ondersteunen. In samenspraak met Ed de Vries heb ik er voor gekozen om onderzoek te doen hoe de Hogeschool Utrecht gebruik kan maken van Network Access Control. De doelstellingen waar dit onderzoek een bijdragen aan zal leveren zijn:

- Een omgeving scheppen om te komen tot een open virtuele kennisorganisatie.
- ICT dienstverlening is gebaseerd op anytime, anywhere, any device.
- De ICT dienstverlening ondersteunt in toenemende mate de zelfredzaamheid en zelfservice van gebruikers (studenten, medewerkers en externen).
- Specifieke ICT dienstverlening op basis van standaard bouwstenen (modulair opgebouwde ICT voorzieningen) en standaard gegevensuitwisseling (interoperabiliteit).

2.2. Probleemstelling

De Hogeschool Utrecht heeft een groot data netwerk, dat netwerk connectiviteit geeft aan een groot aantal apparaten. De diversiteit van deze apparaten loopt uiteen van chipknip oplaadpunten tot privé laptops van studenten, medewerkers en externe partners. Deze apparaten kunnen gebruikmaken van zowel het bedraad als draadloos netwerk van de Hogeschool Utrecht.

Een groot aantal apparaten van de Hogeschool Utrecht, valt buiten het beheer van de organisatie. Hierdoor is de kans erg groot dat de apparaten die op het netwerk zijn aangesloten malware, virussen of ander kwaadwillende software met zich mee dragen. Hierdoor Is de kans groot dat malware, virussen of ander kwaadwillende software zich kunnen verspreiden over het data netwerk en voor grote problemen kunnen zorgen. Daarnaast kan een gebruiker ook kwaadwillende intenties hebben.

Op het bedraad netwerk is geconstateerd dat er regelmatig apparatuur van studenten, medewerkers of externe partners in verkeerde netwerk segmenten terecht komen. Zo komt het voor dat apparatuur van zowel studenten, medewerkers als externe partners, ook terecht komen in betaal, chipknip en andere bedrijf kritische netwerken.

Naast de mogelijke problemen die hierboven zijn genoemd, neem het werkplek onafhankelijk werken een steeds grotere rol in binnen de Hogeschool Utrecht. Hierdoor gaan gebruikers meer werken op verschillende locaties of werken vanuit huis. Door het statische karakter van het netwerk is dit voor medewerkers met een systeembeheer, financiële of dergelijke bedrijfsinformatie gevoelige applicaties niet mogelijk zonder teveel handmatige aanpassingen. Dit omdat per netwerk switchpoort en per vlan rechten worden toegekend.

2.3. Doelstelling van de afstudeeropdracht

De doelstelling van deze afstudeeropdracht is om te onderzoeken hoe en of het mogelijk is om Network Access Control te gebruiken binnen het netwerk van de Hogeschool Utrecht. Hierbij is het de bedoeling dat medewerkers, cursisten en studenten tijds- en plaats onafhankelijk kunnen werken en hebben daarbij keuzevrijheid in de daarvoor benodigde apparatuur. Studenten, cursisten en medewerkers moeten daarbij onafhankelijk van plaats of tijd toegang hebben tot de benodigde informatie. Dit mag echter niet ten kosten gaan van de integriteit, confidentialiteit en authenticiteit. Op het wireless netwerk van de Hogeschool Utrecht wordt er al een Access Controle gedaan. Echte is dit nog beperkt. Naast het bedraad zal dus ook naar het wireless netwerk gekeken moeten worden. Zodat er één oplossing komt voor het toegang krijgen tot het netwerk van de Hogeschool Utrecht. Door middels van een pilot moet blijken of Network Access Control(NAC) volwassen genoeg is om gebruikt te worden binnen de Hogeschool Utrecht.

Concreet heb ik de volgende doelstelling opgesteld:

- Inventariseren welke apparaten er gebruik maakt van het datanetwerknetwerk;
- Inzicht krijgen in welke natuurlijke personen gebruik maken van het netwerk;
- Dynamisch vlan(logische compartimentering) toewijzen aan de persoon op basis van de Functie of Rol;
- Het vroegtijdig detecteren van misbruikt en malware;
- De oplossing moet werken volgens een cliënt-less authenticatie en autorisatie;
- De oplossing mag geen single point of failure(SPOF) zijn;
- De oplossing moet werken met Open standaard of marktconform geaccepteerde standaarden;
- De oplossing moet mogelijkheid bieden tot een gast netwerk;
- De oplossing moet flexibel, uitbreid baar zijn naar de VPN en Wireless omgeving, zodat access control één geheel wordt;
- De oplossing moe mee groeien in de toekomst;
- Dataverkeer moet te herleiden zijn naar een natuurlijk persoon;

3. Het Project

3.1.Organisatie

Het project dat ik ga uitvoeren is een op zichzelf staand project en is geen onderdeel van een ander project. Dit project is wel een gevolg van de Strategisch ICT beleid HU 2010-2015. De opdracht zelf kom naar voren uit de “Roadmap infra 2011 – 2012” van de afdeling infra. Hierin staan onderwerpen waaraan komende jaren gewerkt zullen worden. Network acces control van het data netwerk is hier een onderdeel van. Het is hierbij de bedoeling dat er gekeken gaat worden naar een centraal oplossing voor toegangscontrole op het data netwerk. Het gaat hier zowel om het bedraad als wireless netwerk van de Hogeschool Utrecht.

Naast mijn directe collega’s zullen de volgende personen een onderdeel gaan spelen in dit project.

Opdrachtgever:
Naam : Ed de Vries
Organisatie : Hogeschool Utrecht
Functie : Manager afdeling infra
E-mail : ed.devries@hu.nl

Opdrachtnemer:
Naam : Danny Verbeek
Organisatie : Hogeschool Utrecht
Functie : ICT Beheerder
E-mail : danny.verbeek@hu.nl

Bedrijfsbegeleider:
Naam : Gerard Verwoolde
Organisatie : Hogeschool Utrecht
Functie : Adviseur
E- mail : gerard.verwoolde@hu.nl

Studiebegeleider:
Naam : Leendert van Doesburg
Organisatie : Hogeschool Utrecht
Functie : Docent
E- mail : leendert.vandoesburg@hu.nl

3.2.Activiteiten en producten

Het afstuderen zal bestaan uit een aantal fases. Tevens zullen er uit de verschillende fases verschilden producten worden opgeleverd. De fases en producten die opgeleverd worden zijn als volgt:

- **Fase 1: Initiatiefase**
  De initiatiefase is de voorbereiding op de afstudeeropdracht. Na de goedkeuring van dit afstudeervoorstel door de afstudeercommissie, zal er in februari gestart worden met deze fase.

  Activiteiten:
  - Het maken van de Plan van Aanpak
  - Het maken van de projectplanning
  - Het afsluiten van het afstudeercontract

  Producten:
  - Plan van Aanpak
  - Afstudeercontract

- **Fase 2: Analysefase**
  In de analysefase wordt de inventarisatie gedaan van de informatie die nodig is voor het project. Deze resultaten zullen verwerkt worden in een onderzoeksrapport.

  Activiteiten :
  - Onderzoek: Wat is Network Access Control?
  - Onderzoek naar de huidige situatie
    - Huidige situatie netwerk
    - Huidige situatie toegangscontrole
  - Onderzoek naar de gewenste situatie
    - Onderzoek gewenste situatie vanuit management perspectief
    - Onderzoek gewenste situatie vanuit security perspectief
    - Onderzoek gewenste situatie vanuit beheer perspectief
    - Onderzoek gewenste situatie vanuit gebruikers perspectief

  Producten:
  - Onderzoeksrapport

- **Fase 3: Ontwerpfase**
  In deze fase wordt gestart met het maken van een functioneel en technisch ontwerp. In het functioneel ontwerpt wordt gekeken naar het de functies die de te bouwen oplossing moet bieden. Dit zal zodanig worden omschreven dat het functioneel ontwerp goed te begrijpen is zonder technisch kennis. In het technisch ontwerp zal omschreven worden hoe het functioneel ontwerp technisch gerealiseerd gaat worden.

  Activiteiten:
  - Functioneel Ontwerp maken
  - Technisch Ontwerp maken
  - Proof of Concept ter ondersteuning aan het technisch ontwerp

Producten:

- Functioneel Ontwerp
- Technisch Ontwerp

- **Fase 4: Realisatiefase**
  In de realisatiefase wordt een pilot uitgevoerd op een deel van het netwerk. Daarnaast zal moeten blijken of Network Access Control volwassen is om gebruikt te worden binnen de infrastructuur van de Hogeschool Utrecht.

  Activiteiten:
  - Pilot opstellen en implementeren
  - Resultaten analyseren

  Producten:
  - Adviesrapport: Is Network Access Control volwassen genoeg om gebruikt te worden binnen de hogeschool Utrecht?

- **Afronding**
  Dit is de laatste fase van het project. In deze fase zal de scriptie opgeleverd worden. Deze scriptie wordt vervolgens aangeboden aan de Hogeschool Utrecht ter beoordeling. Na een goedkeuring zal ik deze scriptie gaan verdedigen in de vorm van een presentatie.

  Activiteiten:
  - Afronding scriptie
  - Verdediging scriptie

  Producten:
  - Scriptie

3.3. Projectgrenzen en randvoorwaarden

Het afstudeerproject begint februari 2012 en eindigt 29 mei 2012 om 12.00u. Na deze periode zal er een presentatie gegeven worden aan de afstudeercommissie en zal er tevens de verdediging plaatsvinden. Om er voor te zorgen dat het afstudeerproject op de uiterlijke inleverdatum af is zal er een planning gemaakt worden met verschillende deadlines. Dit zal verder uitgewerkt worden in de planning.

3.3.1. Randvoorwaarden

Er zijn een aantal randvoorwaarden om de afstudeeropdracht tot een succesvol einde te brengen:

- Student zal de ingeplande uren beschikbaar moeten zijn;
- Beschikbaarheid bedrijfsbegeleider Gerard Verwoolde;
- Beschikbaarheid afstudeerbegeleider Leendert van Doesburg;
- Beschikbaarheid hard- en software voor Proof of Concept;
- Beschikbaarheid collega's in verband met de interviews en overleg.

3.3.2. Afbakening

Om aan te geven wat wel/niet gedaan wordt tijdens de afstudeer opdracht zal ik in dit hoofdstuk aangeven wat binnen of buiten de scope van de opdracht valt.

Binnen de scope

- Onderzoek naar Netwerk Access Control;
- Onderzoek naar de huidige situatie;
- Onderzoek naar de gewenste situatie;
- Opstellen onderzoeksrapport;
- Functioneel Ontwerp maken;
- Technisch Ontwerp maken;
- Pilot opstelling implementeren, om te laten zien of NAC wel of geen oplossing is voor de Hogeschool Utrecht;
- Opstellen adviesrapport.

Buiten de scope

- De daadwerkelijke implementatie;
- Onderzoeken naar de functie en rollen die gebruikt worden binnen de HU, denk hierbij aan rollen zoals: onderwijsassistent, bedrijfsbegeleider en p&o medewerkers ;
- Ontwerp maken van de netwerk segmenten (logische compartimentering);
- Onderzoek welk product(merk) er gebruikt moet gaan worden, dit i.v.m. de Europese aanbesteding van het netwerk;
- Opstelling implantatieplan.

3.4. Methoden en technieken.

Tijdens de uitvoering van het project zal gebruik gemaakt worden van de volgende methoden en technieken:

Documenten onderzoek en literatuur onderzoek
Voor het in kaart brengen van de huidige situatie met betrekking tot de netwerk access security zal documenten en literatuur onderzoek uitgevoerd worden. Om kennis te verzamelen over de mogelijk nieuw te implementeren oplossing wordt gebruikt van documentenonderzoek.

Interviews
Voor het in kaart brengen van de knelpunten van de huidige situatie en de eisen die worden gesteld aan de nieuwe oplossing wordt gebruik gemaakt van interviews.

Raadplegen experts/ referentiebezoeken
Tijdens het onderzoek zal ik experts raadplegen, om informatie te verkrijgen betreffende bijvoorbeeld ervaringen met en werking van een bepaalt pakket. Hierbij kan ik de tevredenheid meten van derden over de leverancier en eventuele knelpunten en ervaringen bij invoering.

Proof of Concept
Door middels van een Proof of Concept(PoC) moet het duidelijk worden of Network Access Control volwassen is om gebruikt te worden binnen de Hogeschool Utrecht. Deze PoC zal zowel een Technische als Functionele integratietest ondergaan.

MoSCoW
Om in kaart te brengen aan welke eisen en wensen de oplossing moet voldoen, zal ik gebruik maken van de MoSCoW-methode. Deze methode zal ik gebruiken om de prioriteiten vast te leggen van de eisen en wensen. De prioriteiten zullen op de volgende manier worden vastgelegd
Must have: Aan deze eisen moet de oplossing voldoen, zonder deze eis is de oplossing niet bruikbaar.
Should have: Aan deze eisen moet de oplossing voldoen, zonder deze eis is de oplossing wel bruikbaar, maar niet gewenst.
Could have: deze eis mag alleen aan bod komen als er tijd genoeg is.
Won't have now: deze eis zal in dit project niet aan bod komen, maar kan in de toekomst wel aan bod komen

4. Planning

Projectactiviteit	Op te leveren product	Startdatum	Einddatum	Geschat aantal uren
Fase 1: Initiatieffase		**13-02-2012**	**16-03-2012**	**40**
Het maken van de Plan van Aanpak	Plan van aanpak	13-02-2012	16-03-2012	30
Het maken van de projectplanning		05-03-2012	16-03-2012	8
Het afsluiten van het afstudeercontract	Afstudeercontract	12-03-2012	16-03-2012	2
Fase 2: Analysefase		**12-03-2012**	**08-04-2012**	**130**
Onderzoek: Wat is NAC?	Onderzoeksrapport	12-03-2012	25-03-2012	20
Onderzoek naar de huidige situatie		19-03-2012	01-04-2012	50
Onderzoek naar de gewenste situatie		26-03-2012	08-04-2012	50
Opleveren/Opstellen onderzoeksrapport		02-04-2012	08-04-2012	15
Fase 3: Architectuur Fase		**09-04-2012**	**29-04-2012**	**10**
Functioneel Ontwerp maken	Functioneel en Technisch Ontwerp	09-04-2012	29-04-2012	45
Technisch Ontwerp maken		09-04-2012	29-04-2012	45
Opleveren/Opstellen functioneel en technisch ontwerp				10
Fase 4: Realisatiefase		**23-04-2012**	**20-05-2012**	**150**
Pilot inrichten	Adviesrapport: Is Network Access Control volwassen genoeg om gebruikt te worden binnen de hogeschool Utrecht	23-04-2012	06-05-2012	30
Pilot functionele testen		30-04-2012	20-05-2012	50
Pilot technisch testen		30-04-2012	20-05-2012	50
Resultaten analyseren		14-05-2012	20-05-2012	10
Opleveren/Opstellen Adviesrapport		14-05-2012	20-05-2012	10
Fase 5: Evaluatie Fase		**01-03-2012**	**29-05-2012**	**100**
Opstellen Scriptie	Scriptie	01-03-2012	29-05-2012	75
Opleveren Scriptie		29-05-2012	29-05-2012	1
Opstellen Verdediging	Presentatie	29-05-2012	11-06-212	10
Verdediging Scriptie/Afstudeeropdracht		11-06-2012	22-06-2012	4
Totaal aantal uren				**520**

	Feb.			Maart				April				Mei					Juni		
Activiteit\Weeknummers	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Fase 1: Initiatiefase																			
Het maken van de Plan van Aanpak																			
Het maken van de projectplanning																			
Het afsluiten van het afstudeercontract																			
Fase 2: Analysefase																			
Onderzoek: Wat is NAC?																			
Onderzoek naar de huidige situatie																			
Onderzoek naar de gewenste situatie																			
Opleveren /Opstellen onderzoeksrapport																			
Fase 3: Architectuur en Ontwerp Fase																			
Functioneel Ontwerp maken																			
Technisch Ontwerp maken																			
Opleveren/Opstellen functioneel en technisch ontwerp																			
Fase 4: Realisatiefase																			
Pilot inrichten																			
Pilot functionele testen																			
Pilot technisch testen																			
Resultaten analyseren																			
Opleveren /Opstellen adviesrapport																			
Fase 5: Evaluatie Fase																			
Opstellen Scriptie																			
Opleveren Scriptie																			
Opstellen Verdediging																			
Verdediging Scriptie/Afstudeeropdracht																			

Bijlage 2: Zelfevaluatie

Het begin van mijn afstudeertraject begon moeizaam. Dit kwam omdat ik het doel niet duidelijk voor ogen had. Deze moest ik helder krijgen. Nadat mijn doel: het in kaart brengen van NAC, binnen de Hogeschool Utrecht, op papier stond, werd het duidelijk waar ik naartoe moest werken. Nadat ik het doel scherp voor ogen had, ben ik mij gaan verdiepen in de technieken. Dit heb ik gedaan door me in te lezen in het onderwerp. Dit gaf een richtlijn voor het verdere proces.

Toen ik eenmaal begonnen was aan het afstudeerproject, had ik veel houvast had aan mijn plan van aanpak en de vooraf gemaakte planning. Omdat het afstudeerproject uitgevoerd is in drie maanden tijd, was het belangrijk dat alle producten op tijd werden opgeleverd om de deadline te kunnen halen. Om die reden ben ik zeer tevreden dat ik me goed aan de planning heb gehouden en hierdoor de deadline heb gehaald.

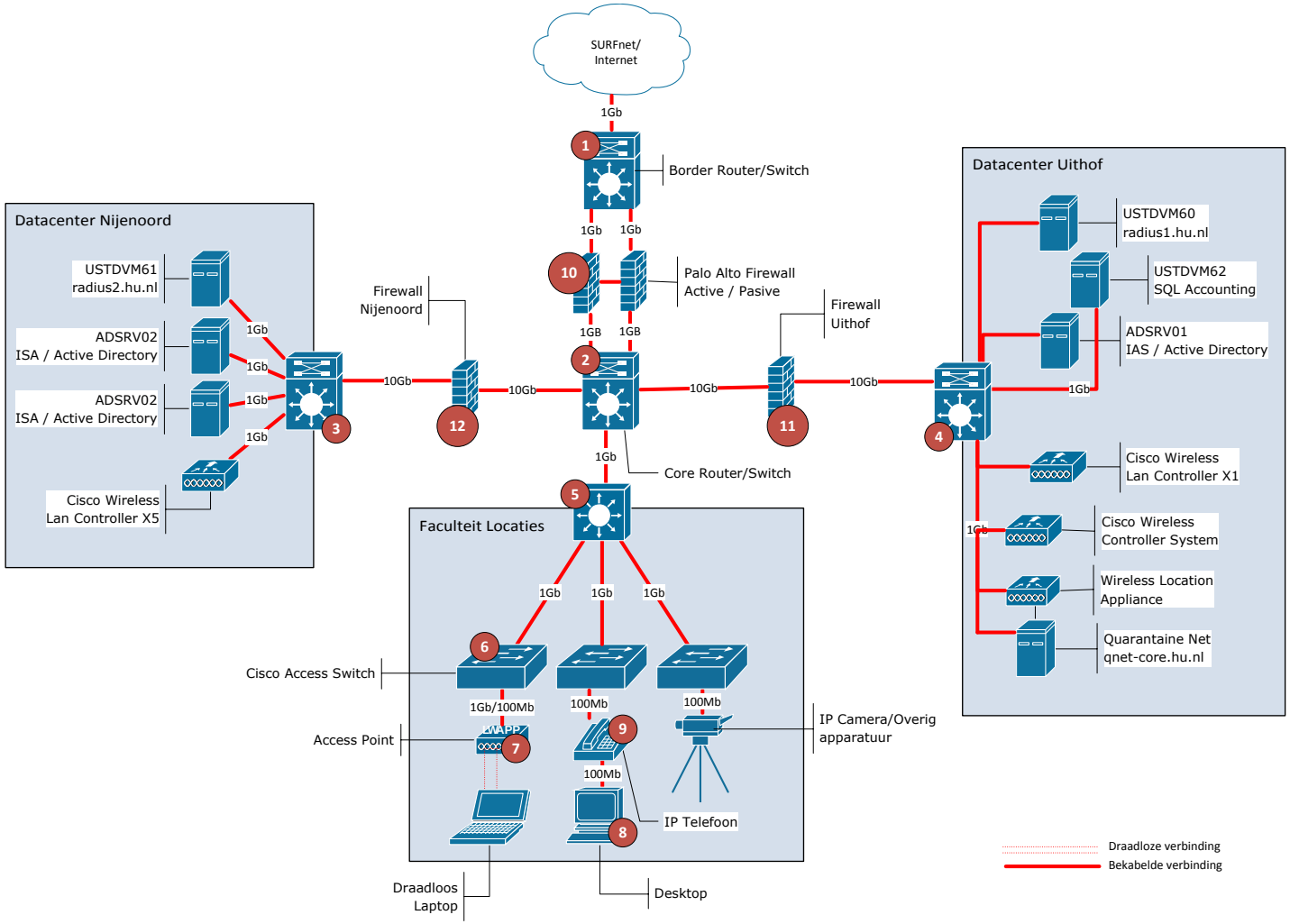
Het in kaart brengen van de huidige situatie en de eisen en wensen heb ik gedaan aan de hand van interviews en het lezen van interne documentatie. De interviews die ik heb gehouden, liepen in het begin moeizaam. In het gesprek ging het een stuk beter. Dit kwam omdat ik de interviews goed had voorbereid.

Tijdens de ontwerpen en opzetten van het nieuwe NAC-ontwerp, heb ik veel geleerd. Voordat ik aan het afstudeertraject begon, wist ik globaal wat NAC inhield. Door het inlezen en het bezoeken van seminars werd mij dit een stuk duidelijker.

Omdat ik heb gekozen om een NAC-oplossing te ontwerpen op basis van bestaande componenten, nam ik ook een risico. Voor deze oplossingen moesten een aantal scripts gemaakt worden in PERL. De script taal PERL was voor mij onbekend. Toch ben ik de uitdaging aangegaan om PERL te leren, zodat ik scripts kon schrijven om het nieuwe NAC-ontwerp te laten werken. En dit is gelukt!

Als ik kijk naar het gehele traject kan ik zeer tevreden zijn. Ondanks de moeizame start, heb ik het afstudeerproject op tijd afgerond. Daarnaast heb ik veel geleerd van het afstudeertraject, zoals het maken van een goed plan van aanpak. Ik kan terugkijken op een leerzame en intensieve periode.

Bijlage 3: Infrastructuur Hogeschool Utrecht



Bijlage 4: Toegangscontroleflow