Adviesrapportage Persoonsgebonden Toegang

Onderzoek en advies voor een strategie voor persoonsgebonden toegang

Auteurs: David Schrok
Studentnr: 1551536
1e examinator: Bert Buitenhuis

avans hogeschool

HOGESCHOOL UTRECHT

Adviesrapportage Persoonsgebonden Toegang

Onderzoek en advies voor een strategie voor persoonsgebonden toegang

Auteurs:	David Schrok	1e examinator:	Bert Buitenhuis
Studentnr:	1551536	Bedrijfsbegeleiders:	Paul Schoot
e-mail:	david.schrok@student.hu.nl		Peter Havekes
Klas:	SI6b		
Versie:	1.0 definitief		
Vak:	Afstuderen		
Vakcode:	TCIF-DU6AFST-05		
Datum:	25-05-2012		

avans hogeschool

HOGESCHOOL UTRECHT

Voorwoord

Voor u ligt het adviesrapport, welke het eindproduct is van de afstudeerperiode voor de opleiding Systeembeheer Duaal aan de Hogeschool Utrecht. In de periode van januari 2012 tot juni 2012, is er in het kader van mijn afstuderen, een onderzoek gedaan naar het realiseren van persoonsgebonden toegang voor systemen van Avans Hogeschool, welke bedrijfsgevoelige informatie of persoonsgegevens bevatten, maar ook om deze systemen voor "het nieuwe werken" op een veilige manier te kunnen ontsluiten.

In dit voorwoord wil ik mijn dank betuigen aan de volgende personen:

- Mijn gezin: Thea en Jelte, voor al het geduld, de behulpzaamheid en het begrip wat ik van hen gehad heb voor de investeringen in tijd voor deze studie de afgelopen drie jaar.
- Bert Buitenhuis: mijn begeleidend docent, die gedurende het onderzoek de nodige feedback heeft gegeven voor het verbeteren en aanvullen van mijn onderzoek.
- Peter Havekes: Niet alleen een gewaardeerd collega, maar ook een goede sparringpartner. Als mijn technische begeleider en projectlid hebben we een paar goede brainstormsessies gehouden om de strategieën en de invullingen daarvan helder te krijgen.
- Paul Schoot: Als mijn bedrijfsbegeleider heeft hij kritische feedback gegeven, maar ook goed geholpen bij het structureren en afbakenen van het afstudeeronderzoek
- Ina Kluijtmans: voor de tijd die ik gedurende mijn werktijd aan mijn afstuderen en mijn studie heb mogen gebruiken.

Gilze-Rijen, 25 Mei 2012

David Schrok.

Managementsamenvatting

Het netwerk van Avans heeft een gelaagde structuur, gebaseerd op het Defense-in-Depth beveiligingsmodel. De plaats van een device in het netwerk, bepaald naar welke netwerken het device kan communiceren. Met de groter wordende mobiliteit, “Bring-Your-Own-Device”-concept is daar een voorbeeld van, wordt de huidige gelaagdheid in toenemende mate een belemmering.

Om beter en flexibeler in te kunnen spelen op deze groter wordende mobiliteit is er onderzoek gedaan naar gangbare strategieën voor persoonsgebonden toegang, ter beveiliging van applicaties die persoons- of bedrijfsgegevens bevatten.

Het onderzoek heeft vier mogelijke strategieën opgeleverd die toepasbaar kunnen zijn voor het oplossen van de probleemstelling. De strategieën zijn als volgt:

- Servers in afgeschermd netwerk, waarbij een firewall geplaatst wordt tussen de services/applicaties en de gebruikers.
- Servers in afgeschermd netwerk, waarbij een VPN techniek geïmplementeerd wordt.
- Clients controleren en authenticeren voordat toegang wordt verleend, op basis van de NAC/NAP oplossing van Cisco en Microsoft.
- Verplaatsen van clients in netwerken na authenticatie en toekennen van een persoonsgebonden ACL.

De vier strategieën worden beoordeeld volgens beschreven beoordelingscriteria. Deze zijn:

- Kan de strategie volgens het beveiligingsmodel van Avans geïmplementeerd worden?
- Kan de strategie gerealiseerd worden met binnen Avans beschikbare techniek?
- Bied de strategie een volledige oplossing voor de probleemstelling?
- Is extra aanschaf (hardware/licenties) nodig?
- Is de strategie eenvoudig (transparant) voor eindgebruikers en beheerders?
- Is de strategie toepasbaar op gangbare end-user devices?

De beoordelingen van de strategieën levert de volgende resultaten:

- Alle strategieën voldoen aan de eisen wat betreft het bieden van de benodigde bescherming en gewenste flexibiliteit.
- Alle strategieën passen binnen het huidige beveiligingsmodel van Avans.
- Voor alle strategieën zal een investering moeten worden gedaan bij implementatie van de strategie.

De strategie gebaseerd op het plaatsen van servers in een afgeschermd netwerk, waarbij een firewall geplaatst wordt tussen de services/applicaties en de gebruikers, wordt als beste beoordeeld en dan met name op de volgende punten:

- Door het centraal georiënteerde beheer en de afwezigheid van een client voor het end-user device, zijn de beheerlasten lager dan bij de andere strategieën, welke allen een actie vragen van zowel beheerders als gebruikers.
- De ondersteuning van alle gangbare end-user devices
- De oplossing is transparant, doordat deze in de netwerklaag is ingebed.

Bij deze strategie zou de vraag kunnen opkomen of er inbreuk wordt gemaakt op de privacy van de gebruikers. Echter, doordat de strategie wordt ingezet als beveiligingselement voor persoonsgegevens en er sprake is van generiek monitoren met sturing als doel, is er vermoedelijk geen sprake van inbreuk op de Wet Bescherming Persoonsgegevens.

Het persoonsgebonden monitoren van netwerkverkeer zoals wordt gedaan in de aanbevolen strategie is relatief nieuw. Daardoor heerst er veel onduidelijkheid over wat er wel en niet mag volgens de wet. De wet- en regelgeving past zich aan op de ontwikkelingen op dit gebied en is continu aan veranderingen onderhevig door reactie op deze ontwikkelingen.

Inhoudsopgave

1 - Inleiding

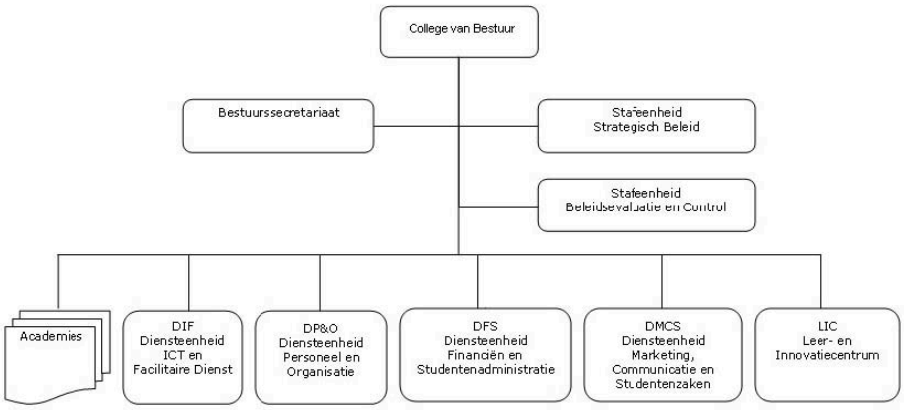
Op dit moment wordt binnen Avans gewerkt aan de implementatie van 'Het Nieuwe Werken' concept ter ondersteuning van de toenemende mobiliteit. Dit concept heeft grote gevolgen voor de ict-infrastructuur van Avans, met betrekking tot inrichting en beheer. Bij de implementatie van 'Het Nieuwe Werken' concept is Avans tot de conclusie gekomen dat de gelaagde netwerkinfrastructuur, waarop nu de beveiliging is ingericht, in zijn huidige vorm niet meer voldoet. Op dit moment bepaalt namelijk de plaats van een device in het interne netwerk, welke systemen vanaf die plaats in het netwerk bereikbaar zijn. Het is een wens van Avans dat ook het autorisatieprofiel/rechtenprofiel/werkprofiel van de gebruiker van een device, dat gekoppeld is aan zijn/haar functie, rol of activiteiten binnen de organisatie, mede bepaalt welke systemen bereikbaar zijn, waardoor meer flexibiliteit wordt gecreëerd.

In dit onderzoek wordt gezocht naar een strategie voor persoonsgebonden toegang. Deze persoonsgebonden toegang gaat worden toegepast op systemen die persoons- of bedrijfsgegevens bevatten, maar wel toegankelijk moeten zijn vanaf elk netwerk binnen Avans, teneinde meer flexibiliteit te creëren. Het eindproduct is een adviesrapport, waarin een advies wordt gegeven over de te volgen strategie met betrekking tot persoonsgebonden toegang.

1.1 - De organisatie

Avans is een onderwijs organisatie ontstaan uit een fusie van de Hogescholen Brabant en 's-Hertogenbosch. Met 7 locaties verdeeld over de steden Breda, Tilburg en 's-Hertogenbosch is het één van de grote Hogescholen van Nederland. Avans biedt 54 verschillende HBO opleidingen in de sectoren Economie en Management, Gezondheid, ICT, Kunst en Vormgeving, Onderwijs, Techniek, Recht en Welzijn. Avans Hogeschool biedt onderwijs aan ongeveer 26.000 studenten en heeft ruim 2500 medewerkers.

Avans is opgebouwd rond een medezeggenschapsstructuur. Avans Hogeschool heeft twee stafeenheden, namelijk het College van Bestuur en de Raad van Toezicht. Deze worden ondersteund door het Bestuur-secretariaat, Stafeenheid Strategisch Beleid en Stafeenheid Beleidsevaluatie en Control. Daaronder bevinden zich de 19 verschillende academies en 5 ondersteunende diensten. In afbeelding 1.1 is het organogram van Avans Hogeschool weergegeven.



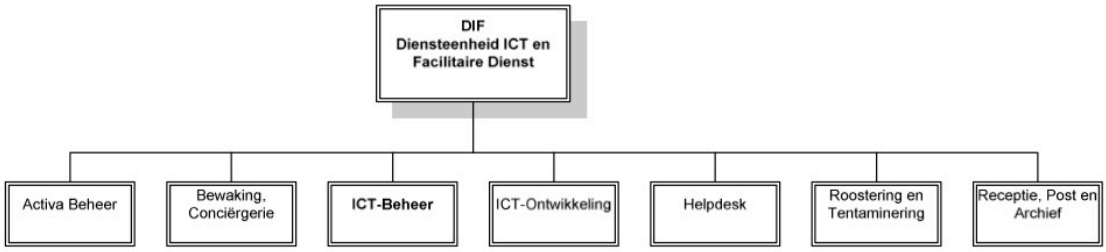
Afbeelding 1.1: Organogram Avans Hogeschool

De Dienst ICT en Facilitair (DIF) is een van de 5 ondersteunende diensten.
DIF is een afdeling die gericht is op de algemene dienstverlening naar de studenten en medewerkers toe. Hierbij valt te denken aan alle ICT gerichte zaken, zoals helpdesk en ICT-beheer, facilitaire zaken zoals bewaking en gebouwenbeheer, roostering en archivering.

De Dienst ICT en Facilitair bestaat uit de volgende subafdelingen:

- Activa Beheer.
- Bewaking en Conciërgerie.
- ICT-Beheer.
- ICT-Ontwikkeling.
- De Servicedesk.
- De Helpdesk.
- Roostering en Tentaminering.
- Receptie, Post en Archief.

In afbeelding 1.2 is de organisatiestructuur van DIF weergegeven.



Afbeelding 1.2: Organogram Dienst ICT en Facilitair

Het onderzoek wordt uitgevoerd bij de afdeling ICT-Ontwikkeling. De afdeling ICT-Ontwikkeling is verantwoordelijk voor onderzoek naar en vernieuwing van ICT voorzieningen voor Avans Hogeschool. Daarnaast zorgt ICT-ontwikkeling ook voor implementatie van deze nieuwe ICT voorzieningen. De projecten die door ICT-Ontwikkeling succesvol worden afgesloten, zullen worden overgedragen aan ICT Beheer.

1.2 - Positie van de student binnen de organisatie

Binnen Avans Hogeschool ben ik vanaf 2005 werkzaam in de ICT. Sinds 1 januari 2011 ben ik werkzaam als netwerkbeheerder bij de afdeling ICT-Beheer van de Dienst ICT en Facilitair. De werkzaamheden van de netwerkbeheerder vinden plaats op alle locaties van Avans. Dit zijn de locaties Breda (Hogeschoollaan, Lovensdijkstraat, Beukenlaan), 's Hertogenbosch (Onderwijsboulevard, Hervenplein) en Tilburg (Cobbenhagenlaan). Hierbij kan men denken aan:

- Het onderhouden en verbeteren van het hogeschool-brede WLAN-netwerk.
- Het beheer van de beide firewalls.
- Het beheren van de vaste netwerkinfrastructuur.
- IP-adres-management.
- Netwerk security.
- Het beheer van IDS/IPS.
- Het monitoren van het netwerk en proactief reageren op gebeurtenissen aan de hand van deze monitoring.

Naast de werkzaamheden bij netwerkbeheer, ben ik ook lid van het Computer Security Incident Response Team (CSIRT) van Avans. Get CSIRT van Avans draagt zorg voor het, met de juiste voortvarendheid, afhandelen van veiligheidsincidenten op het gebied van ICT. Daarnaast is zij het contactadres van Avans met betrekking tot ICT Security Incidenten. Andere taken van het CSIRT:

- Advies geven op het gebied van informatie beveiliging.
- Het dienen als klankbord/adviesorgaan met betrekking tot ingediende Request For Change's (RFC's), lopende projecten of vragen vanuit de interne organisatie.
- Het creëren van bewustwording bij gebruikers en communicatie met gebruikers over ICT beveiliging.
- Dient als crisisteam bij computer gerelateerde beveiligingsincidenten.

Alle beveiligingsincidenten worden geregistreerd in Clientele, zodat de voortgang kan worden bewaakt door de leden van het CSIRT. Aan het hoofd van het CSIRT staat de Security Manager.

2 - Projectbeschrijving

In dit hoofdstuk wordt het onderzoeksproject beschreven zoals deze is uitgevoerd als afstudeeronderzoek van David Schrok. Het afstudeeronderzoek is onderdeel van de studie Systeembeheer Duaal aan de Hogeschool Utrecht.

In dit hoofdstuk wordt beschreven:

- De probleemstelling waarop het afstudeeronderzoek is gebaseerd.
- De doelstellingen van het afstudeeronderzoek.
- De formulering van het afstudeeronderzoek, inclusief afbakening van het project.

Als onderwerp van de afstudeeropdracht is gekozen om onderzoek te doen naar een flexibele en persoonsgebonden manier van toegang voor systemen die bedrijfsgevoelige informatie bevatten. Dit onderzoek bekijkt de mogelijkheden hiertoe en levert een aanbeveling op waarin de mogelijke strategieën voor het geschetste probleem worden beschreven.

2.1 - Probleembeschrijving

Gebruikers worden steeds mobieler. Iedereen heeft een laptop of een ander mobiel device en wil dat gebruiken in hun privé en werksituatie. Dit heet het “Bring-Your-Own-Device” principe. De verwachting van de gebruikers is daarbij dat zij hun werkzaamheden kunnen uitvoeren, onafhankelijk van het gebruikte device en de fysieke manier waarop ze verbinden met het netwerk. Dit strookt echter niet met het huidige, op een gelaagde netwerkstructuur gebaseerde, beveiligingsmodel van Avans. Binnen dit model zijn er twee lagen die bepalen of gebruikers toegang krijgen tot Avans applicaties.

- De positie van een device binnen het netwerk bepaald of toegang verkregen wordt tot de netwerken waarin de systemen met een specifieke applicatie zich bevinden.
- Het gebruikersprofiel bepaald of de gebruikers geautoriseerd zijn voor het gebruik van de betreffende specifieke Avans applicatie.

Gezien het BYOD-principe wil Avans dit gaan flexibiliseren.

Deze wens kan worden gerealiseerd door niet de fysieke plaats van het device in het netwerk, maar het gebruikersprofiel te laten bepalen of toegang tot de netwerken met een specifieke applicatie wordt toegestaan. In het vervolg wordt dit persoonsgebonden toegang genoemd. Daarbij wordt er ook onderzocht of de status van het apparaat (virusscanner, patches enzovoort) en de fysieke locatie als extra criteria voor het wel of niet beschikbaar stellen van Avans applicaties kunnen worden meegenomen. Bij de authenticatie wordt op beperkte schaal gebruik gemaakt van sterke authenticatie. Hier is al onderzoek naar gedaan binnen Avans.

2.2 - Doelstellingen

De doelstellingen van het onderzoek zijn als volgt:

- Het verschaffen van inzicht naar mogelijkheden om persoonsgebonden toegang tot bepaalde services/netwerken te verlenen, met reeds aanwezige technieken. Binnen het onderzoek wordt gekeken naar methoden voor persoonsgebonden toegang die reeds binnen Avans aanwezig zijn, maar nog niet worden gebruikt.
- Beter benutten van de bestaande infrastructuur.
- Het beter en flexibel beveiligen van systemen die persoons- of bedrijfsinformatie bevatten.

2.3 - Opdrachtformulering

Het onderzoek richt zich op de mogelijkheid om persoonsgebonden toegang tot bepaalde services/netwerken te verlenen

In het onderzoek worden de volgende onderdelen behandeld:

1. Beschrijving van het huidige interne beveiligingsmodel van Avans.
2. Inventarisatie van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang en waarbij dit ook gewenst is.
3. (Literatuur)Onderzoek en inventarisatie van de strategieën om persoonsgebonden toegang te realiseren op basis van de beschikbare infrastructuur van Avans.
4. Beoordelen en evalueren over de bij punt 3 genoemde mogelijkheden.
5. Adviseren van de strategieën die gebruikt zou kunnen worden voor persoonsgebonden toegang bij Avans.
6. Advies uitbrengen met betrekking tot wijzigingen in het beveiligingsbeleid die voort kunnen komen uit een implementatie van de gekozen strategie.
7. Onderzoek naar de gevolgen voor ICT-beheer in geval van een implementatie van de aanbevolen strategie.
8. Deze strategie toetsen op een bestaande situatie waarbij flexibele persoonsgebonden toegang is gewenst.

Buiten de scope van dit onderzoek vallen de volgende onderwerpen:

1. Onderzoek naar vormen van sterke authenticatie of de manier waarop sterke authenticatie wordt toegepast binnen Avans.
2. Er wordt geen nieuw beveiligingsmodel voor Avans ontwikkeld.
3. Er wordt binnen het onderzoek geen nieuwe apparatuur of software geïntroduceerd.
4. De juridische aspecten die nodig zijn voor de implementatie van de gekozen oplossing.
5. De (sterkere) beveiliging van web-gebaseerde diensten; dit is al gerealiseerd.

Het onderzoek is uitgevoerd conform het Plan van Aanpak. Deze is opgenomen in Bijlage 1.

3 - Huidige Beveiligingsmodel Avans

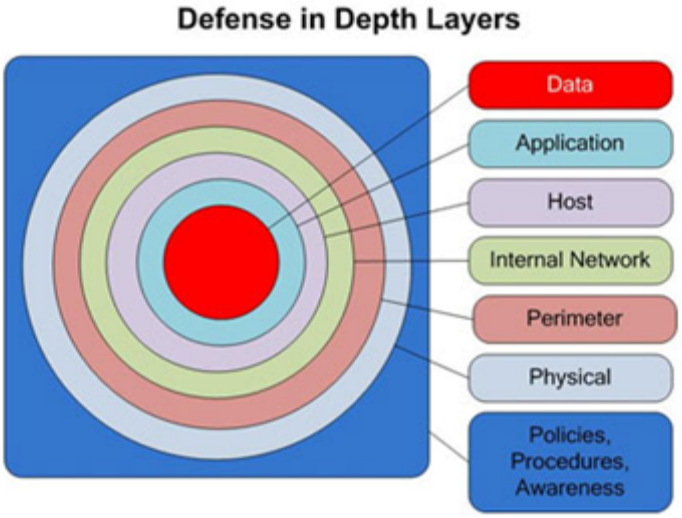
Dit hoofdstuk beschrijft het huidige netwerk- en beveiligingsmodel van Avans. Hierbij wordt de opbouw en de beveiliging van het netwerk beschreven, waarbij de volgende onderwerpen worden behandeld:

- Beveiligingsmodel van Avans.
- Welke netwerkgroepen er bij Avans aanwezig zijn.
- Welke gebruikersgroepen er bij Avans aanwezig zijn.
- Welke beveiligingsvlakken er bij Avans aanwezig zijn.
- Welke authenticatie/autorisatiemiddelen er aanwezig zijn.
- Hoe de onderlinge relaties vormgegeven zijn tussen deze groepen en middelen.

De beschrijving van het huidige beveiligingsmodel vormt de basis en het uitgangspunt voor het onderzoek.

3.1 - Beveiligingsmodel Avans

Het netwerk van Avans is gebaseerd op het "Defense-In-Depth" beveiligingsmodel. Dit model is oorspronkelijk afkomstig uit militaire toepassingen en wordt tegenwoordig voor een groot aantal zaken toegepast, waaronder de beveiliging van netwerken.



Afbeelding 3.1 – Overzicht van "Defense in Depth" lagen(1).

"Defense in Depth" is gebaseerd op het toepassen van een gelaagde beveiligingsstructuur. Het doel van deze structuur is niet direct het optimaal beveiligen van de systemen, maar het aanzienlijk vertragen van mogelijke aanvallen. In de praktijk van netwerkbeveiliging komt dit neer op het introduceren van verschillende netwerken die afzonderlijk van elkaar beveiligd zijn. Het meest bekende voorbeeld is: "Internet -> DMZ -> Intranet". Hierbij zijn er drie lagen gecreëerd waar tussen verschillende vormen van beveiliging worden toegepast. Een aanvaller vanuit het internet dient in eerste instantie toegang te verkrijgen tot het perimeternetwerk, de "demilitarized zone" (DMZ), om vervolgens tegen de beveiliging tussen de DMZ en het intranet als nieuw obstakel aan te lopen. De kracht achter het "Defense in Depth" model is dat men niet in staat is om meerdere lagen te overbruggen. Men mag enkel communiceren met de eerstvolgende laag in het model, zonder een stap van meerdere lagen te maken.

Het aantal lagen dat wordt toegepast kan per toepassing verschillen en is afhankelijk van de mate van noodzakelijke beveiliging. Het toepassen van het "Defense in Depth" model in het netwerk van Avans biedt een verhoogde mate van beveiliging en introduceert meer tijd om te kunnen reageren op een beveiligingsaanval.

Naast het toepassen van het "Defense in Depth" model op het netwerk van Avans, worden servers binnen Avans beveiligd door middel van "Host Hardening" en een eigen client firewall. "Host Hardening" omvat het uitschakelen van onnodige services en applicaties op het doelsysteem. Hierdoor worden de niet noodzakelijke poorten op het systeem afgesloten, zodat het aanvalsoppervlak van het systeem kleiner wordt. De client firewalls zijn in vrijwel alle gangbare besturingssystemen te vinden, of kunnen als extra component worden geïnstalleerd. Het voordeel van deze client firewalls is dat deze volledig integreren met de softwarecomponenten op het systeem. Hierdoor is het vrij eenvoudig om deze oplossingen toe te passen, zonder dat dit tot extra beheer zal leiden. Net als de hardening van de systemen, zal ook de client firewall bijdragen aan het verkleinen van het aanvalsoppervlak. Bij deze aanpak wordt gebruik gemaakt van het "Host Hardening" principe, wat inhoud dat alleen die services door de firewall worden toegelaten die nodig zijn voor het ontsluiten van de applicatie of service, welke op de server wordt gehost. De serverbeheerder en applicatiebeheerder zijn samen verantwoordelijk voor de "Host Hardening". Alle servers worden getoetst op "Host Hardening" middels detectiesoftware die binnen Avans aanwezig is. Binnen Avans wordt Nessus[2] gebruikt.

3.2 - De netwerken

Het netwerk van Avans is opgedeeld in verschillende kleinere netwerken, welke allen een eigen functie hebben. Daarnaast is Avans gekoppeld aan het internet. De opdeling van het interne netwerk geschied middels het "Virtual Local Area Network" (VLAN)-principe.

De techniek en de principes achter VLAN's zijn samengevat in de 801.1Q standaard[3]. VLAN's worden met name toegepast in grote netwerkomgevingen, waarbij men een logische scheiding in netwerken wil realiseren, ook wel segmentatie genoemd. Het reguleren van het verkeer tussen de VLAN's geschiedt middels Access-Control-Lists (ACL). Een ACL is een lijst opgebouwd uit regels waarin staat gedefinieerd waar een netwerk wel of geen toegang toe heeft. De ACL's worden binnen Avans toegepast op alle netwerken waar gebruikers in worden geplaatst of netwerken die geheel moeten worden afgeschermd. De ACL's worden geïnstalleerd op de core-routers en building concentrators van Avans.

Aan een VLAN kan een ip-adresreeks worden toegekend. Bij Avans is het zo opgezet dat een VLAN hetzelfde nummer krijgt als het derde octet van de ip-adresreeks van dat VLAN. Bijvoorbeeld: VLAN 10 heeft ip-adresreeks 145.48.10.0/24. Avans heeft de netwerkreeks 145.48.0.0/16 ter beschikking gekregen, welke is onderverdeeld in de kleine functionele netwerken.

3.2.1 - De gebruikersnetwerken

Gebruikersnetwerken zijn netwerken waarin hardware is geplaatst die door gebruikers wordt gebruikt. In elk gebouw van Avans zijn de gebruikersnetwerken apart gedefinieerd. Binnen Avans zijn de volgende gebruikersnetwerken aanwezig, welke worden afgeleid uit de gebruikersgroepen die aanwezig zijn binnen Avans:

- Studenten: Studenten werken zowel op beheerde werkstations als op eigen devices. De beheerde werkstations worden in de studentennetwerken geplaatst. Deze Studentennetwerken mogen alleen bij de Algemene en DMZ-netwerken komen. De eigen devices maken gebruik van de WLAN omgeving en worden als onveilig beschouwd.
- Medewerkers en docenten: Medewerkers werken zowel op beheerde werkstations als op eigen devices. De beheerde werkstations worden in de medewerkersnetwerken geplaatst. Deze medewerkersnetwerken mogen bij de Algemene, BedrijfsProcessen en DMZ-netwerken komen. De eigen devices maken gebruik van de WLAN omgeving en worden als onveilig beschouwd.
- Helpdesk personeel: Helpdeskpersoneel werken vooral op beheerde werkstations, maar ook op eigen devices. De beheerde werkstations worden in de helpdesknetwerken geplaatst. Deze helpdesknetwerken zijn vrijwel gelijk aan de medewerkersnetwerken, aangevuld met taakspecifieke toegang. De eigen devices maken gebruik van de WLAN omgeving en worden als onveilig beschouwd.
- Beheerders: Beheerders werken zowel op beheerde werkstations als op eigen devices. De beheerde werkstations van beheerders worden in de beheernetwerken geplaatst. Het beheerdersnetwerk heeft overal vrije toegang tot het gehele netwerk. De eigen devices maken gebruik van de WLAN omgeving en worden als onveilig beschouwd.

- Iedereen: Alle gebruikersgroepen mogen gebruik maken van de WLAN netwerken. In deze netwerken komen alle gebruikersgroepen samen, waarbij dan voornamelijk gebruik wordt gemaakt van eigen devices. Deze netwerken worden als onveilig aangemerkt.

Op alle gebruikersnetwerken worden access-control-lists toegepast, waarbij het netwerk waarin vreemde onbeheerde apparatuur is geplaatst (WLAN), de minste toegang geeft binnen Avans. Het netwerk waarin beheerde werkstations worden geplaatst, hebben steeds meer toegang binnen Avans, afhankelijk van in welk gebruikersnetwerk het beheerde werkstation is geplaatst.

3.2.2 - Servicenetwerken

De servicenetwerken zijn de netwerken waarin de services en applicaties van Avans zijn ondergebracht. De servicenetwerken zijn intern via ACL's beveiligd en van buitenaf door een firewall. Avans heeft de volgende service netwerken:

- DMZ : In dit netwerk staan services die gericht zijn op het gebruik vanaf het internet. Deze services zijn vrijwel altijd publiekelijk beschikbaar. Voorbeelden van services zijn DNS en publieke websites.
- Algemene services (AL): Services in dit netwerk zijn beschikbaar voor alle gebruikers van Avans. Meestal zijn deze services ook vanaf extern (geauthentiseerd) beschikbaar. Voorbeelden van services in dit netwerk zijn de Elektronische Leer Omgeving (ELO).
- BedrijfsProces Services (BP): De diensten in dit netwerk zijn gericht op de medewerkers (docenten, ondersteuners) van Avans. Deze zijn alleen vanaf het Avans-netwerk bereikbaar, of met versterkte authenticatie vanaf het internet. Voorbeelden: Callregistratiesysteem.
- Facilitaire hosts (FH): De services in dit netwerk worden alleen gebruikt door andere services. Deze services worden dus nooit rechtstreeks door (eind)gebruikers aangesproken. Voorbeelden: Databases, Enterprise Service Bus.
- Overige netwerken: De overige client netwerken zijn netwerken waarin hardware wordt geplaatst die niet in bovenstaande netwerken behoort. Voorbeelden hiervan zijn netwerken voor lab-apparatuur, telefonie, multifunctionals en gebouwbeheersystemen.

3.2.3 - Internet

Avans heeft een koppeling met Internet. Tussen het internet en het interne netwerk van Avans is een zogenoemde hard-boundry aanwezig in de vorm van een firewall. De firewall is een zone-based firewall waarop drie zones aanwezig zijn:

- Intern: De zone intern is de zone waarin zich het interne netwerk van Avans bevindt.
- DMZ: De zone DMZ is de zone waarin zich de DMZ services en applicaties zich bevinden.
- Internet: Aan deze zone zit de internet-feed van Avans gekoppeld.

De firewall reguleert het verkeer tussen de drie genoemde zones.

Binnen Avans mogen alle gebruikers- en servicenetwerken een verbinding opzetten naar Internet. Uitgezonderd zijn een aantal netwerken die geen verbinding met internet hoeven te hebben voor correct functioneren of waar dit niet gewenst is. Voorbeelden hiervan zijn de printernetwerken en de gebouwbeheernetwerken.

Vanuit internet bepaald de firewall welke connecties mogen worden opgebouwd en wat wordt geblokkeerd. Vanaf Internet mogen er via de firewall twee netwerken rechtstreeks worden benaderd:

- DMZ-netwerk: In dit netwerk staan servers die een front-end vormen voor service/applicaties die zich in het interne netwerk bevinden.
- AL-netwerk: In dit netwerk staan algemene resources die door iedereen, na authenticatie aan de betreffende service/applicatie, mogen worden gebruikt.

Voor de services/applicaties in deze zones die vanaf internet benaderbaar zijn, worden alleen die ip-poortnummers vrijgegeven die nodig zijn voor het correct functioneren van de services/applicaties. Dit wordt gewaarborgd door de firewall beheerders en de security-manager.

3.3 - Beveiligingsvlakken

Tussen de verschillende client- en servicenetwerken van Avans zijn beveiligingsvlakken aangebracht die de beveiliging tussen de verschillende netwerken controleert. Binnen Avans zijn dit de volgende beveiligingsvlakken:

- ACL's in de core-routers: De ACL's regelen het interne netwerkverkeer tussen de verschillende interne client- en servicenetwerken. De ACL's zijn op dit moment het belangrijkste interne beveilingsvlak dat binnen Avans aanwezig is. Buiten de beveiliging van de ACL's vallen de DMZ- en internetzone.
- Policies op de firewall: De firewall regelt het verkeer tussen de zones Internet, DMZ en het intern netwerk en kan dus worden gezien als perimiter-beveliging. Waar de ACL's zich beperken tot hele netwerkranges die worden toegestaan of geblokkeerd, is de firewall specifieker en worden in de policies ook de beveiliging van specifieke serverobjecten beheerd.
- Acces-gateways: Verzorgen de authenticatie en autorisatie van webapplicaties en webservices. De access-gateways beperken zich tot de beveiliging van webservices en webapplicaties.

De verschillende beveiligingsvlakken verschillen in scope en toepasbaarheid. Waar in de ACL's toegang van en tot interne netwerken is geregeld, wordt in de firewall de toegang van en naar het internet en van en naar de DMZ geregeld en verzorgen de access-gateways de toegang tot de diverse webapplicaties en webservices. De verschillende beveiligingsvlakken zijn gescheiden en onafhankelijk van elkaar.

3.4 - Authenticatie en autorisatie

Voor authenticatie en autorisatie zijn er binnen Avans een aantal systemen en protocollen die worden toegepast. Dit zijn:

- Microsoft Active Directory (AD): Microsoft Active Directory is binnen Avans de standaard geworden, waartegen geauthenticeerd wordt in de beheerde omgevingen van Avans. Dit houdt in dat beheerde servers, zowel Linux als Windows servers, gekoppeld zijn aan de AD.
- Novell eDirectory: De eDirectory van Novell wordt gebruikt voor de authenticatie op systemen die op Novell technologie zijn gebaseerd, bijvoorbeeld Groupwise. Ook de services die van LDAP gebruik maken, worden tegen de eDirectory geauthenticeerd. Ook is de Active Directory van Avans gekoppeld aan de eDirectory.
- Radius: Radius wordt binnen Avans gebruikt voor authenticatie en toegang tot hardware en (web)applicaties, zoals bijvoorbeeld Osiris.
- 802.1X: Dit op Radius gebaseerde protocol wordt gebruikt om toegang tot de WLAN omgeving te realiseren.
- SAML2 via de Access Gateways: SAML2 wordt gebruikt om Single Sign-on te realiseren voor de meeste webapplicaties. Dit houdt in dat een gebruiker niet opnieuw op de betreffende webapplicatie hoeft in te loggen als:
    - de gebruiker via single sign-on al een keer is ingelogd op de access-manager omgeving.
    - de gebruiker is ingelogd via een beheerd werkstation.

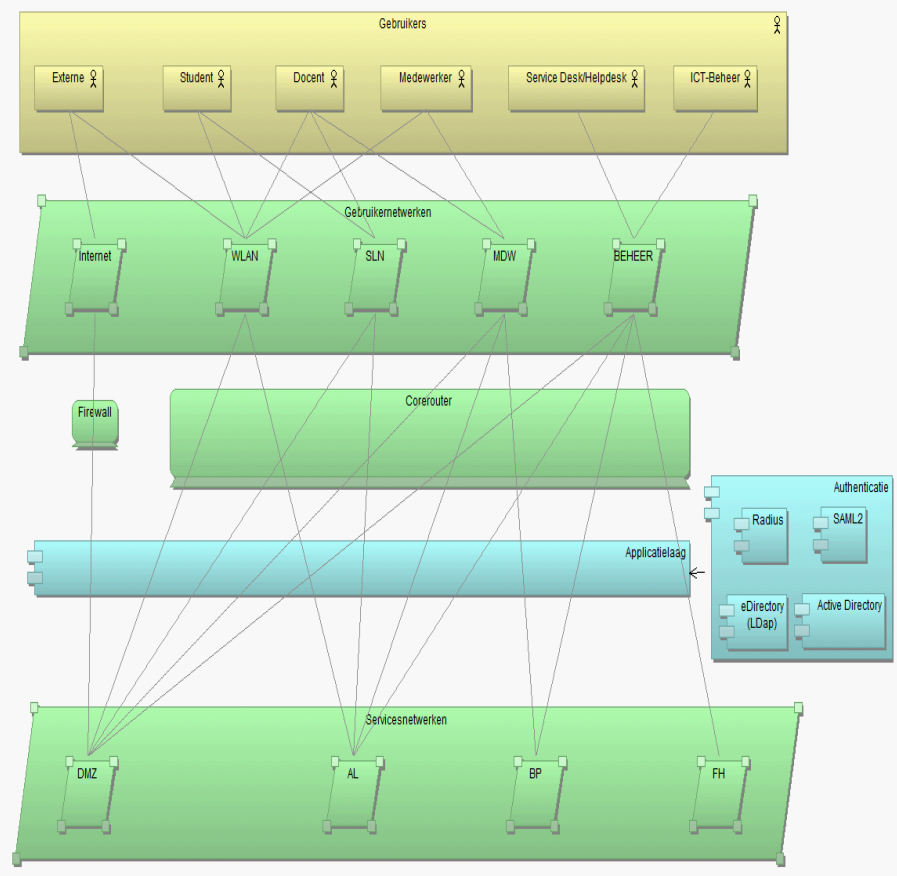
Met deze authenticatie en autorisatie systemen zal in het afstudeeronderzoek rekening moeten worden gehouden. De gekozen oplossing dient te kunnen integreren met de bestaande authenticatie en autorisatie systemen.

3.5 - Netwerkarchitectuur

Om een duidelijk beeld te krijgen van de logische opbouw van het netwerk, is er met behulp van het softwarepakket BizzDesign Architect[4], een architectuur tekening gemaakt gebaseerd op de architectuurstandaard Archimate[5]. Deze architectuur tekening is te vinden in afbeelding 3.2.

In afbeelding 3.2 zijn de verschillende lagen afgebeeld die zich in het netwerk bevinden, evenals de gebruikers en de koppelingen naar de verschillende netwerken.
In het gele vlak zijn de diverse gebruikers afgebeeld, die zijn gekoppeld aan verschillende gebruikersnetwerken. De diverse gebruikersnetwerken zijn beschreven in paragraaf 3.2.1.

De diverse gebruikersnetwerken worden gekoppeld c.q. gescheiden met behulp van de netwerkcomponenten (core-switches). Deze hardware vormt daarmee de beveiligingsgrens tussen de diverse gebruikers- en servicenetwerken. De servicenetwerken zijn beschreven in paragraaf 3.2.2.



Afbeelding 3.2 - Architectuurmodel netwerk Avans Hogeschool[6].

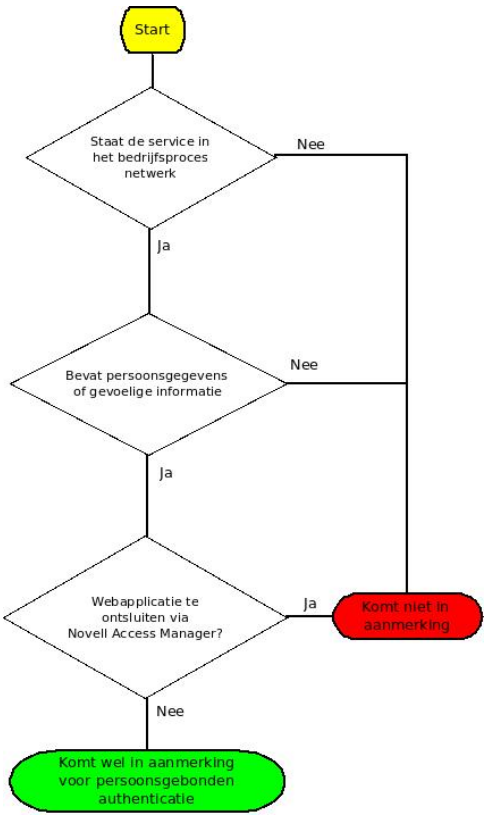
In afbeelding 3.2 is ook te zien wat de kern is van het probleem dat dient te worden opgelost. Om dit te illustreren zal gebruik worden gemaakt van een voorbeeld:

Gekozen is de gebruikersgroep medewerkers. Op een beheerd werkstation van Avans zal de betreffende medewerker zich in het medewerkers-netwerk bevinden en toegang hebben tot de servicenetwerken DMZ, AL en BP. Als dezelfde medewerker met een eigen device (BYOD-principe bijvoorbeeld) zich op het WLAN-netwerk bevind, heeft de medewerker enkel toegang tot de servicenetwerken DMZ en AL. De medewerker zal dan een beperking ondervinden op wat hij kan en mag. Indien de medewerker in de huidige situatie wel bij het BP-netwerk zou mogen, ervaart de gebruiker geen belemmering, maar is er geen vorm van controle van wat de gebruiker op dat BP-netwerk doet en naar welke services/applicaties hij probeert te verbinden, ongeacht of de medewerker daartoe gemachtigd is.

4 - Applicatie Inventarisatie

Dit hoofdstuk beschrijft een inventarisatie van de applicaties binnen Avans die in aanmerking kunnen komen voor persoonsgebonden toegang.

De applicaties die zeker in de selectie voor dienen te komen zijn applicaties die zich in het bedrijfsprocessen netwerk bevinden en persoons- of bedrijfsgegevens bevatten. Deze servers in dit netwerk zijn nu benaderbaar door alle medewerkers van Avans. Het persoonsgebonden afschermen van deze servers verhoogt de beveiliging van deze kritische systemen. Applicaties die niet in aanmerking komen binnen deze selectie zijn (web)applicaties die worden ontsloten via de Novell Access Manager en applicaties waar persoonsgebonden toegang niet gewenst is. Dit is in afbeelding 4.1 zichtbaar.



Afbeelding 4.1 - Flowchart voor applicatieselectie

Door het bepalen van het type en soort applicatie dat met de onderzochte strategieën wordt ontsloten, wordt duidelijk welke eisen en wensen er gesteld dienen te worden aan de te kiezen strategieën voor persoonsgebonden authenticatie/autorisatie. De techniek van de gekozen strategieën dient toepasbaar te zijn op de selectie van applicaties die in aanmerking komen voor persoonsgebonden toegang.

In tabel 4.1 wordt een overzicht gepresenteerd van de betreffende applicaties. Er wordt niet gestreefd naar een compleet overzicht, maar naar enkele voorbeelden die ontsloten kunnen gaan worden met de gekozen strategieën voor persoonsgebonden toegang. De genoemde applicaties worden toegelicht in wat voor soort applicatie het is en met welke technieken er rekening dient te worden gehouden voor de ontsluiting van deze applicatie. Een omschrijving van de applicaties is te vinden in bijlage 3.

Naam	Doelgroep	Netwerk	Omschrijving	Toegangsrestricties	Probleem	Karakteristieken autorisatie/authenticatie
Clientele	Medewerkers Helpdesk en Beheer	BP	Callmanagement	Alleen toegankelijk voor de doelgroep.	Niet alle medewerkers zijn geautoriseerd, maar kunnen wel bij de resources.	Client-server applicatie. AD authenticatie. Autorisatie binnen de applicatie
Osiris	Studenten Docenten en Administratief Medewerkers	AL+BP	Studievoortgang	Verschillende doelgroepen met verschillende autorisatieniveaus.	Studenten mogen alleen inzien, enkele medewerkers mogen ook invoeren.	Client-server applicatie (via Java-applet). LDAP authenticatie
Corsa	Budgethouders Beheerders eindgebruikers	BP	Factuurstromen	Verschillende doelgroepen met verschillende autorisatieniveaus.	Niet alle medewerkers zijn geautoriseerd, maar kunnen wel bij de resources. Bevat financiële gegevens.	Client-server applicatie. Ldap authenticatie. Eigen database. Rollen worden handmatig toegekend.
Untis	Roosterbureau	BP	Roostering	Alleen toegankelijk voor de doelgroep.	Niet alle medewerkers zijn geautoriseerd, maar kunnen wel bij de resources. Geen authenticatiemechanisme.	Lokale applicatie met database-communicatie. Geen authenticatie/autorisatie.
Superoffice	DMCS secretariaten externen	BP	CRM	Verschillende doelgroepen met verschillende autorisatieniveaus. Externen alleen via web, lokale authenticatie.	Niet alle medewerkers zijn geautoriseerd, maar kunnen wel bij de resources.	Client-server applicatie. Active Directory authenticatie. Externe partijen authenticeren tegen een lokale database in Superoffice. Eigen autorisatie.
PICA LBS4	Medewerkers LIC	Extern	Bibliotheek-systeem voor uitleen en indexering.	Alleen toegankelijk voor de doelgroep. Geen verschil in autorisaties.	Niet alle medewerkers zijn geautoriseerd, maar kunnen wel bij de resources. Server staat extern.	Client-server applicatie. Lokale userdatabase. Wordt ook gebruikt door 'hardware'.

Tabel 4.1: Applicatie Selectie overzicht.

De afkortingen die in de tabel voor de diverse netwerken gebruikt zijn, zijn terug te vinden in hoofdstuk 3, waarin het huidige beveiligingsmodel van Avans is beschreven.

5 - Onderzoek naar strategieën voor persoonsgebonden toegang

Dit hoofdstuk beschrijft het onderzoek dat is uitgevoerd naar gangbare technieken voor persoonsgebonden toegang die toepasbaar zijn op de gestelde probleemomschrijving. Om gericht te kunnen zoeken naar deze gangbare technieken dient eerst vast te staan welke strategieën er kunnen worden gehanteerd. Door het vaststellen van de strategieën wordt een afbakening gecreëerd voor de toepassing van de in de literatuur omschreven technieken voor persoonsgebonden authenticatie en autorisatie. Met literatuur worden bronnen bedoeld zoals informatie van de fabrikant, gerenommeerde bronnen zoals de databanken waarop de Hogeschool Utrecht is geabonneerd[12] en publicaties die over het onderwerp zijn gevonden op internet.

Vanuit de strategieën wordt beschreven welke technieken aansluiten of toepasbaar zijn. Daarna wordt een inventarisatie gemaakt van de technieken die binnen Avans aanwezig zijn. Aan de hand van de bij Avans aanwezige technieken wordt een selectie gedaan naar de aanbevolen strategie met de bijbehorende technieken. Hier zal vervolgens een voorbeeld uitwerking van worden geschetst, zoals de strategie in de praktijk zou kunnen gaan functioneren.

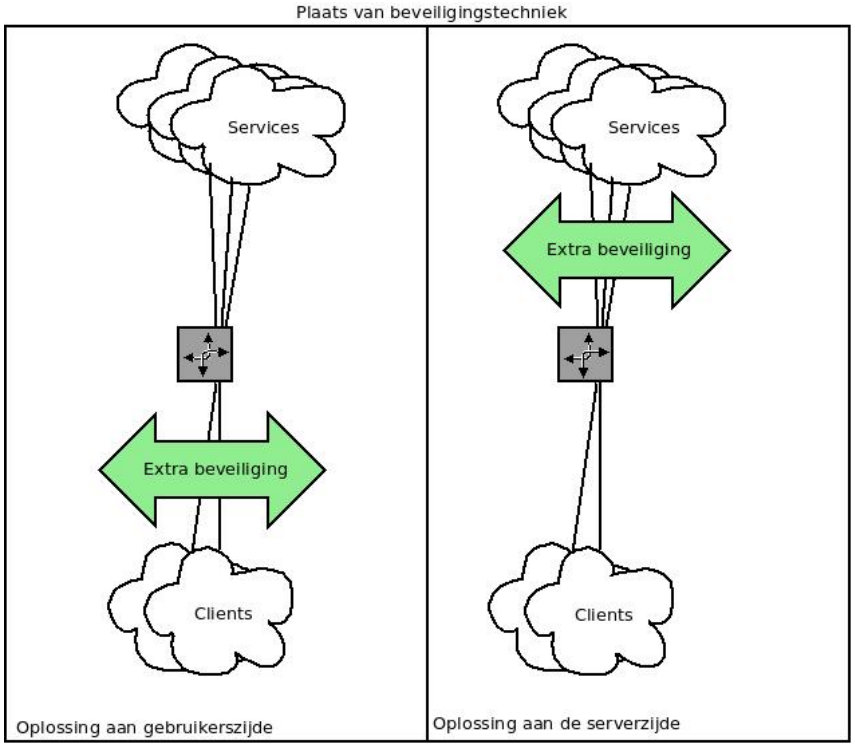
Bij het uitwerken van de strategieën is de plaatsing van de techniek van belang. Uit het onderzoek in de literatuur komt naar voren dat dit voornamelijk gebeurt door techniek toe te passen op de gebruikers-zijde van het netwerk, of aan de serverzijde van het netwerk. Gevonden oplossingsrichtingen/strategieën zijn hierbij:
Plaatsing van de techniek aan de serverzijde:

- Servers in afgeschermd netwerk, dynamische ACLs aan de gebruiker koppelen.
- Servers in afgeschermd netwerk, afgeschermd en getunneld netwerkverkeer.

Plaatsing van de techniek aan de clientzijde:

- Clients controleren voordat toegang wordt verleend.
- Verplaatsen van clients in netwerken na authenticatie en toekennen van een persoonsgebonden ACL.

Op welke wijze een techniek geplaatst kan worden is weergegeven in afbeelding 5.1.



Afbeelding 5.1 – De invloed van het plaatsen van de beveiligingsstrategie

De techniek kan tussen de gebruikers en het netwerk worden geplaatst of vóór de services/applicaties. Het plaatsen van de techniek tussen de gebruikers en het netwerk heeft als gevolg dat er acties worden uitgevoerd op alle gebruikers. Het plaatsen van de techniek vóór de services/applicaties heeft gevolgen voor de services/applicaties en wordt de beveiliging uitgevoerd op het moment dat een gebruiker een service/applicatie wil benaderen. De plaatsing van de techniek wordt bij elke strategie gemotiveerd. Ook de gevolgen van de plaatsing van de techniek worden in kaart gebracht.

5.1 - Kaders en randvoorwaarden

In de afstudeeropdracht is gesteld dat de geadviseerde strategie moet zijn opgebouwd uit technieken die reeds binnen Avans aanwezig zijn. Door deze stelling staan de fabrikanten voor de technieken die gebruikt gaan worden in de strategieën, vast. De belangrijkste fabrikanten waarvan wordt verwacht dat deze de techniek kunnen leveren die zou kunnen worden gebruikt binnen de strategieën, worden hieronder genoemd:

- Cisco: Alle netwerkcomponenten voor het vaste netwerk van Avans, met uitzondering van de firewalls, zijn van Cisco.
- Novell: De authenticatie en autorisatie oplossing Novell Access Manager is reeds aanwezig bij Avans. Daarnaast maakt Avans gebruik van Novell eDirectory. Indien er servers worden ingericht op Linux, dan wordt er gebruik gemaakt van Novell SUSE Linux.
- Microsoft: Een gedeelte van de serversystemen van Avans zijn voorzien van het besturingssystemen van Microsoft.
- Palo Alto: De firewalls van Avans zijn van deze fabrikant.
- Juniper Networks: Avans heeft de WLAN oplossing van Trapeze/Juniper. Juniper is een netwerk partner, die naast WLAN ook actief is in de security, routing en switching markt.

Door het beschrijven van de strategieën wordt er een afbakening gecreëerd voor de te gebruiken technieken. Over de technieken die toepasbaar zijn in een strategie zal kennis moeten worden opgedaan door informatie welke wordt verstrekt door de fabrikant/leverancier.

Bij elke strategie wordt ook een inschatting gemaakt of deze kan worden ingevoerd in het huidige beveiligingsmodel van Avans, of welke aanpassingen daar voor nodig zouden zijn. De beschrijving van de strategie kan ook inzicht geven in hoeverre de gestelde probleemstelling wordt opgelost.

5.2 - Beoordelingscriteria voor de gevonden strategieën

Om te controleren of een strategie voldoet aan de gestelde eisen en wensen van Avans, worden er beoordelingscriteria voor de gevonden strategieën vastgesteld. Elke uitgewerkte strategie wordt beoordeeld op de volgende punten:

- Kan de strategie volgens het beveiligingsmodel van Avans geïmplementeerd worden?
- Kan de strategie gerealiseerd worden met binnen Avans beschikbare techniek?
- Bied de strategie een volledige oplossing voor de probleemstelling?
- Is extra aanschaf (hardware/licenties) nodig?
- Is de strategie eenvoudig (transparant) voor eindgebruikers en beheerders?
- Is de strategie toepasbaar op gangbare end-user devices?
- Heeft de strategie een hoge of lage geschatte beheerlast?

De beschreven strategieën worden getoetst op de beoordelingscriteria. Aan de hand van deze toetsing zal een strategie worden aanbevolen.

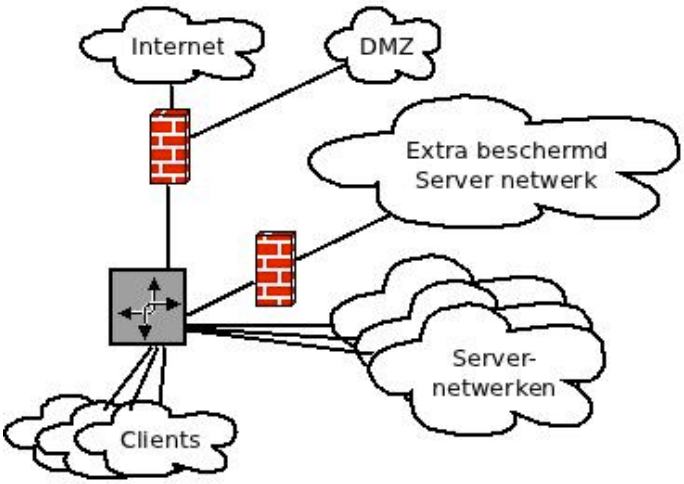
5.3 - Uitwerking strategieën

In deze paragraaf worden de gangbare strategieën uit de literatuur beschreven voor persoonsgebonden toegang, die een extra laag van beveiliging creëren voor het beveiligen van services/applicaties die in aanmerking komen voor persoonsgebonden toegang. Zoals in hoofdstuk 4 staat beschreven, zijn de applicaties die zeker in de selectie voorkomen, applicaties die zich in het bedrijfsprocessen netwerk bevinden en persoons- of bedrijfsgegevens bevatten. Het persoonsgebonden afschermen van deze servers verhoogd de beveiliging van deze kritische systemen. In de volgende paragrafen zijn de in de literatuur gevonden oplossingsrichtingen/strategieën uitgewerkt die zijn gebaseerd op de volgende gangbare methodieken voor beveiliging:

- Servers in afgeschermd netwerk, dynamische ACLs aan de gebruiker koppelen[13].
- Servers in afgeschermd netwerk, afgeschermd en getunneld netwerkverkeer[13,14,17,18,19,20].
- Clients controleren voordat toegang wordt verleend[21,22,23].
- Verplaatsen van clients in netwerken na authenticatie[24,25].

5.3.1 - Afgeschermd servernetwerk

Bij deze strategie worden services/applicaties die in aanmerking komen voor persoonsgebonden toegang in een apart servernetwerk geplaatst. Het aparte servernetwerk is niet direct benaderbaar, maar wordt afgeschermd van de gebruikersnetwerken door het toevoegen van een firewall als extra tussenlaag. In dit geval is dat een hard-boundry, in plaats van een soft-boundry, waarmee in dit geval een ACL wordt bedoeld. Hiermee wordt het netwerkmodel waarop het netwerk van Avans is opgezet, het 'Defense in Depth-model', in stand gehouden. Het ontwerp van deze strategie is te vinden in afbeelding 5.2.

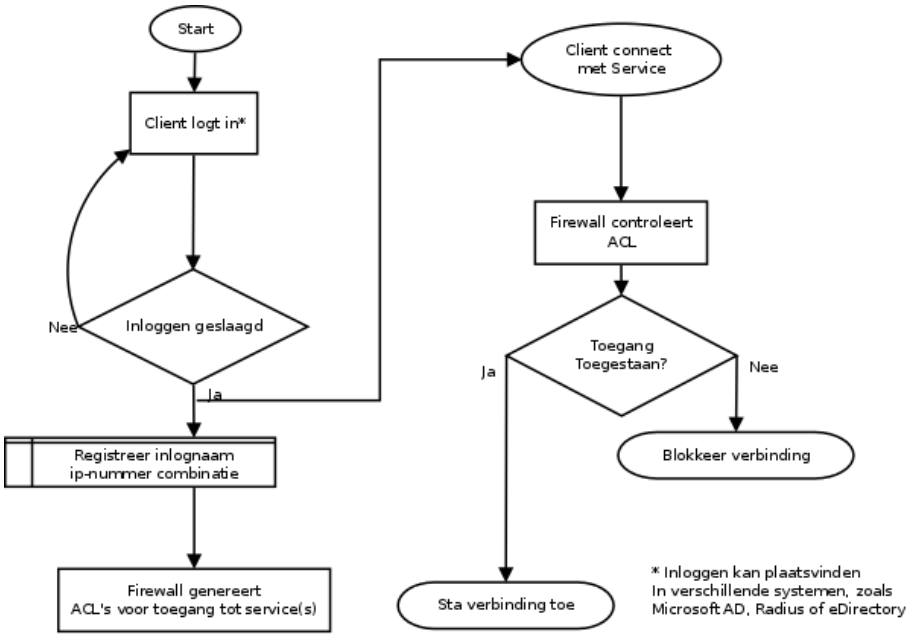


Afbeelding 5.2 – Ontwerp van de strategie afgeschermd servernetwerk.

Dit servernetwerk wordt voorzien van strikte en persoonsgebonden toegangscontrole. Pas na authenticatie/autorisatie wordt de toegang van de gebruiker tot de service/applicatie toegestaan. Voor dit netwerk geldt het deny-unless principe, wat inhoudt dat niemand kan verbinden naar dit netwerk, tenzij daar specifiek toegang voor is verleend.

5.3.1.1 - Technische beschrijving

Zoals in de vorige paragraaf is beschreven, wordt in deze strategie een firewall geplaatst tussen de gebruikers en de te beschermen services/applicaties. Deze firewall zorgt voor de afscherming en bescherming van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, maar tevens voor de authenticatie. Hiervoor is het nodig dat de firewall, naast het kunnen reguleren van het verkeer, kan worden gekoppeld aan de bestaande authenticatie mechanismen. Door het koppelen van de authenticatie mechanismen aan de firewall kunnen gebruiker/ip-adres koppelingen worden bijgehouden. Op basis van deze gebruiker/IP-adres koppeling wordt door de firewall een persoonlijke en dynamische access-control list gemaakt, welke bepaald tot welke services/applicaties de gebruiker toegang heeft. De flow van dit proces is weergegeven in afbeelding 5.3.



Afbeelding 5.3 – flowschema van het authenticatieproces.

Een gebruiker/IP-adres koppeling komt tot stand doordat een gebruiker op een moment authenticeert aan het netwerk en hij daarbij een IP-adres gebruikt of na authenticatie krijgt toegewezen. Wanneer beide gegevens worden gekoppeld, ontstaat een gebruiker/IP-adres koppeling. Op de tussenliggende firewall staan de firewall regels per gebruiker ingesteld. Op het moment dat de gebruiker/IP-adres mapping gereed is, kan een voor de gebruiker specifiek gegenereerde access-control-list (ACL) aan het door de gebruiker gebruikte IP-adres worden gekoppeld en krijgt hij al dan niet toegang tot de service/applicatie. Het maakt daarbij niet uit vanaf welk gebruikersnetwerk de betreffende gebruiker komt. Hij is op dat moment geauthenticeerd en geautoriseerd om de betreffende service/applicatie te benaderen.

Naast persoonsgebonden toegang, kan controle van de beveiligingsstatus van een end-user device gewenst zijn voor de bescherming van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang. Dit kan worden gerealiseerd door een antivirus/anti-malware appliance op de netwerk laag toe te voegen. In een moderne firewall waarmee op gebruikersniveau verkeer kan worden gereguleerd, kan ook gebruik worden gemaakt van antivirus en anti-malware mogelijkheden welke aanwezig zijn op de firewall.

5.3.1.2 - Toepasbaarheid binnen Avans

Binnen deze strategie wordt een firewall ingezet als technische oplossing, welke over de volgende functionaliteit moet beschikken:

- Mogelijkheid tot authenticatie.
- Mogelijkheid tot koppelen aan gangbare identiteitsproviders, zoals Active Directory, LDAP of Radius.
- Mogelijkheid tot koppelen van een identiteit aan een IP-adres.
- Mogelijkheid tot het creëren van persoonsgebonden ACLs of regels.
- Scannen van het netwerkverkeer op virussen/malware.

Binnen Avans wordt er gebruik gemaakt van een zogenoemde next-generation firewall, namelijk een Palo Alto 5050[13]; Deze next-generation firewall is een statefull firewall, welke naast applicatiedetectie, ook kan worden gekoppeld aan de verschillende authenticatiemechanismen van Avans. Volgens de specificaties[13] voldoet deze firewall aan de gestelde technische specificaties van deze strategie.

Deze firewall wordt nu gebruikt als exterior firewall van Avans. Bij implementatie van de betreffende strategie zijn er twee keuzemogelijkheden:

- deze strategie zal aanvullend op de exterior firewall worden geïmplementeerd.
- er wordt gebruik gemaakt van een tweede firewall, die daartoe moet worden aangeschaft.

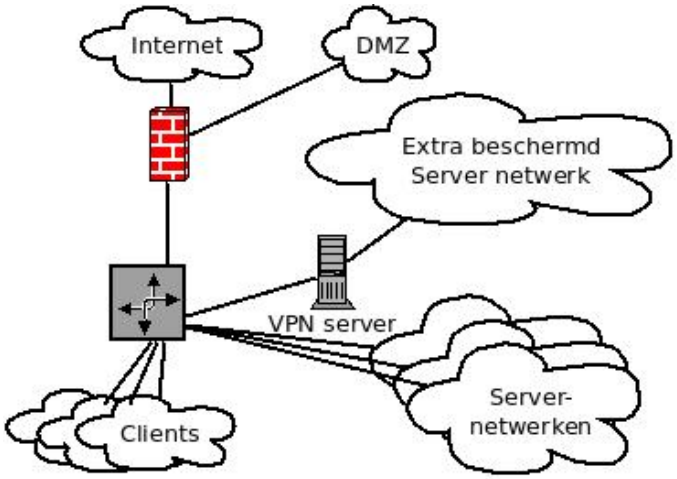
Het gebruiken van de huidige exterior firewall voor deze strategie strookt met het "Defense in Depth" model waarop het netwerk van Avans is gebaseerd. Er is dan maar één hard-boundry die de beveiligingen tussen alle netwerken/zones regelt. Indien deze firewall wordt gecompromitteerd, is ook het bedrijfsprocessennetwerk waarin de services/applicaties die zijn voorzien van persoonsgebonden toegang, gecompromitteerd. Daarom wordt aanbevolen voor deze strategie een tweede firewall aan te schaffen als interior firewall. Hiermee wordt er een tweede hard-boundry gecreëerd en is de beveiliging van dit netwerk niet afhankelijk van één device, welke dan een Single Point Of Failure zou vormen.

5.3.2 - Toegang op basis van VPN

In deze strategie krijgt een gebruiker via een Virtual Private Network, toegang tot de services/applicaties die zijn voorzien van persoonsgebonden toegang. Via VPN kan een gebruiker transparant, vanaf elk netwerk, toegang krijgen tot de service/applicatie waarvoor de gebruiker is geautoriseerd. Om gebruik te kunnen maken van afgeschermde services/applicaties dient de gebruiker eerst een VPN verbinding op te zetten. Alle verkeer richting de beschermde services/applicaties verloopt dan via de VPN verbinding. Er is voor gebruikers zonder VPN, geen rechtstreeks verkeer naar deze services mogelijk.

5.3.2.1 - Technische beschrijving

Om gebruik te kunnen maken van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, dient de gebruiker eerst een VPN verbinding op te zetten. Het verkeer bestemd voor de services/applicaties wordt via een (gecodeerde) tunnel gerouteerd. De werking van een VPN is weergegeven in afbeelding 5.4. De services/applicaties die in aanmerking komen voor persoonsgebonden toegang worden bij dit scenario ook in een apart servernetwerk geplaatst, zodat ze afgeschermd zijn van de gebruikersnetwerken.



Afbeelding 5.4: Ontwerp van de strategie VPN

De keuze voor een VPN techniek is afhankelijk van het gebruiksdoel van de VPN, maar ook van de ondersteuning door clients en de encryptiemogelijkheden. Globaal kunnen VPN technieken worden ingedeeld in 3 categorieën:

- Encrypted VPN: Encrypted VPNs versleutelen de data tussen de verzender en de ontvanger. Dit type VPN wordt meestal gebruikt om enkelvoudige niet-permanente VPN verbindingen op te zetten, zoals bijvoorbeeld in thuiswerksituaties. Encrypted VPNs zijn tegenwoordig het meest gebruikte VPN type dat er is. Voorbeelden van Encrypted VPNs zijn:
  - PPTP: Point-to-Point Tunneling Protocol: PPTP is een doorontwikkeling van het PPP protocol. Het PPP protocol is gemaakt om computers via modems met elkaar te verbinden. Bij PPTP worden de PPP-pakketten door middel van een versleutelde tunnel van het begin naar het eindpunt getransporteerd. PPTP wordt tegenwoordig gebruikt in simpele VPN implementaties, bijvoorbeeld als VPN voor thuisgebruik. De beveiliging van PPTP is achterhaald en minder veilig.

    - IPSec: Internet Protocol Security: IPSec is een techniek die IP-pakketten versleutelt of kan voorzien van een wachtwoord. IPSec is een verzameling van standaard protocollen, die het mogelijk maken om een versleutelde verbinding tot stand te brengen. IPSec wordt gezien als redelijk complex door de verscheidenheid aan encryptie technieken en standaarden die kunnen worden ingezet. De techniek wordt wel als veilig beschouwd.
    - SSL: Secure Socket Layer: SSL VPNs is een veelgebruikte VPN techniek die wordt ingezet als thuiswerkoplossing. SSL VPN is in de meeste gevallen multi-platform, goedkoop in de aanschaf en makkelijk te beheren. SSL-VPN werkt op de applicatie-laag van het OSI-model. Een SSL-VPN verbinding wordt opgebouwd via een webbrowser. De gebruiker logt in op een authenticatiepagina, waarna er via SSL een beveiligde tunnel wordt opgebouwd. Het verkeer over deze tunnel wordt middels SSL versleuteld.
- Tunnel-based VPN: De meest gebruikte tunnel-vpn implementaties zijn Layer 2 Tunneling Protocol (L2TP) en Multi Protocol Layer Switching (MPLS). Beide zijn Tunneltechnieken waarop een VPN gebouwd kan worden. Bij een L2TP VPN wordt er een beveiligde tunnel opgebouwd tussen het begin- en eindpunt, waarover een OSI Laag-2 verbinding wordt opgezet. De data over een tunnel-based VPN is niet versleuteld. Bij MPLS kunnen VPNs worden gecreëerd op Laag-1, Laag-2 en Laag-3 van het OSI-model. Tunnel-based VPNs worden vooral gebruikt bij ISPs en grote enterprises.
- Optical Private Networks (OPN): is gericht op het aanbieden van hogesnelheid verbindingen tussen een begin- en eindpunt. OPNs worden veel gebruikt om locaties via een optische glasvezelverbinding van een ISP te koppelen aan elkaar. OPNs hebben veel gemeen met VPNs, maar verschillen op de onderliggende protocollen. Daarnaast zijn OPNs in beheer van de ISP, waar dat bij VPN niet hoeft. Avans beschikt over 3 OPNs van SURFnet om de locaties in de verschillende steden te koppelen. Deze OPNs worden afgenomen van SURFnet, welke de OPNs ook in beheer heeft.

Voor persoonsgebonden toegang worden encrypted VPN technieken gebruikt. In het onderzoek komt naar voren dat SSL VPN de meest gangbare VPN techniek is om persoonsgebonden toegang te verlenen[14].

5.3.2.2 - Toepasbaarheid binnen Avans

Binnen Avans zijn er voor deze strategie meerdere SSL VPN technieken van verschillende fabrikanten aanwezig, welke hieronder kort worden beschreven:

- SSL-VPN van de Palo Alto Firewall[13,17]: De SSL VPN techniek van Palo Alto wordt binnen Avans gebruikt als VPN voor remote toegang tot het Avans netwerk voor externen en medewerkers. De SSL VPN techniek van Palo Alto ondersteund een beperkt aantal besturingssystemen, namelijk de Microsoft Windows varianten en Apple Mac OS X. Via IPSec technieken kunnen ook Apple iDevices een VPN-verbinding opzetten. Gezien de trend binnen Avans voor het “Bring Your Own Device” en device onafhankelijke oplossingen is de SSL VPN techniek van Palo Alto binnen Avans minder goed toepasbaar voor deze strategie.
- SSL VPN van de Novell Access Manager[18]: De SSL VPN techniek van Novell hoort bij het Product Novell Access Manager (NAM). NAM ontsluit bij Avans op dit moment de websites middels een Single-Sign-On methodiek. De SSL VPN techniek van NAM is een clientless implementatie; er hoeft geen client applicatie te worden geïnstalleerd op het device dat verbinding maakt. er worden diverse besturingssystemen ondersteund:
    - Microsoft Windows: XP, Vista en 7.
    - Apple Mac OS X.
    - Linux: Alleen Suse wordt ondersteund.
    - Mobiele devices zoals tablets en smartphones, worden volgens de specificaties niet ondersteunt.
- SSL VPN op Microsoft Windows Server 2008 R2[19]: Microsoft biedt in Windows Server 2008 een SSL VPN techniek aan die werkt in combinatie met Microsoft eigen Secure Socket Tunneling Protocol (SSTP). SSTP is ontwikkeld om veilig en simpel een SSL VPN op te kunnen bouwen. Meer informatie over SSTP is te vinden in de literatuur[19]. De SSL VPN functionaliteit zit standaard in Windows Server 2008 R2 en is onderdeel van de “Routing and Remote Access”-component van dit product. Bij het gebruik van deze VPN techniek is een client vereist. Er zijn clients beschikbaar voor Microsoft Windows, Apple OS X, Linux, en het mobiele besturingssysteem Google Android.

Met uitzondering van de Microsoft besturingssystemen, zijn de clients voor deze SSL-VPN allen third-party clients en niet standaard in de meeste operating systemen aanwezig.

- OpenVPN op een Linux OS[20]: OpenVPN is een SSL VPN techniek welke is ontwikkelt op het Linux platform door OpenVPN Technologies. De techniek is vergelijkbaar met die van Palo Alto en NAM. Bij het gebruik van deze VPN techniek is een client vereist. Er zijn clients beschikbaar voor Microsoft Windows, Apple OS X, Linux en voor mobiele clients voorzien van het Apple iOS of Google Android besturingssysteem.

Gezien de trend binnen Avans voor het "Bring Your Own Device" en device onafhankelijke oplossingen zijn de technieken van Microsoft en OpenVPN de meest geschikte technieken voor deze strategie. Voor het gebruik van OpenVPN in een enterprise omgeving, dient een licentieovereenkomst te worden afgesloten. Bij Microsoft is dit niet aan de orde, aangezien Avans over de goede licenties beschikt.

Tunnel-based VPNs worden vooral gebruikt bij ISPs en grote enterprises voor het koppelen van bijvoorbeeld twee vestigingen, maar niet voor persoonsgebonden toegang. Tunnel-based VPNs kunnen daardoor voor deze strategie niet worden gebruikt.

OPNs zijn gericht op het faciliteren van een verbinding tussen twee eindpunten over een optisch netwerk. OPNs worden niet gebruikt voor het aanbieden van persoonsgebonden toegang. De techniek is hier niet geschikt voor en daardoor ook niet bruikbaar voor deze strategie.

5.3.3 - Network Access Control - Network Access Protection

In de strategie voor Network Access Control (NAC) en Network Access Protection (NAP) wordt de toegang tot services/applicaties bepaald door het creëren van een persoonlijke ACL en controle van het end-user device op beveiliging. De beveiliging wordt bij deze strategie geregeld op het end-user device door middel van een client-applicatie. Het device dient wel te voldoen aan de veiligheidseisen die zijn gesteld door het bedrijf door middel van NAP. NAC zorgt vervolgens voor het uitvoeren van de ACL op het end-user device.

Het voordeel van deze techniek is dat op device niveau voldaan moet worden aan de gestelde beveiligingseisen alvorens met kan worden toegelaten tot de services/applicaties waar voor persoonsgebonden toegang is ingeregeld. Indien een end-user device niet voldoet aan de gestelde eisen, krijg de gebruiker de mogelijkheid om zijn apparaat 'compliant' te krijgen. Daarna kan de toegang naar de persoonsgebonden services/applicaties alsnog worden verleend.

Nadelen van deze techniek zijn dat er een client-applicatie dient te worden gebruikt op elk end-user device, voordat toegang kan worden verkregen. Ook is er geen controle over eventuele manipulatie van de beveiligingsstatus van het device of de client-applicatie voor deze techniek die op het device aanwezig is. Indien gegevens worden gemanipuleerd op het end-user device, bestaat de kans dat een gebruiker ongeoorloofd toegang krijgt tot de services/applicaties die in aanmerking komen voor persoonsgebonden toegang.

5.3.3.1 - Technische beschrijving

De in de literatuur meest omschreven NAC/NAP techniek, is de oplossing die wordt geboden door Cisco en Microsoft. De NAC/NAP oplossing is ontstaan uit een samenwerkingsverband tussen Cisco en Microsoft. Cisco verzorgt hierbij de NAC-techniek en Microsoft de NAP-techniek.

De NAC/NAP oplossing van Cisco en Microsoft heeft wel eisen met betrekking tot de hardware die moet worden gebruikt binnen de oplossing. Voor NAC is het verplicht gebruik te maken van enterprise switches als Network Access Device (NAD), welke 802.1x authenticatie ondersteunen. Voorbeelden hiervan zijn de Catalyst 6500, 4500 en 3750 serie switches. Ook is een Cisco Access Control Server[21] vereist. Deze server creëert de dynamische ACLs aan de hand van de gebruikersgegevens en de NAP-status van het end-user device en handelt de doorgifte van authenticatiegegevens af.

NAP bestaat uit een Network Policy server, welke een end-user device controleert op het up-to-date zijn van de beveiliging en daarmee voldoet aan de beveiligingseisen die zijn gesteld aan de eindgebruiker en diens device. Deze controle gebeurd door middel van een Health Requirement server. Deze server wordt gebruikt om een baseline vast te stellen waaraan de Network Policy Server, waarop de beveiligingseisen zijn gedefinieerd, zijn controle uitvoert. Beide NAP onderdelen zijn een serverrol in het Microsoft besturingssysteem "Windows Server 2008" en hoger. Clients van een ander merk of type kunnen wel gebruik maken van NAC en worden als "vreemd" aangemerkt binnen NAC. Er kan echter niet worden gecontroleerd op de status van het end-user device door middel van NAP.

Samengevat verzorgt de NAC/NAP oplossing van Cisco en Microsoft netwerktoegang tot afgeschermde resources, waarbij het informatie verzameld over het gebruikersapparaten met betrekking tot de beveiligingsstatus van het apparaat. Voorbeelden hiervan zijn:

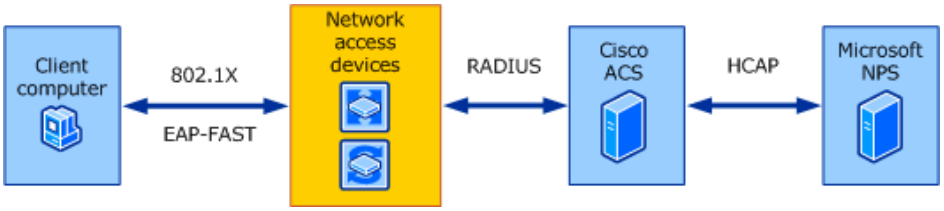
- Is de virusscanner up-to-date.
- Staat de client-firewall aan.
- Zijn alle Windows updates geïnstalleerd.

Naast het verzamelen van informatie, zorgt de NAC/NAP oplossing er voor dat het device in overeenstemming kan worden gebracht met de gestelde beveiligingseisen.

De NAC/NAP oplossing zorgt voor de op de gebruiker gebaseerde ACL, die toegang verschaft tot het bedrijfsnetwerk. De ACL wordt opgebouwd aan de hand van de overeenstemming van het end-user device met de beveiligingseisen. De beveiligingseisen voor publiek toegestane services/applicaties kan eenvoudiger zijn dat de beveiligingseisen die zijn gesteld aan services/applicaties die bijvoorbeeld persoonsgegevens bevatten.

De werking van de oplossing is te zien in afbeelding 5.5. De stappen die een client maakt om verbinding te krijgen met het netwerk zijn[22]:

1. Er wordt een 802.1x connectie opgebouwd tussen het end-user device (Client Computer) en het NAD.
2. De NAD vraagt de credentials aan het end-user device. De gevraagde gegevens worden versleuteld naar de NAD verstuurd en bevatten de gebruikersgegevens, apparaat gegevens en de status van het end-user device.
3. De client die op het end-user device is geïnstalleerd, verstuurd de gevraagde gegevens naar de NAD.
4. De NAD zend de gegevens door naar de Radius server. Radius is in vele gevallen gekoppeld aan een andere identiteitsprovider, zoals Active Directory. Daar worden de opgegeven gegevens gevalideerd.
5. De status van het end-user device worden doorstuurt naar de Microsoft NPS server. De NPS server controleert en valideert de verstrekte gegevens. De uitkomst hiervan wordt teruggestuurd naar de Cisco Secure ACS.
6. Aan de hand van de validatie van de NPS-server en de gebruikersgegevens wordt het end-user device via de Cisco ACS door de NAD in een VLAN geplaatst, dat overeenkomt met de compliance van het device en de betreffende gebruiker. Indien het end-user device voldoet aan de gestelde eisen, zal deze worden toegelaten tot het bedrijfsnetwerk. Indien het end-user device niet voldoet aan de gestelde beveiligingseisen, wordt het end-user device in een quarantainenetwerk geplaatst.
7. De gebruiker ontvangt, via de client op het end-user device, een melding van de uitkomst van de authenticatie. Indien een end-user device niet voldoet aan de gestelde eisen, zal dat op deze manier kenbaar worden gemaakt aan de gebruiker.



Afbeelding 5.5: De werking van NAC/NAP[23].

Het voordeel van deze oplossing is dat het end-user device veilig op het netwerk wordt toegelaten. Daarnaast vindt er authenticatie plaats, waarop de gebruiker wordt toegelaten.

Het nadeel van deze oplossing is dat er een NAC/NAP-client dient te worden geïnstalleerd op de client. Deze client wordt alleen ondersteund op Microsoft besturingssystemen Vista SP1 of hoger.

5.3.3.2 - Toepasbaarheid binnen Avans

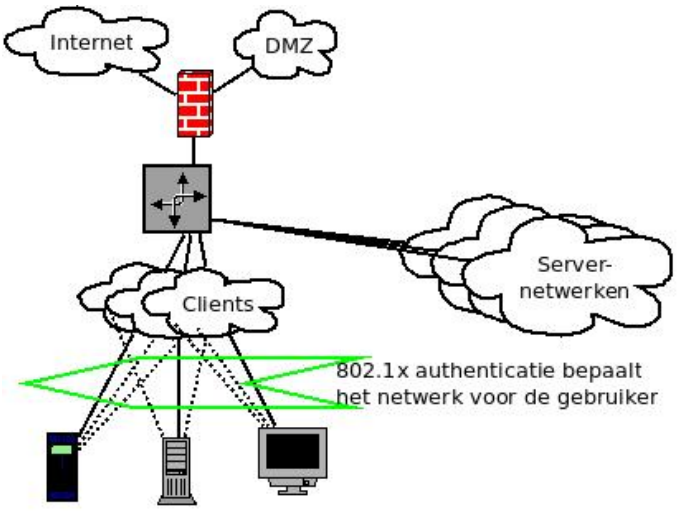
Voor implementatie van deze strategie zal rekening moeten worden gehouden met de reeds aanwezige 802.1x authenticatie mechanismen die voor het WLAN worden gebruikt. Deze moet aan de oplossing van Cisco/Microsoft te koppelen zijn. Daarnaast zal de techniek moeten worden geïmplementeerd op het vaste netwerk. Op dit moment wordt er geen 802.1x authenticatie toegepast op de vaste netwerken, maar komen vaste werkplekken in een vast netwerk terecht, waarop de rechten van toepassing zijn die zijn gesteld in de ACL van dat betreffende netwerk. De vaste werkplekken worden wel op beveiligingsstatus gecontroleerd middels een virusscanner en kunnen de werkstations ook in quarantaine worden geplaatst, echter wordt er niet gecontroleerd op beveiligingsstatus van een werkplek middels een NAP-systeem.

Binnen Avans is niet alle techniek, benodigd voor deze strategie, aanwezig. De Cisco Secure ACS server is niet binnen Avans beschikbaar en zal, in geval van aanname van deze strategie, moeten worden aangeschaft. NAP is standaard aanwezig binnen Microsoft Windows Server 2008 en hoger. Dit besturingssysteem is het standaard Windows besturingssysteem voor servers bij Avans en is beschikbaar. Volgens de literatuur[23] is het niet mogelijk om alle typen devices te ontsluiten door middel van deze strategie. De oplossing is toepasbaar voor devices die zijn voorzien van het Microsoft besturingssysteem Windows Vista SP1 of hoger. Gezien de trend binnen Avans voor het “Bring Your Own Device” en OS onafhankelijke oplossingen is deze strategie binnen Avans minder goed toepasbaar.

5.3.4 - Verplaatsen van clients in netwerken

In deze strategie krijgt een gebruiker toegang tot de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, door plaatsing in het voor de gebruiker geschikte netwerken en het toekennen van een persoonsgebonden ACL voor deze gebruiker.

Om gebruik te kunnen maken van afgeschermde services/applicaties dient de gebruiker zich eerst aan te melden op het netwerk. Het aanmelden op het netwerk gebeurd via 802.1x. Na het succesvol aanmelden op het netwerk worden de gebruikers aan de hand van de authenticatie gegevens in een netwerk geplaatst. Aan de gebruikers die zijn geautoriseerd om services/applicaties die in aanmerking komen voor persoonsgebonden toegang te gebruiken, wordt een persoonsgebonden ACL toegekend, die de gebruiker toegang geeft tot de services/applicaties waarvoor hij is geautoriseerd. Het ontwerp voor deze strategie is weergegeven in afbeelding 5.6.



Afbeelding 5.6: Het ontwerp van de strategie “Verplaatsen van clients in netwerken” .

5.3.4.1 - Technische beschrijving

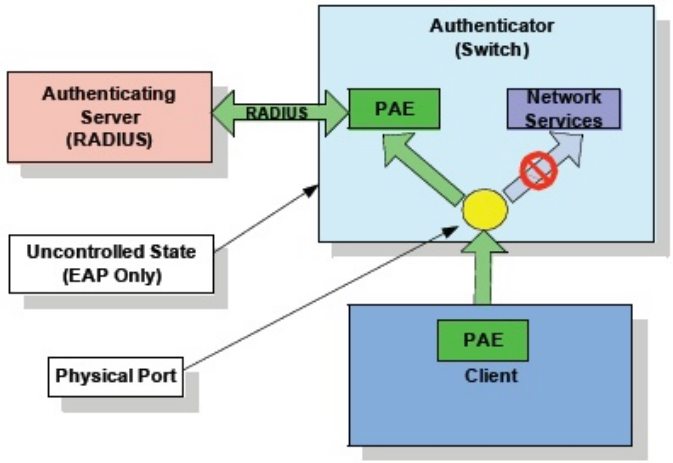
Deze strategie is gebaseerd op 802.1x authenticatie in combinatie met Radius. De voorwaarden voor deze strategie zijn dat de netwerkapparatuur 802.1x ondersteund. Voorbeelden hiervan zijn de Catalyst 6500, 4500 en 3750 serie switches. 802.1x is een framework voor port-based authenticatie, ontwikkeld door de Institute of Electrical and Electronics Engineers (IEEE). 802.1x authenticatie is opgebouwd uit 3 componenten:

- De client: De client is het device dat wil authenticeren aan het netwerk. In IEEE termen wordt dit een supplicator genoemd.
- NAD: De NAD is het device waaraan de client is gekoppeld. Dit kan een LAN switch of WLAN access point zijn. In IEEE termen wordt dit een authenticator genoemd.
- Authenticatie server: In de 802.1x standaard staat omschreven dat de te gebruiken authenticatie techniek RADIUS moet zijn.

Als een client wordt aangesloten op het netwerk, is er nog geen netwerkverkeer mogelijk. behalve authenticatieverkeer voor 802.1x. De pakketten voor authenticatie worden uitgewisseld met behulp van een authenticatie mechanisme. Het authenticatie mechanisme tussen NAD en de client is het Extensible Authentication Protocol (EAP). EAP-berichten kunnen over verschillende media worden getransporteerd. Dit hangt af van het gebruikte encapsulatie mechanisme van de EAP-pakketten. Er zijn twee encapsulatie mechanismen voor EAP-berichten:

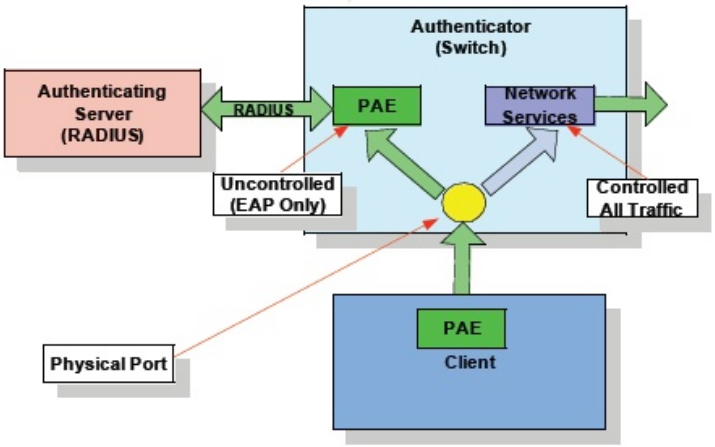
- EAP over LAN (EAPOL), welke het encapsulatie mechanisme omschrijft voor encapsulatie van EAP berichten over vaste media.
- EAP over Wireless (EAPOW), welke het encapsulatie mechanisme omschrijft voor encapsulatie van EAP berichten over draadloze media.

De EAP-pakketten worden door de NAD doorgestuurd naar de authenticatieserver. De situatie vóór de authenticatie is weergegeven in afbeelding 5.7.



Afbeelding 5.7: Netwerk flow vóór authenticatie[24].

De authenticatieserver controleert de ontvangen authenticatiegegevens en geeft een response over de uitkomst van deze controle terug aan de NAD. Indien de response negatief is, zal geen netwerkverkeer worden doorgelaten. Indien de response positief is, zal de NAD een netwerk-ID ontvangen van de authenticatieserver. De NAD zal de client in het correcte netwerk plaatsen en het netwerkverkeer doorlaten. Dit is weergegeven in afbeelding 5.8.



Afbeelding 5.8: Netwerk flow na authenticatie[24].

De authenticatieserver geeft bij een positieve response, ook de ACL-IDs mee van de ACLs die op de geauthenticeerde gebruiker van toepassing zijn. De persoonsgebonden dynamische ACLs die na authenticatie worden toegepast, is opgebouwd uit verschillende kleinere ACLs, die aan de hand van gebruikersrollen of toegangseisen worden opgebouwd. Zo kan er een ACL "Financiën" zijn, die alleen toegang geeft tot financiële services/applicaties en een ACL "Geen-http", welke geen webverkeer toestaat. Als een gebruiker in Radius allebei de ACLs toegekend heeft gekregen, mag deze gebruiker geen http-verkeer versturen en ontvangen, maar wel naar de financiële services/applicaties. Afhankelijk van de toegekende ACLs wordt er op deze wijze een persoonsgebonden dynamische ACL opgebouwd.

Na een succesvolle authenticatie bevindt de gebruiker zich in een voor hem geautoriseerd netwerk met toegangsrechten die op zijn rol of functie binnen de organisatie zijn toegekend.

5.3.4.2 - Toepasbaarheid binnen Avans

802.1x authenticatie is goed inzetbaar binnen Avans en wordt al ingezet voor het authenticeren van WLAN gebruikers. Alle netwerkapparatuur die binnen Avans aanwezig is, ondersteund het 802.1x protocol. Voor implementatie van deze strategie zal rekening moeten worden gehouden met de reeds aanwezige 802.1x authenticatie mechanismen die voor het WLAN worden gebruikt. Er zal moeten worden onderzocht of de gebruikte WLAN oplossing kan worden gekoppeld aan de LAN-oplossing. 802.1x is op dit moment niet actief op het vaste netwerk. Vaste werkplekken worden in een vast netwerk geplaatst, waarop de rechten van toepassing zijn, die zijn gesteld in de globale ACL van dat betreffende netwerk. Bij deze strategie zal 802.1x op het vaste netwerk moeten worden geïmplementeerd.

Radius wordt binnen Avans nu gebruikt voor authenticatie van WLAN gebruikers, maar kan zonder veel aanpassingen worden ingezet voor 802.1x authenticatie op het gehele netwerk van Avans.

802.1x authenticatie is toepasbaar op de meeste typen devices, zoals Microsoft Windows, Apple OS X, Linux en de meeste mobiele devices. Gezien de trend binnen Avans voor het "Bring Your Own Device" en device onafhankelijke oplossingen is deze strategie binnen Avans goed toepasbaar. Het nadeel van deze techniek is dat de beveiligingsstatus van het apparaat waarmee de gebruiker is verbonden aan het netwerk, niet wordt gecontroleerd. 802.1x authenticatie met persoonsgebonden ACLs wordt ook niet door alle operating software op de Cisco apparatuur ondersteund. Er zal moeten worden uitgezocht of de versie operating software die actief is op de huidige omgeving van Avans, geschikt is voor deze strategie. Indien dit niet het geval is, kan deze strategie alsnog worden toegepast door het inzetten van een Cisco Secure Access Control Server[21].

6 - Strategie Selectie

In hoofdstuk 5 zijn vier toepasbare strategieën uitgewerkt voor toegang tot de services/applicaties die in aanmerking komen voor persoonsgebonden toegang. In dit hoofdstuk worden de beschreven strategieën getoetst op vastgestelde beoordelingscriteria. Aan de hand van de uitkomst van de beoordeling op de beschreven beoordelingscriteria, zal een strategie worden aanbevolen. De beoordelingscriteria worden in paragraaf 6.1 toegelicht. Ook zullen er wegingsfactoren worden toegevoegd aan de beoordeling.

6.1 - Beoordelingscriteria

Voor het vaststellen van de beoordelingscriteria aan de strategie voor persoonsgebonden toegang, wordt gebruik gemaakt van de MoSCoW-methodiek. Bij deze methodiek worden de eisen en wensen die worden gesteld aan een strategie in kaart gebracht en geprioriteerd, waarbij MoSCoW de afkorting is voor:

- M: Must Have: een eis of wens dat in de strategie aanwezig moet zijn, wil het product bruikbaar zijn voor dit onderzoek.
- S: Should Have: een eis of wens in deze categorie is zeer gewenst, maar zonder deze eis of wens kan de strategie nog steeds bruikbaar zijn voor dit onderzoek.
- C: Could Have: de eisen en wensen in deze categorie mogen alleen aan bod komen als er nog tijd over is in het onderzoek om deze eisen en wensen te behandelen en deze eisen en wensen een goede aanvulling zijn op de inhoud van het onderzoek.
- W: Would like to Have: Deze eisen en wensen zijn niet essentieel voor het onderzoek, maar zouden interessant kunnen zijn in een vervolgonderzoek.

Aan de MoSCoW classificatie worden een wegingsfactor toegekend. Must Haves wegen zwaarder mee in de beoordeling van Would Like to Have. De wegingsfactoren zijn als volgt:

- M: Must Have: score x 4.
- S: Should Have: score x 3.
- C: Could Have: score x 2.
- W: Would like to Have: score x 1.

Om te beoordelen of een strategie voldoet aan de gestelde eisen en wensen van Avans, zijn er beoordelingscriteria voor de gevonden strategieën vastgesteld. Elke uitgewerkte strategie wordt beoordeeld op de volgende punten:

1. ***Kan de oplossing volgens het beveiligingsmodel van Avans geïmplementeerd worden*:** De strategie voor persoonsgebonden toegang moet in het huidige beveiligingsmodel passen. In het Plan van Aanpak is gesteld dat er geen nieuw beveiligingsmodel wordt ontwikkeld binnen het onderzoek. Dit beoordelingscriterium is een Must Have en heeft een weegfactor van 4. Indien de strategie goed integreert met het huidige beveiligingsmodel, wordt er een hoge score toegekend.
2. ***Kan de oplossing gerealiseerd worden met binnen Avans beschikbare techniek*:** Binnen Avans zijn veel technieken aanwezig, welke niet worden gebruikt of niet nog niet zijn ingezet, maar die wel toepasbaar zijn in de beschreven strategieën. Er wordt in het onderzoek gesteld dat de probleemstelling zal moeten worden opgelost met technieken die reeds binnen Avans aanwezig zijn. Daarnaast is het een bijkomend voordeel dat de benodigde expertise van de technieken die reeds aanwezig zijn, al binnen Avans aanwezig is. De investeringen die dienen te worden gedaan in de aanbevolen strategie, zullen daardoor lager zijn. De strategieën worden beoordeeld in hoeverre de techniek en expertise benodigd voor de strategie, reeds binnen Avans aanwezig is. Dit beoordelingscriterium is een Must Have en heeft een weegfactor van 4. Indien de strategie volledig kan worden gerealiseerd met binnen Avans aanwezige technieken, wordt een hoge score toegekend.
3. ***Bied de oplossing een volledige oplossing voor de probleemstelling*:** Het onderzoek naar persoonsgebonden toegang is opgezet rond de probleemstelling zoals vermeld in het Plan van Aanpak. Het doel van het onderzoek is het adviseren van een strategie voor het oplossen van het probleem. In dit beoordelingscriterium wordt getoetst of de strategie voldoet voor het oplossen van de probleemstelling. Dit beoordelingscriterium is een Must Have. Indien de strategie in theorie een volledige oplossing voor de probleemstelling kan zijn, wordt een hoge score toegekend.

4. ***Is extra aanschaf (hardware/licenties) nodig*:** In het onderzoek is gesteld dat de techniek die nodig is voor het implementeren van de strategie, reeds bij Avans aanwezig moet zijn. Ook al is de techniek binnen Avans aanwezig, dan kan het nog steeds zo zijn dat er licenties moeten worden aangeschaft of, om de strategie schaalbaar te maken, er extra hardware moet worden aangeschaft. Dit beoordelingscriterium is een Should Have en heeft een weegfactor van 3. Voor het uitvoeren van de strategie mag er een investering worden begroot. Indien de strategie volledig kan worden gerealiseerd zonder aanschaf van hardware/licenties, wordt een hoge score toegekend.
5. ***Is de oplossing eenvoudig (transparant) voor eindgebruikers en beheerders*:** Het is wenselijk voor Avans om een strategie aan te nemen die transparant en eenvoudig is in gebruik, vooral voor de eindgebruiker. Dit houdt in dat de strategie wordt beoordeeld op het aantal handelingen dat een gebruiker moet uitvoeren, of er een client nodig is die ingesteld moet worden of andere handelingen die als lastig zouden kunnen worden ervaren door de eindgebruiker. Dit beoordelingscriterium is een Should Have en heeft een weegfactor van 3. Het is voor Avans acceptabel indien de gebruiker extra handelingen moet verrichten om gebruik te maken van de services/applicaties die persoonsgebonden zijn afgeschermd door middel van een strategie. Er wordt een lage score aan de strategie toegekend als deze minder eenvoudig door de eindgebruiker kan worden bediend.
6. ***Is de oplossing toepasbaar op gangbare end-user devices*:** Gezien de trend binnen Avans voor het "Bring Your Own Device" en OS onafhankelijke oplossingen is dit beoordelingscriterium voor Avans belangrijk. Het is vereiste dat de strategie zo veel mogelijk voldoet aan dit beoordelingscriterium. Dit beoordelingscriterium is een Must Have en heeft een weegfactor van 4. Indien de strategie op gangbare end-user devices kan worden toegepast, wordt een hoge score toegekend.
7. ***Heeft de strategie een hoge of lage geschatte beheerlast*:** De beheerlast wordt in deze gedefinieerd als de kosten die zijn gemoeid met het ondersteunen en onderhouden van de strategie. Hierbij kan men denken aan het onderhoud dat moet worden uitgevoerd aan de hardware of software van de strategie of de ondersteuning die bij de helpdesk moet worden geboden in geval van een probleem bij de eindgebruiker. Hierbij kan worden gesteld dat bij een strategie welke is geïmplementeerd aan de gebruikerszijde en waarbij software wordt geïnstalleerd op het end-user device, het onderhouden van dit device meer ondersteuning nodig heeft, dan een strategie die aan de serverzijde is geïmplementeerd. Bij een strategie aan de serverzijde is de ondersteuning geconcentreerd rond de beheerorganisatie en op de objecten waaruit de strategie is opgebouwd. Dit beoordelingscriterium is een Must Have. De strategie krijgt een lage score op dit beoordelingscriterium indien:
    - Er beheer op veel plaatsen/systemen dient plaats te vinden.
    - Componenten in de strategie veel afstemming vereisen.
    - Er veel handelingen van eindgebruikers moeten plaatsvinden voor het gebruik van de strategie.
    - De frequentie van wijzigingen die nodig zijn om de strategie goed te kunnen beheren.
    - De complexiteit van de strategie of het te beheren object. De complexiteit van een strategie heeft direct gevolgen voor de beheerlasten.

Aan deze beoordelingscriteria worden waarden toegekend van 1 tot en met 5. Deze waarden hebben daarbij de volgende betekenis:

- 1: voldoet niet aan het beoordelingscriterium.
- 2: voldoet voor een klein deel aan het beoordelingscriterium.
- 3: voldoet, afhankelijk van nog te maken keuzes, wel of niet aan het beoordelingscriterium.
- 4: voldoet voor het grootste deel aan het beoordelingscriterium.
- 5: voldoet geheel aan het beoordelingscriterium.

De toegekende waarden worden met de wegingsfactor vermenigvuldigd. Dit levert een score per beoordelingscriterium op. De sommatie van deze scores levert een eindcijfer op voor de betreffende strategie, waarbij geldt: hoger is beter.

De beoordeling van de diverse strategieën wordt in de volgende paragraaf beschreven.

6.2 - Beoordeling strategieën

In deze paragraaf worden de vier strategieën die zijn beschreven in hoofdstuk 5.3 getoetst op de beoordelingscriteria zoals deze zijn gesteld in paragraaf 6.1.

De vier strategieën die worden beoordeeld zijn:

1. Servers in afgeschermd netwerk, dynamische ACLs aan de gebruiker koppelen. Bij deze strategie wordt een firewall geplaatst tussen de services/applicaties die in aanmerking komen voor persoonsgebonden toegang en de gebruikers. De techniek wordt geïmplementeerd aan de serverzijde.
2. Servers in afgeschermd netwerk, afgeschermd en getunneld netwerkverkeer. Bij deze strategie wordt een VPN techniek geïmplementeerd die toegang geeft tot de services/applicaties die in aanmerking komen voor persoonsgebonden toegang. De techniek wordt geïmplementeerd aan de serverzijde.
3. Clients controleren voordat toegang wordt verleend. Bij deze strategie wordt de NAC/NAP oplossing van Cisco en Microsoft ingezet, welke er voor zorgt dat de client aan het netwerk wordt geauthenticeerd en er een controle wordt uitgevoerd op de status van het device van de gebruiker. Deze laatste moet daarbij voldoen aan de gestelde beveiligingseisen. De techniek wordt geïmplementeerd aan de clientzijde.
4. Verplaatsen van clients in netwerken na authenticatie en toekennen van een persoonsgebonden ACL. Deze strategie is gebaseerd op de 802.1x techniek van Cisco in combinatie met Radius authenticatie. De techniek wordt geïmplementeerd aan de clientzijde.

De scores van de diverse strategieën zijn toegekend op basis van de volgende argumentatie bij de gestelde beoordelingscriteria:

1. Kan de oplossing volgens het beveiligingsmodel van Avans geïmplementeerd worden?
Alle vier de strategieën kunnen worden geïmplementeerd volgens het beveiligingsmodel van Avans en ontvangen daar voor de hoogste score van 5. Alle strategieën vormen een extra beveiligingslaag tussen de services/applicaties die in aanmerking komen voor persoonsgebonden toegang.

2. Kan de oplossing gerealiseerd worden met binnen Avans beschikbare techniek?
De firewall techniek voor strategie 1 is reeds binnen Avans aanwezig in de vorm van een firewall cluster als hard-boundry tussen Internet, het DMZ netwerk en het interne netwerk. De specifieke technieken voor persoonsgebonden toegang zijn wel aanwezig maar worden op dit moment niet ingezet. Ook de technieken voor strategieën 2 en 4 zijn binnen Avans aanwezig, waarbij de techniek van strategie 2 wordt ingezet om toegang te bieden voor externen en strategie 4 al wordt gebruikt in de WLAN omgeving van Avans. De enige techniek die niet volledig binnen Avans aanwezig is, is de techniek van strategie 3. Hierbij ontbreekt de Cisco Secure ACS server, welke zal moeten worden aangeschaft. Daardoor is de score bij strategie 3 vastgesteld op 2. Aan de overige strategieën wordt een score van 5 toegekend.

3. Bied de oplossing een volledige oplossing voor de probleemstelling?
Alle strategieën bieden een complete oplossing voor de gestelde probleemstelling, namelijk het persoonsgebonden afschermen van services/applicaties die in aanmerking komen voor persoonsgebonden toegang. De techniek van strategie 1 doet dit op een eenvoudige manier. Bij de overige strategieën moet er nog iets aanvullends gebeuren aan de gebruikerszijde op het end-user device. Bij strategie 2, 3 en 4 dient er een client aanwezig te zijn op het device en worden bij strategie 3 en 4 devices van netwerk gewisseld. Ondanks de complexiteit van sommige strategieën, wordt er wel een oplossing gecreëerd voor de probleemstelling. Alle strategieën wordt een score 5 toegekend.

4. Is extra aanschaf (hardware/licenties) nodig?
Afhankelijk van de keuzes die bij een implementatietraject worden gemaakt, dienen er hardware/licenties te worden aangeschaft bij alle strategieën. Bij strategie 1 is de aanschaf afhankelijk van de keuze die wordt gemaakt bij implementatie. De strategie kan worden ondergebracht op het huidige firewall cluster. Hiervoor hoeft geen investering worden gedaan. Omdat er wordt aanbevolen om een separate firewall aan te schaffen en dit een investering met zich meebrengt, wordt een score van 3 toegekend. Voor strategie 2 zal er naar alle waarschijnlijkheid, afhankelijk van de techniekkeuze, licenties moeten worden aangeschaft; dit betreft dan een beperkte investering. Aan strategie 2 wordt daarom een score van 4 toegekend.

Voor strategie 3 geldt dat er een Cisco Secure ACS oplossing moet worden aangeschaft voor het kunnen realiseren van de strategie. Er wordt daardoor een score van 1 toegekend. Bij strategie 4 is de aanschaf van een Cisco Secure ACS optioneel en afhankelijk van keuzes die moeten worden gemaakt bij een implementatietraject. Voor het toekennen van een score, wordt er vanuit gegaan dat de Cisco Secure ACS wel wordt aangeschaft. Aan strategie 4 een score van 3 toegekend.

5. Is de oplossing eenvoudig (transparant) voor eindgebruikers en beheerders?
Strategie 1 kan wordt gekenmerkt als transparant en eenvoudig voor eindgebruiker en beheerder. Doordat een dergelijke firewall een netwerkcomponent is, die door middel van koppelingen met de authenticatiemechanismen van Avans de persoonsgebonden ACL kan opbouwen, is geen actie van een gebruiker nodig, maar worden de services/applicaties die in aanmerking komen voor persoonsgebonden toegang wel goed afgeschermd. De gebruiker zal geen services/applicaties kunnen benaderen waarvoor hij niet geautoriseerd is. Aan strategie 1 wordt een score van 5 toegekend. Bij de strategieën 2, 3 en 4 moet er gebruik worden gemaakt van een client. Voor strategie 4 is een gebruiksvriendelijke client beschikbaar. Daarom wordt aan deze strategie een score van 4 toegekend. Elk gangbaar besturingssysteem is immers voorzien van een 802.1x client. Voor strategie 2 en 3 zal op het end-user device een aparte client moeten worden geïnstalleerd. Dit kan voor sommige eindgebruikers minder eenvoudig zijn. Dit levert de strategieën 2 en 3 een score van 2 op.

6. Is de oplossing toepasbaar op gangbare end-user devices?
De strategieën 1, 2 en 4 zijn toepasbaar op de gangbare end-user devices. Strategie 3 is alleen toepasbaar voor devices die zijn voorzien van het Microsoft besturingssysteem Windows Vista SP1 of hoger. Door de beperkte ondersteuning van devices van strategie 3 wordt een score van 1 toegekend. De overige strategieën wordt een score van 5 toegekend.

7. Heeft de strategie een hoge of lage geschatte beheerlast?
De beheerlasten van de strategie 1 kunnen worden ingeschat als laag, doordat er centraal beheer kan worden gevoerd. Daarnaast is er geen ondersteuning nodig van de gebruikte end-user devices, omdat de oplossing aan de serverzijde wordt geïmplementeerd en transparant is. De gebruikers hoeven bij strategie 1 zelf geen beheer uit te voeren op de end-user devices, omdat er geen client wordt gebruikt. Wel moeten de beveiligingsregels, zoals deze zijn aangebracht, periodiek worden gecontroleerd op juistheid. Dit vergt enige beheerlast. Aan de strategie 1 wordt een score van 4 toegekend. De overige strategieën kennen een meer of minder intensieve vorm van beheer. Door de toepassing van clients bij deze strategieën, wordt het beheer van de client op het end-user device bij de eindgebruiker neergelegd waardoor een vraag om ondersteuning van de helpdesk te verwachten is. Bij strategie 2 dragen met name gebruikersbeheer en het beheer van de client op het end-user device bij aan de geschatte beheerlast van deze strategie. Aan strategie 2 wordt een score van 2 toegekend. Strategie 3 en 4 zijn complex in opzet omdat de gebruikte techniek i opgebouwd uit meerdere componenten die afhankelijk zijn van elkaar. De complexiteit kan er voor zorgen dat deze strategieën beheerintensief zijn; de componenten dienen immers op elkaar afgestemd te blijven. Het gebruikersbeheer bij deze strategieën is niet geautomatiseerd en beheerintensief. Daardoor wordt aan deze strategieën een score van 1 toegekend.

De resultaten en de beoordeling van de diverse strategieën zijn weergegeven in Tabel 6.1. Uit de tabel is af te leiden dat de beste strategie voor het verlenen van persoonsgebonden toegang, strategie 1 is. Deze heeft de hoogste eindscore van 120 behaald.

Beoordelings criterium	MoSCoW	Weging	Strategie 1	Strategie 2	Strategie 3	Strategie 4
1	Must Have	4	5	5	5	5
2	Must Have	4	5	5	2	5
3	Must Have	4	5	5	5	5
4	Should Have	3	3	4	1	3
5	Should Have	3	5	2	2	4
6	Must Have	4	5	5	1	5
7	Must Have	4	4	2	1	1
Eindscore			120	106	65	105

Tabel 6.1: Strategie beoordeling.

7 - Voorbeelduitwerking

In dit hoofdstuk wordt een voorbeelduitwerking geschetst van de strategie 1 met één van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang. De servers van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang worden bij deze strategie in een apart netwerk geplaatst, waarbij dit netwerk van de rest gescheiden wordt door een firewall. De applicatie die hierbij is gekozen is Osiris. Osiris is een applicatie die uit meerdere diensten met verschillende autorisatieniveaus bestaat.

Van Osiris en de aanbevolen strategie wordt een voorbeeldontwerp gemaakt en wordt beschreven hoe de diverse netwerkflows lopen wanneer toegang wordt gevraagd naar de diverse diensten van Osiris.

Osiris bestaat globaal uit twee onderdelen waar gebruikers aan kunnen verbinden:

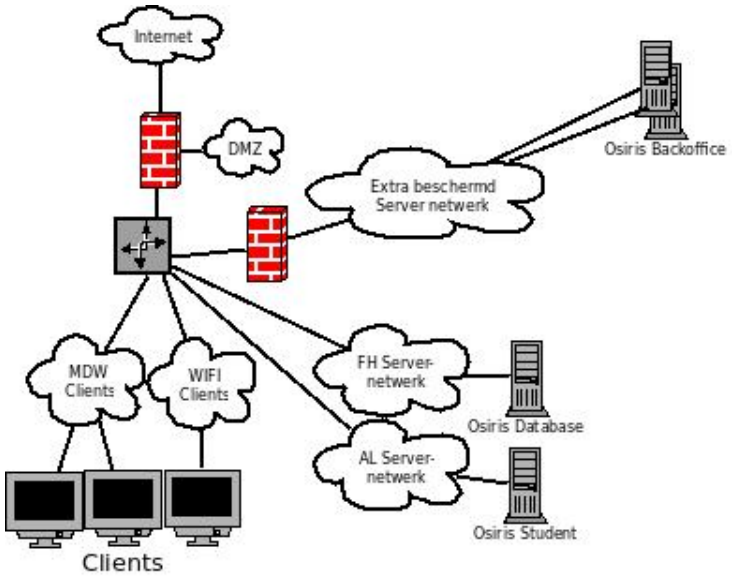
- Osiris Student: Studentenomgeving van Osiris en geplaatst in het AL-netwerk.
- Osiris Backoffice: Backoffice omgeving voor docenten en medewerkers, bestaande uit Osiris Begeleider en Manager, nu geplaatst in het BP-netwerk.

De Osiris Database server, geplaatst in het FH-netwerk, is alleen toegankelijk vanaf andere servicenetwerken. De beveiliging van het FH netwerk wordt geregeld door de ACL op de core-switch.

In het huidige beveiligingsmodel kunnen alle gebruikersnetwerken naar het AL-netwerk. De Backoffice van Osiris, welke nu in het BP-netwerk is geplaatst, is toegankelijk voor de medewerkersnetwerken. Dit houdt in dat:

- De Osiris Backoffice alleen toegankelijk is vanaf het medewerkersnetwerk.
- Alle gebruikers in een medewerkersnetwerk kunnen communiceren met de Osiris Backoffice, ook de medewerkers die niet zijn geautoriseerd.
- Er vanaf andere gebruikersnetwerken, waaronder WLAN, niet naar de Osiris Backoffice kan worden gecommuniceerd.

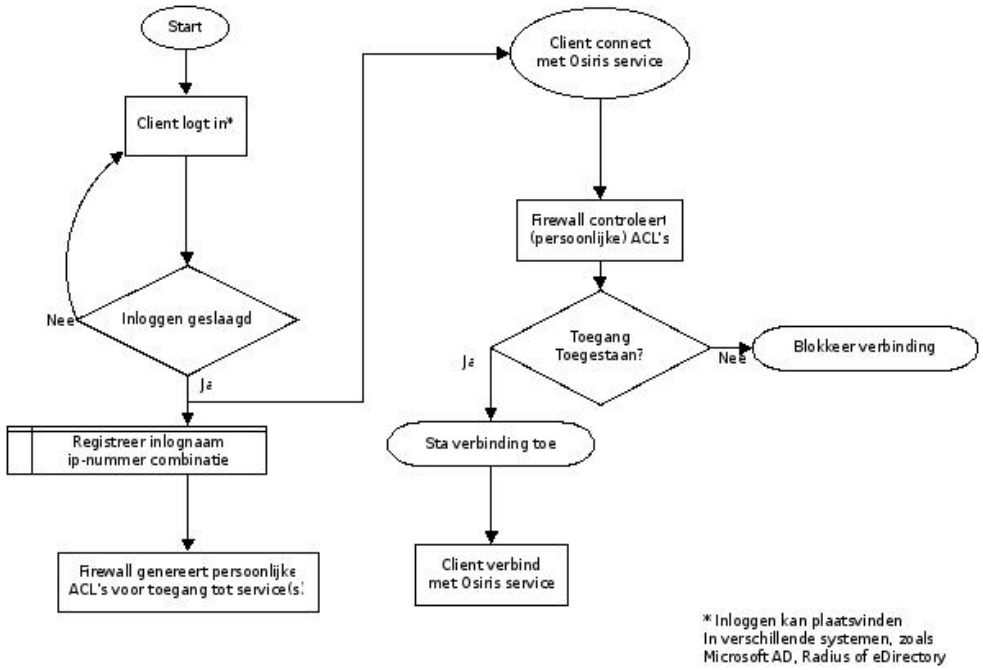
Implementatie van strategie 1 zorgt voor een veilige ontsluiting van de Osiris Backoffice en het afvangen van bovenstaande punten. Indien een globaal ontwerp wordt geschetst van strategie 1 in combinatie met Osiris, wordt een situatie verkregen zoals in figuur 7.1.



Figuur 7.1: Globaal ontwerp strategie 1 in combinatie met Osiris.

Hierin is te zien dat de Osiris Database in het FH netwerk en Osiris Student in het AL netwerk, toegankelijk zijn zoals in de ACL van de core-switch is ingericht. Indien er een connectie wordt gemaakt naar de Osiris Student omgeving, zal dit, zoals voorheen, door de ACL in de core-switch worden toegestaan of geblokkeerd.

De Osiris Backoffice omgeving is in een apart, extra beschermd, servernetwerk gezet, afgescheiden door een geavanceerde firewall. Indien er een connectie wordt gemaakt door een medewerker/docent naar de Osiris Backoffice omgeving, zal eerst door de firewall worden bepaald of deze persoon geautoriseerd is om naar Osiris Backoffice te mogen. Indien de persoon wél is geautoriseerd, wordt de connectie naar de Osiris Backoffice omgeving toegestaan. De Osiris Backoffice behoud wel zijn eigen wijze van authenticeren en autoriseren. Indien de persoon niet is geautoriseerd, wordt de connectie geweigerd. Het flowschema in figuur 7.2 illustreert hoe dit proces in zijn werking gaat.



Figuur 7.2: Flowschema authenticatieproces Osiris Backoffice.

Bij deze strategie kan een gebruiker vanaf elk gebruikersnetwerk bij de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, zolang de gebruiker maar is geauthenticeerd aan het netwerk. Gebruikers die niet zijn geautoriseerd voor het gebruik van Osiris, kunnen ook niet met de Osiris Backoffice communiceren. Op welke manier de authenticatie plaats vindt, maakt bij deze strategie niet uit, zolang de koppeling van het authenticatiemechanisme met de firewall aanwezig is en de user/ip-mapping kan worden gecreëerd.

Indien er gebruikers van het Internet af komen en naar de services/applicaties in het afgeschermde netwerk willen, kan er door Avans worden gekozen om dit via een VPN of sterk-authenticatie mechanisme te ontsluiten.

Aan de hand van dit hoofdstuk is geïllustreerd hoe de geadviseerde strategie in de praktijk zou kunnen functioneren.

8 - Privacy aspecten

Bij een implementatie van persoonsgebonden toegang, of dit nu digitaal of een andere vorm van toegang is, wordt geregistreerd wie wanneer toegang heeft of heeft gehad. Zo ook bij de implementatie van strategie 1: Avans kán zien wie er wanneer toegang heeft tot de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, maar ook wat er voor verkeer is uitgewisseld, doordat er gebruik wordt gemaakt van een geavanceerde firewall. Beveiliging van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang worden door middel van deze techniek beveiligd en gemonitord.

Bij het registreren van deze gegevens, dient de werkgever te voldoen aan wet- en regelgeving op dit gebied. Het persoonsgebonden registreren van netwerk- en internet verkeer is relatief nieuw. De wet- en regelgeving past zich aan op de ontwikkelingen op dit gebied en is continu aan veranderingen onderhevig door reactie op deze ontwikkelingen. Daardoor is er nog geen eenduidige wet- en regelgeving aanwezig.

In dit document worden een aantal overwegingen beschreven die gedurende het onderzoek ter sprake zijn gekomen op het gebied van privacy en de gevolgen van de keuze voor strategie 1.

8.1 Overweging 1

De eerste overweging die ter sprake is gekomen bestaat uit de volgende vraag:
Is er bij de geselecteerde strategie, waarbij sprake is van het vastleggen van persoonsgebonden gegevens met betrekking tot netwerkverkeer, sprake van persoonsgegevens of privacy inbreuk?

Hierbij dient eerst te worden vastgesteld óf er sprake is van persoonsgegevens en de verwerking ervan. De Wet Bescherming persoonsgegevens definieert persoonsgegevens en de verwerking ervan als volgt:
Artikel 1, lid a[28]:
"*persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*[28]".
Artikel 1, lid b[28]:
"*verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens*[28]".

Uit de Wet Bescherming Persoonsgegevens blijkt dat het wél gaat om persoonsgegevens en de verwerking ervan. Er wordt namelijk een gebruikersnaam, welke te herleiden is tot een natuurlijk persoon, gekoppeld aan een IP-adres. Met deze gegevens wordt vervolgens een verzameling van netwerkverkeer gegevens opgebouwd die zijn te herleiden naar dezelfde natuurlijke persoon. Bij deze strategie is de Wet Bescherming Persoonsgegevens van kracht.

Maar is er dan sprake van privacy inbreuk voor de gebruikers die gebruik maken van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang? Naar alle waarschijnlijkheid is het antwoord daarop: "nee". De services/applicaties die in aanmerking komen voor persoonsgebonden toegang bevatten persoons- en bedrijfsgegevens. Op het beschermen van persoonsgegevens is artikel 13 van de Wet bescherming Persoonsgegevens[28] van kracht, welke stelt dat:
"*De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.*[28]".
Strategie 1 is in deze de passende technische maatregel ter beveiliging van deze persoonsgegevens.

Wat betreft het op deze manier beveiligen van bedrijfsgegevens kan worden gesteld dat is toegestaan, mits dit aan medewerkers is bekendgemaakt. Bij Avans dient de werknemer akkoord te gaan met het beveiligingsbeleid bij indiensttreding. Het College Bescherming Persoonsgegevens beschrijft de volgende inhoud van zo een beleid:
"Persoonsgegevens mogen slechts voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden verwerkt worden. Deze doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn. In overleg moet worden vastgesteld welke doeleinden voor controle van e-mail en internetgebruik noodzakelijk zijn voor de eigen organisatie. De privacybelangen van de werknemers horen hierbij meegewogen te worden.[27]"

Bovenstaand citaat geldt niet alleen voor internet en e-mailverkeer, maar eigenlijk voor alle netwerkverkeer. Als er wél naar de communicatie inhoud wordt gekeken, moet dat zeker zijn vastgelegd onder welke voorwaarden dit gebeurd. De systeembeheerders die de gegevens mogen bekijken, hebben geheimhoudingsplicht, welke ook dient te worden vastgelegd:
"De systeembeheerder is als het ware de sleutel tot de persoonsgegevens over het gebruik van e-mail en internet. Vanuit het oogpunt van de privacy is het belangrijk om afspraken te maken over wie in welke gevallen opdracht kan geven over de controle. Ook de geheimhoudingsplicht (artikel 12, lid 2, WBP) moet ter sprake komen in verband met de eigen integriteit van de systeembeheerder.[27]" Beheerders bij Avans hebben een geheimhoudingsverklaring getekend.

8.2 Overweging 2

Ook de tweede overweging bestaat uit een vraag:
Het doel bij strategie 1 voor het persoonsgebonden monitoren van netwerkverkeer is sturing.
Het is technisch wel mogelijk om van het geregistreerde verkeer naar de communicatie inhoud kunnen kijken. Mag dat?

Het antwoord op deze vraag is: "nee". Dat mag niet zomaar. Het monitoren zoals gebeurd in strategie 1, valt onder de noemer "generiek monitoren". Bij generiek monitoren is het niet toegestaan naar de communicatie inhoud te kijken. Bij strategie 1 gaat het echter niet om de inhoud van de communicatie, maar om sturinggegevens. De persoonsgegevens die worden vastgelegd, worden gebruikt om de beveiliging en toegang van de systemen te realiseren en niet om te controleren wat de medewerker op de systemen uitvoert. Indien er sprake is van misbruik, dient wel in het beveiligingsbeleid te zijn vastgelegd hoe er moet worden gehandeld.

9 - Conclusie

Er is onderzoek gedaan naar gangbare strategieën voor persoonsgebonden toegang, zoals deze door Avans is gewenst voor het beter en flexibeler beveiligen van services/applicaties die persoons- of bedrijfsgegevens bevatten. De aanleiding hiervoor is de groter wordende mobiliteit, waardoor het huidige beveiligingsmodel in toenemende mate een belemmering vormt

Onderzoek in de literatuur heeft vier mogelijke strategieën opgeleverd die toepasbaar kunnen zijn voor het oplossen van de probleemstelling. De strategieën zijn als volgt:
Strategie 1: Servers in afgeschermd netwerk, dynamische ACLs aan gebruiker koppelen.
Strategie 2: Servers in afgeschermd netwerk, afgeschermd en getunneld netwerkverkeer.
Strategie 3: Clients controleren voordat toegang wordt verleend op basis van een NAC/NAP oplossing van Cisco en Microsoft.
Strategie 4: Verplaatsen van clients in netwerken na authenticatie en toekennen van een persoonsgebonden ACL.

De beoordelingen van de strategieën levert de volgende resultaten:

- Alle strategieën voldoen aan de eisen wat betreft het bieden van de benodigde bescherming en gewenste flexibiliteit voor de services/applicaties die in aanmerking komen voor persoonsgebonden toegang.
- Alle strategieën passen binnen het huidige beveiligingsmodel van Avans en voegen daarbij een extra beveiligingslaag toe aan het interne netwerk.
- Bijna alle strategieën zijn bruikbaar voor alle gangbare end-user devices, waarbij strategie 3 een uitzondering is. Deze ondersteunt alleen Microsoft Windows systemen.
- De meeste strategieën, met uitzondering van strategie 1, vergen een gebruikers actie, doordat een client op het end-user device is vereist.
- Alle strategieën zijn beheerintensief, met uitzondering van strategie 1. Strategie 1 heeft de laagste beheerlast, omdat de gebruiker bij deze strategie geen beheer hoeft te voeren.
- Voor alle strategieën zal een investering moeten worden gedaan bij implementatie van de strategie. Bij de strategieën 1 en 4 is de investering afhankelijk van de keuze die in het ontwerp wordt gemaakt.

Strategie 1 onderscheidt zich op de volgende punten van de overige strategieën:

- Door het centraal georiënteerde beheer en de afwezigheid van een client voor het end-user device, zijn de beheerlasten lager dan bij de andere strategieën, welke allen een actie vragen van zowel beheerders als gebruikers.
- De ondersteuning van alle gangbare end-user devices.
- De oplossing is transparant, doordat deze in de netwerklaag is ingebed.

Op basis van bovenstaande beoordeling sluit deze strategie het beste aan bij de door Avans gewenste flexibele beveiliging van services/applicaties die in aanmerking komen voor persoonsgebonden toegang.

Binnen de geadviseerde beveiligingsstrategie worden persoonsgebonden netwerkverkeergegevens vastgelegd, welke worden ingezet ter beveiliging van persoons- en bedrijfsgegevens. Bij deze strategie zou de vraag kunnen opkomen of er inbreuk wordt gemaakt op de privacy van de gebruikers. Echter, doordat de strategie wordt ingezet als beveiligingselement voor persoonsgegevens en er sprake is van generiek monitoren met sturing als doel, is er vermoedelijk geen sprake van inbreuk op de Wet Bescherming Persoonsgegevens. Het is echter wel aan te bevelen om voor de gekozen strategie de gegevens die worden vastgelegd en de wijze waarop, op te nemen in het beveiligingsbeleid van Avans.

Het persoonsgebonden monitoren van netwerkverkeer zoals wordt gedaan in strategie 1 is relatief nieuw. Daardoor heerst er veel onduidelijkheid over wat er wel en niet mag volgens de wet. De wet- en regelgeving past zich aan op de ontwikkelingen op dit gebied en is continu aan veranderingen onderhevig door reactie op deze ontwikkelingen.

10 - Aanbevelingen

Dit onderzoek is een eerste stap voor het realiseren van persoonsgebonden en plaatsonafhankelijke toegang binnen Avans. Voor het vervolgtraject kunnen nog een aantal aanbevelingen worden gegeven. Deze zijn in dit hoofdstuk beschreven.

Business Case
Aan te bevelen valt om na dit onderzoek een vervolgtraject te starten waarin een business-case wordt uitgewerkt op basis van de aanbevolen strategie: het plaatsen van servers in een afgeschermd netwerk, waarbij een firewall geplaatst wordt tussen de services/applicaties en de gebruikers.

Aanbevolen wordt om in de business-case de volgende onderdelen op te nemen:

- Kosten en baten van de strategie in al zijn varianten.
- De verschillende varianten van de strategie. De strategie kan technisch worden gerealiseerd op het huidige firewall-cluster, maar aanbevolen wordt om dit op een eigen firewall omgeving onder te brengen.
- Onderzoek naar de werkelijke beheerlast.
- Tijd die het kost om de strategie en de gekozen variant te implementeren.
- Een gedegen risicoanalyse.

Proof of Concept
Aanbevolen wordt om na de selectie van een variant op strategie 1, een Proof of Concept uit te voeren. Met een Proof of Concept kan worden getoetst of de strategie die is geselecteerd, ook in de praktijk haalbaar is.

Applicatie inventarisatie
Aanbevolen wordt om een meer uitgebreide inventarisatie of selectie van services/applicaties uit te voeren die in aanmerking komen voor persoonsgebonden toegang. In de inventarisatie van dit onderzoek is gekozen om een inventarisatie te maken van de services/applicaties met een grote gebruikerspopulatie of services/applicaties die een primair bedrijfsproces dienen. Deze gekozen strategie kan, indien gewenst, breder worden ingezet. Dit houdt in dat ook de wat kleinere services/applicaties op deze manier kunnen worden voorzien van persoonsgebonden toegang.

11 - Evaluatie van het afstudeeronderzoek

De basis voor het afstudeeronderzoek, is het Plan Van Aanpak, welke is te vinden in bijlage 1. In deze leidraad staat beschreven hoe het onderzoek wordt gedaan, welke producten worden opgeleverd en de tijdplanning van het onderzoek. Het Plan van Aanpak is in dit onderzoek de rode draad geweest, maar gaandeweg het onderzoek zijn er een paar wijzigingen doorgevoerd. Deze worden hieronder toegelicht:

- De afstudeeropdracht:
    - Er zijn geen drie, maar vier strategieën voor persoonsgebonden toegang uitgewerkt. De rede hiervoor is dat deze vier strategieën de meest gangbare technieken zijn voor persoonsgebonden toegang en ik het daarom een verbetering van het onderzoek vind om er vier uit te werken in plaats van drie.
    - Proof of Concept: dit onderdeel is komen te vervallen na overleg met de eerste examinator. Hij en ik waren het er beide over eens dat een goed gestructureerd onderzoek beter is dan een Proof of Concept.

- De producten:
    - Applicatie Selectie overzicht: is hernoemd naar Applicatie inventarisatie. In dit onderzoek is er namelijk geen sprake van een selectie van applicaties die zeker gaan worden geselecteerd voor persoonsgebonden toegang. Wel een inventarisatie van applicaties waarvan de onderzoekers denken dat deze in aanmerking komen voor persoonsgebonden toegang. Ook kunnen deze applicaties in het onderzoek dienen als voorbeeld voor de toetsing van de aanbevolen strategie.
    - Literatuuronderzoek en inventarisatie technieken: is hernoemd naar Onderzoek naar strategieën voor persoonsgebonden toegang. Na overleg met de eerste examinator is besloten dit hoofdstuk geen literatuuronderzoek te noemen. De strategieën die in dit onderzoek zijn beschreven, zijn zo relatief nieuw, dat er geen “traditionele” literatuur over deze strategieën beschikbaar is. Het onderzoek heeft zich gericht op informatie van fabrikanten van dergelijke oplossingen.
    - Beleidsadvies: is hernoemd naar privacy aspecten. Gaandeweg het onderzoek is besloten om ons meer te focussen op de privacy aspecten van de aanbevolen strategie. Hieruit volgt vanzelf een beleid, aangezien dat door wet- en regelgeving is voorgeschreven.
    - Beheerlast Inventarisatie: is komen te vervallen en verwerkt in het onderzoek als zijnde een beoordelingscriterium. Deze keuze vonden we beter passen bij het onderzoek.
    - Toepasbaarheidsrapportage: Naam is gewijzigd in voorbeelduitwerking. Dat de strategie toepasbaar is, blijkt al uit het onderzoek dat is uitgevoerd. In de voorbeelduitwerking is één van de services/applicaties die in aanmerking komen voor persoonsgebonden toegang, uitgewerkt.

Buiten deze veranderingen is het project opgezet zoals is beschreven in het Plan van Aanpak. Het Plan van Aanpak is te vinden in Bijlage 1. De achtergrondinformatie zoals deze in de eerste hoofdstukken is beschreven, is beperkt gehouden tot datgene wat noodzakelijk is voor de positionering van het onderzoek.

12 - Bronvermeldingen

1. Defense in Depth afbeelding; weblink : http://technet.microsoft.com/en-us/library/cc512681.aspx

2. Nessus Product Overview; Tennable Network Security; weblink: http://www.tenable.com/products/nessus/nessus-product-overview

3. IEEE Standard for Local and metropolitan area networks; 19 mei 2006; weblink: http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf

4. BizzDesign Architect; weblink: www.bizzdesign.com

5. Archimate Refrence architecure; informatie over ArchMate referentie architectuur; weblink: http://www.opengroup.org/archimate/

6. Architectuurschets van het Avans netwerk; Avans Hogeschool; weblink: http://architectuur.avans.nl/diagram11650.html#netwerkbeveiliging_lagen
   Links is afgeschermd en alleen toegankelijk voor medewerkers van Avans.

7. 802.1x informatie; weblink: http://www.ieee802.org/1/pages/802.1x-2004.html

8. Radius protocol informatie; weblink: http://technet.microsoft.com/nl-nl/library/cc781821%28v=ws.10%29.aspx

9. Definitie LDAP protocol; weblink: http://www.rfc-editor.org/rfc/rfc4511.txt

10. SAML2 definitie; weblink: http://www.xml.com/pub/a/2005/01/12/saml2.html

11. Omschrijving Osiris, uitwerking opdracht NEAM1, opleiding systeembeheer duaal, vakcode DU1-NEAM1; 15-11-2009; Netwerkarchitectuurmodellen, Osiris Avans, Opdracht NEAM 1; David Schrok.

12. Hogeschool Utrecht mediatheek; Hogeschool Urecht; weblink: http://www.mediatheek.hu.nl/Mediatheek/Informatiebronnen/Databanken.aspx

13. Specificatieoverzicht Palo Alto 5050 firewall; Palo Alto networks; 2012; weblink: http://www.paloaltonetworks.com/literature/datasheets/PA5000_Specsheet.pdf

14. VPN Technologies: Definitions and requirements; VPN Consortium; July 2008; weblink: http://www.vpnc.org/vpn-technologies.html

15. Different Flavours of VPN; JaNet (UK); 03 july 2007; weblink: http://www.ja.net/documents/development/vpn/different-flavours-of-vpn-web.pdf

16. How Virtual Private Networks Work; Cisco Networks; Document ID 14106; weblink: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.shtml#vpn_tech

17. Palo Alto Networks Administrator Guide 4.1; Palo Alto Networks; 2007-2011; weblink: http://digitalscepter.com/wp-content/uploads/PAN-Guides/Palo-Alto-4.1_Administrators_Guide.pdf

18. SSL VPN User Guide - Novell Access Manager; Novell, Inc; October 2011; weblink: http://www.novell.com/documentation/novellaccessmanager31/pdfdoc/sslvpnclienthelp/sslvpnclienthelp.pdf

19. Windows Server 2008 Remote Access Options; Microsoft Corporation; 09 june 2010; weblink: http://technet.microsoft.com/en-us/security/ff730324#HTTP_VPN

20. OpenVPN; OpenVPN Website; OpenVPN Technologies; weblink: http://openvpn.net/

21. Cisco Access Control Server; Cisco Systems; weblink: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

22. Cisco NAC and Microsoft NAP Interoperability Architecture - Cisco Network Admission Control and Microsoft Network Access Protection Integration Deployment Guide; Cisco Networks; weblink: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns466/ns812/guide_c07-491729.html

23. Appendix D: NAP-NAC Design; Microsoft Technet; 29-02-2012; weblink: http://technet.microsoft.com/en-us/library/dd125393(v=ws.10).aspx

24. Wired 802.1x Security; Mohammed Younus; SANS Institute; 2000-2005; weblink: http://www.sans.org/reading_room/whitepapers/firewalls/wired-8021x-security_1654

25. Catalyst 6500 Series Software Configuration Guide - Configuring 802.1x Authentication; Cisco Systems; weblink: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/catos/8.x/configuration/guide/8021x.html

26. Belemmeringen in een veranderproces; Gertjanschop.com; weblink: http://www.gertjanschop.com/praktijkcaseveranderen/3_8__programma_van_eisen.html

27. Goed werken in netwerken. Regels voor controle op e-mail en internetgebruik van werknemers; Terstegge, mr. drs. J.H.J. ; 2e druk, april 2002; weblink: http://www.cbpweb.nl/Pages/av_21_Goed_werken_in_netwerken.aspx

28. Wet bescherming persoonsgegevens; Overheid.nl; weblink: http://wetten.overheid.nl/BWBR0011468/geldigheidsdatum_14-05-2012

29. Rechtmatig operationeel handelen in ICT; Bert-Jaap Koops, Colette Cuijpers, Paul de Hert; Universiteit van Tilburg, TILT - Centrum voor Recht, Technologie en Samenleving; Versienummer 1.0, mei 2011; weblink: http://www.surfnet.nl/Documents/rapport_201105_rechtmatig_operationeel_handelen_in_ICT.pdf

13 - Begrippen en Afkortingen

- **802.1x:** 802.1x is een IEEE standaard die een authenticatiemechanisme beschrijft voor poort-gebaseerde netwerk toegang. Met 802.1x is fysieke netwerk toegang te beveiligen met inlognaam en wachtwoord.
- **ACL - Access Control List:** Een lijst met regels op routers of switches die de toegang tussen diverse netwerken reguleert.
- **Building Concentrator:** Vervult dezelfde taken als een core-switch, echter voor een via OSI laag 3 gekoppelde nevenvestiging.
- **BYOD - Bring Your Own Device:** Principe waarmee iedereen met zijn eigen device, zowel privé als van de zaak, kan meenemen om zijn werkzaamheden te kunnen vervullen.
- **Core-router:** Een hardware device dat in de het hart van het netwerk voor de routering van netwerkpakketten zorgt.
- **CRM - Customer Relationship Management:** is een werkwijze en technologie voor het beheren van klant- en relatiegegevens van een onderneming.
- **ELO - Elektronische Leer Omgeving:** Een applicatie omgeving die is ontworpen om educatieve inhoud en de organisatie van leerprocessen aan te bieden. Binnen Avans is het Blackboard E-learning systeem geïmplementeerd.
- **IPSec - IP Protocol Security**: IPSec is een verzameling van standaard protocollen, die het mogelijk maken om een versleutelde verbinding tot stand te brengen en wordt onder andere gebruikt als VPN techniek.
- **L2TP: Layer 2 Tunneling Protocol**: L2TP is een OSI Laag 2 protocol dat is ontwikkeld voor het tunnelen van netwerkverkeer tussen 2 peers. Wordt veel gebruikt bij tunnel-vpn oplossingen. Kan worden voorzien van versleuteling door middel van IPSec.
- **LDAP - Lightweight Directory Access Protocol:** LDAP is een netwerkprotocol dat beschrijft hoe gegevens uit een directory service, zoals Active Directory of eDirectory, benaderd moet worden over TCP/IP.
- **LIC - Leer- en Innovatie Centrum:** De afdeling die verantwoordelijk is voor de Studentenleeromgeving en mediatheek van Avans.
- **Microsoft Active Directory:** is een directory service gebaseerd op Microsoft technologie. Active directory is een centrale en gestandaardiseerde omgeving voor het beheer van gebruikers objecten, gedistribueerde objecten zoals printers en servers, en beveiliging van een Microsoft infrastructuur.
- **MPLS: Multi Protocol Layer Switching**: MPLS is een mechanisme dat actief is op Laag 2 of 3 van het OSI-model en netwerkpakketten van een label voorziet. Routering en switching gebeurd op basis van de labels en niet op basis van de ip-pakketten. Dit zorgt voor snelheidswinst en een lagere hardware belasting.
- **NAD - Network Access Device**: Is een benaming voor een apparaat waarop een user-device is aangesloten. Dit kan een switch of WLAN Access Point zijn.
- **Next-Generation firewall**: Een next-generation Firewall is in staat om netwerk verkeer te filteren op applicatie niveau en applicaties te herkennen ongeacht poort en protocol.
- **Novell eDirectory:** is een directory service gebaseerd op Novell technologie. Novell eDirectory is een centrale en gestandaardiseerde omgeving voor het beheer van gebruikers objecten, gedistribueerde objecten zoals printers en servers, en beveiliging van een beheerde infrastructuur.
- **OSI-model**: Het OSI model is een model dat beschrijft hoe data wordt verstuurd over een netwerk. Het OSI model bestaat uit zeven lagen: toepassing, presentatie, sessie, transport, netwerk, datalink en fysiek.
- **PPP - Point to Point Protocol**: Het PPP protocol is gemaakt om computers via modems met elkaar te verbinden.
- **PPTP - Point to Point Tunneling Protocol**: PPTP is een doorontwikkeling van het PPP protocol. Bij PPTP worden de PPP-pakketten door middel van een versleutelde tunnel van het begin naar het eindpunt getransporteerd.
- **Radius - Remote Authentication Dial In User Service:** RADIUS is een netwerk protocol dat gecentraliseerde authenticatie, autorisatie en accounting realiseert. RADIUS is bij Avans gekoppeld aan de LDAP omgeving van Novell.

- **SAML2 - Security Assertion Markup Language 2.0:** SAML is een op XML gebaseerd framework voor het uitwisselen van beveiligings- en identiteitsinformatie en is gericht op het ontsluiten van webapplicaties of webservice.
- **SSH - Secure Shell**: SSH is een applicatieprotocol dat wordt gebruikt om op afstand in te loggen op systemen die SSH ondersteunen. SSH is een doorontwikkeling van telnet. SSH is een terminalomgeving, welke vooral wordt gebruikt op Unix/Linux systemen of andere systemen met terminal toegang, zoals switches en routers.
- **SSL: Secure Socket Layer**: SSL is een encryptieprotocol dat wordt gebruikt om communicatie tussen twee computersystemen te versleutelen.
- **VLAN - Virtual Local Area Network:** Techniek waardoor er virtuele netwerken kunnen gebouwd die logisch worden gescheiden op basis van VLAN-tag.
- **VPN - Virtual Private Network**: Een Virtual Private Network is een goedkope manier om beveiligde verbindingen op te bouwen over een open netwerk zoals Internet, waarbij de vertrouwelijkheid over een bestaande verbinding behouden blijft.
- **WLAN - Wireless Local Area Network:** Een netwerk gebaseerd op de 802.1a/b/g/n standaard, wat inhoud dat devices draadloos kunnen worden verbonden met een netwerk. Deze techniek wordt ook WiFi genoemd.

14 - Bijlagen

Hieronder zijn de bijlagen bij dit onderzoek beschreven.

1. Plan van Aanpak Afstuderen.
2. Evaluatie David Schrok.
3. Omschrijvingen applicaties die in aanmerking komen voor persoonsgebonden toegang.

Projectvoorstel Afstuderen

Making Avans even more secure...

Auteurs:	David Schrok
Studentnr:	1551536
e-mail:	david.schrok@student.hu.nl
Klas:	SI6b
Versie:	3.0
Vak:	Afstuderen
Vakcode:	TCIF-DU6AFST-05
Datum:	08-02-2011

Inhoudsopgave

1 - Inleiding

In dit document wordt het onderzoeksproject omschreven dat gaat worden uitgevoerd als afstudeerproject van David Schrok. Het afstudeerproject is onderdeel van de studie Systeembeheer Duaal aan de Hogeschool Utrecht.

In dit afstudeervoorstel wordt omschreven:

- De organisatie waarbinnen het afstudeerproject wordt uitgevoerd;
- De positie van de student binnen het bedrijf;
- Een probleembeschrijving waaruit het onderwerp van het afstudeeronderzoek volgt;
- Een globale formulering van het afstudeeronderzoek;
- De relatie van het afstudeeronderzoek met andere projecten/onderzoeken;
- De relatie van het afstudeeronderzoek tot de hoofdfase van de opleiding;
- De op te leveren producten gedurende het afstuderen;
- Een globale planning van het afstudeeronderzoek;
- De uitdaging van de student;
- Het voorstel voor beoogde bedrijfsbegeleider;
- De bedrijfs- en persoonsgegevens van het bedrijf, bedrijfsbegeleider en student.

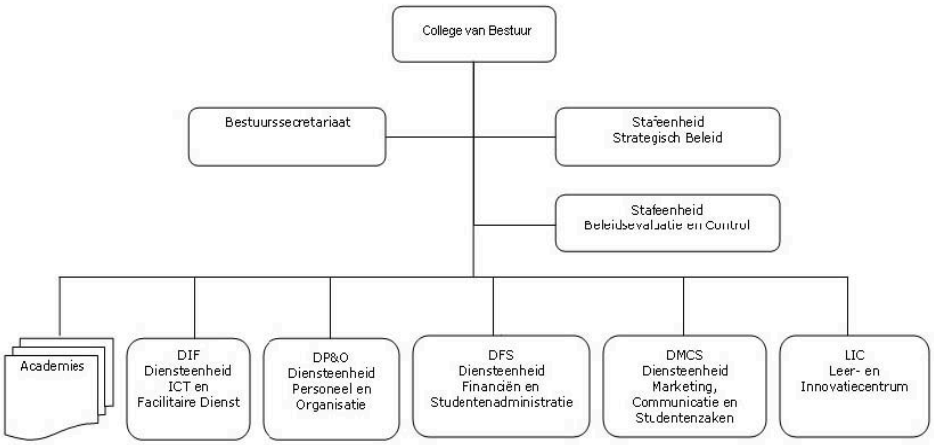
Als onderwerp van de afstudeeropdracht is gekozen om onderzoek te doen naar een flexibelere manier van toegang voor systemen die bedrijfsgevoelige informatie bevatten. Op dit moment bepaalt de plaats van een device in het netwerk, welke systemen vanaf die plaats in het netwerk bereikbaar zijn. Het is een wens van Avans dat ook de gebruikersgegevens bepalen welke systemen bereikbaar zijn en niet meer de plaats van de systemen in het netwerk, waardoor meer flexibiliteit wordt gecreëerd.

Deze opdracht onderzoekt de mogelijkheden hiertoe, levert een aanbeveling en, indien nodig, een ‘Proof of Concept’ op waarin de mogelijke oplossingen voor het geschetste probleem worden getest.

2 - Situatieschets Avans Hogeschool

Avans is een onderwijs organisatie ontstaan uit een fusie van de Hogescholen Brabant en Hogeschool 's-Hertogenbosch. Met 6 locaties verdeeld over de steden Breda Tilburg en 's-Hertogenbosch is het één van de grote Hogescholen van Nederland. Avans biedt 54 verschillende HBO opleidingen in de sectoren Economie en Management, Gezondheid, ICT, Kunst en Vormgeving, Onderwijs, Techniek, Recht en Welzijn. Avans Hogeschool biedt onderwijs aan ongeveer 26.000 studenten en heeft ruim 2500 medewerkers.

Avans is opgebouwd rond een medezeggenschapsstructuur. Avans Hogeschool heeft twee stafeenheden, namelijk het College van Bestuur en de Raad van Toezicht. Deze worden ondersteund door het Bestuur-secretariaat, Stafeenheid Strategisch Beleid en Stafeenheid Beleidsevaluatie en Control. Daaronder bevinden zich de 19 verschillende academies en 5 ondersteunende diensten.



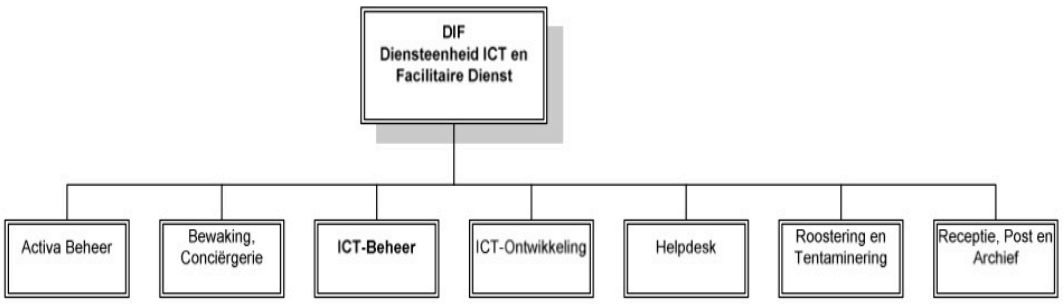
Afbeelding 1: Organogram Avans Hogeschool

De Dienst ICT en Facilitair (DIF) is een van de 5 ondersteunende diensten.
DIF is een afdeling die gericht is op de algemene dienstverlening naar de studenten en medewerkers toe. Hierbij valt te denken aan alle ICT gerichte zaken, zoals helpdesk en ICT-beheer, facilitaire zaken zoals bewaking en gebouwenbeheer, roostering en archivering.

De Dienst ICT en Facilitair bestaat uit de volgende subafdelingen:

- Activa Beheer;
- Bewaking en Conciërgerie;
- ICT-Beheer;
- ICT-Ontwikkeling;
- De Servicedesk;
- De Helpdesk;
- Roostering en Tentaminering;
- Receptie, Post en Archief.

In onderstaande afbeelding is de organisatiestructuur van DIF weergegeven.



Afbeelding 2: Organogram Dienst ICT en Facilitair

Het onderzoek zal worden uitgevoerd door de afdeling ICT-ontwikkeling van DIF.

2.1 - Positie student binnen Avans Hogeschool

Binnen Avans Hogeschool ben ik vanaf 2005 werkzaam in de ICT. Sinds 1 januari 2011 ben ik werkzaam als netwerkbeheerder bij de afdeling ICT-Beheer van de Dienst ICT en Facilitair. De taak van netwerkbeheer is het onderhouden en verbeteren van de netwerkinfrastructuur van Avans Hogeschool, het adviseren van het management op het gebied van netwerkbeheer en het maken van de investeringsbegroting behoord ook tot onze taak.

De werkzaamheden vinden plaats op alle locaties van Avans. Dit zijn de locaties in Breda (Hogeschoollaan, Lovensdijkstraat, Beukenlaan), 's Hertogenbosch (Onderwijsboulevard, Hervenplein) en Tilburg (Cobbenhagenlaan).
Hierbij kan men denken aan:

- Het onderhouden en verbeteren van het hogeschool-brede wifi-netwerk;
- Het beheer van de firewalls;
- Het beheren van de vaste netwerkinfrastructuur;
- IP-adres-management;
- Netwerk beveiliging;
- Het beheer van QuarantaineNet;
- Het monitoren van het netwerk en proactief reageren op gebeurtenissen aan de hand van deze monitoring.

Voor het beheer van het netwerk maakt netwerkbeheer hoofdzakelijk gebruik van de volgende gereedschappen, die tevens door mij is ingericht en wordt onderhouden:

- PRTG: Actieve netwerkmonitoring voor netwerkcomponenten en services;
- KiWi Cattools: Tool die wordt gebruikt voor het geautomatiseerd uitvoeren van command-line gebaseerde scripts voor Cisco apparatuur, de WiFi-controllers van Trapeze/Juniper en de Palo Alto Firewalls;
- Kiwi Syslog Server: Wordt gebruik voor centrale systeem logging. Alle netwerkapparatuur stuurt de logging door naar de Kiwi Syslog Server
- Trapeze Ringmaster: Tool voor het beheer van het Juniper/Trapeze WiFi netwerk van de Hogeschool.
- Man And Mice: DHCP en DNS beheer tool voor het centraal managen van de DHCP en DNS servers.

- Clientele: Registratietool aangaande incidenten en verzoeken, gebaseerd op ITIL. Alle diensten maken gebruik van Clientele. Netwerkbeheer heeft een eigen oplosgroep genaamd ICTB_Netwerk.
- Wombat: Wombat is een door Avans zelf ontwikkelde applicatie voor het beheer van de wall-outlet-administratie en het configureren van deze wall-outlets. Wombat is dan ook de afkorting voor WallOutlet Management Beheer en Administratie Tool.

De firewalls en QuarantaineNet worden via een webbrowser beheerd. Deze beheertools staan uiteraard in een volledig afgeschermd netwerk en zijn alleen toegankelijk voor beheerders.

Naast de werkzaamheden bij netwerkbeheer, ben ik ook lid van het Computer Security Incident Response Team (CSIRT) van Avans. Get CSIRT van Avans draagt zorg voor het, met de juiste voortvarendheid, afhandelen van veiligheidsincidenten op het gebied van ICT. Daarnaast is zij het contactadres van Avans met betrekking tot ICT Security Incidenten. Andere taken van het CSIRT:

- Advies geven op het gebied van informatie beveiliging;
- Het dienen als klankbord/adviesorgaan met betrekking tot ingediende Request For Change's (RFC's), lopende projecten of vragen vanuit de interne organisatie;
- Het creëren van bewustwording bij gebruikers en communicatie met gebruikers over ICT beveiliging;
- Het CSIRT dient als crisisteam bij computer gerelateerde beveiligingsincidenten.

Alle beveiligingsincidenten worden geregistreerd in Clientele, zodat de voortgang kan worden bewaakt door de leden van het CSIRT. Aan het hoofd van het CSIRT staat de Security Manager.

2.2 De afdeling waar het afstudeeronderzoek zal plaatsvinden

De opdracht wordt uitgevoerd bij de afdeling ICT-Ontwikkeling. De afdeling ICT-Ontwikkeling is verantwoordelijk voor onderzoek naar en vernieuwing van ICT voorzieningen voor Avans Hogeschool. Daarnaast zorgt ICT-ontwikkeling ook voor implementatie van deze nieuwe ICT voorzieningen. De projecten die door ICT-Ontwikkeling succesvol worden afgesloten, zullen worden overgedragen aan ICT Beheer.

Voor het uitvoeren van de opdracht zal ik voor 2 werkdagen per week werkzaam zijn bij de afdeling ICT-ontwikkeling.

3 - Probleemomschrijving

De gebruiker verwacht dat hij/zij zijn werkzaamheden kan verrichten ongeacht de plaats en het type device. Met het huidige gelaagde beveiligingsmodel van Avans is dit niet mogelijk.

Gebruikers worden steeds mobieler. Iedereen heeft een laptop of een mobiel device dat men wil gebruiken in hun privé en werksituatie. Dit heet het Bring-Your-Own-Device principe. De verwachting van de gebruikers is daarbij dat zij hun werkzaamheden kunnen uitvoeren, onafhankelijk van het gebruikte device en de manier waarop ze verbinden met het netwerk. Dit strookt echter niet met het huidige beveiligingsmodel van Avans. Binnen dit model zijn er daarbij twee lagen die bepalen of gebruikers toegang krijgen tot Avans applicaties:

- De plaatsing van de apparaten bepaalt de toegang tot de netwerken waarin de specifieke applicatie zich bevind;
- De gebruikers-authenticatie bepaalt of de gebruikers geautoriseerd zijn voor het gebruik van de betreffende specifieke Avans applicatie.

Gezien het BYOD-principe wil Avans dit gaan flexibiliseren.

Dit probleem kan worden opgelost door niet de fysieke plaats van het device in het netwerk, maar de gebruikersauthenticatie en autorisatie te laten bepalen of toegang tot de netwerken waarin de specifieke applicatie zich bevind, wordt toegestaan. Daarbij wordt er onderzocht of de status van het apparaat (virusscanner, patches enzovoort) en de fysieke locatie als extra criteria voor het wel of niet beschikbaar stellen de Avans applicaties kunnen worden meegenomen. Bij de authenticatie wordt op beperkte schaal gebruik gemaakt van sterke authenticatie. Hier is al onderzoek naar gedaan binnen Avans en de resultaten van dit onderzoek naar sterke authenticatie worden in dit onderzoek meegenomen.

De verbeterde en flexibelere toegang tot systemen is een wens die langer speelt binnen het Avans Computer Security Incident Response Team (CSIRT). Het CSIRT, in de persoon van Ad van Dreumel, security-manager Avans, zal de opdracht voor dit onderzoek verstrekken.

4 - Globale formulering van de opdracht

Er wordt onderzoek verricht naar de mogelijkheden om persoonsgebonden toegang tot bepaalde services/netwerken te verlenen. Dit onderzoek wordt een deelonderzoek van het project “Nieuwe ICT Werkomgeving” (NIW). In het project NIW wordt een nieuwe ICT omgeving aangeboden om plaats- en tijdsonafhankelijk te werken. Dit onderzoek levert een advies voor het vervolgtraject van NIW, door de toegang tot Avans applicaties plaats onafhankelijk te maken. Het huidige traject van NIW wordt afgerond in Augustus 2012. De resultaten van dit onderzoek moeten voor deze tijd bekend zijn.

In dit afstudeeronderzoek worden de volgende onderdelen behandeld:

1. Inventarisatie van de diensten en services die in aanmerking komen voor persoonsgebonden beveiliging en waarbij dit ook gewenst is.
2. Beoordelen, evalueren en eventueel adviseren van de beleidsaspecten met betrekking tot de bij punt 1 genoemde systemen;
3. Onderzoek van de technische (on)mogelijkheden om persoonsgebonden toegang te realiseren op basis van de beschikbare infrastructuur van Avans.
4. Beoordelen en evalueren over de bij punt 3 genoemde mogelijkheden;
5. Adviseren van de oplossingen die gebruikt zou kunnen worden voor persoonsgebonden toegang bij Avans;
6. Onderzoek naar de gevolgen voor ICT-beheer na een implementatie van de aanbevolen oplossing;
7. Deze oplossing toetsen op een bestaand probleem waarbij flexibelere beveiliging is gewenst bijvoorbeeld de koppeling van Corsa met Osiris;
8. Indien nodig, het realiseren van een Proof-Of-Concept met de resultaten uit punt 3.

Buiten de scope van dit onderzoek vallen de volgende onderwerpen:

1. Onderzoek naar vormen van sterke authenticatie of de manier waarop sterke authenticatie wordt toegepast binnen Avans;
2. Er wordt geen nieuw beveiligingsmodel voor Avans ontwikkeld;
3. Er wordt binnen het onderzoek geen nieuwe apparatuur of software geïntroduceerd;
4. De juridische aspecten die nodig zijn voor de implementatie van de gekozen oplossing.

4.1 Trefwoorden die de afstudeeropdracht omschrijven

Het afstudeerproject is te omschrijven met onderstaande trefwoorden:

- Cisco
- Netwerk
- Firewall
- Beleid
- LAN
- Vlan
- afschermen
- Palo Alto
- Beveiliging
- Proof-of-concept
- Beleidsadvies
- Servers
- Bedrijfsprocessen
- techniek

- personen
- plaats in het netwerk
- autorisatie
- devices
- authenticatie
- 802.1X

4.2 Relatie van de opdracht tot andere projecten/onderzoeken

Het onderzoeksproject zoals geformuleerd, heeft aansluiting tot de volgende Avans Projecten:

- Project Sterke Authenticatie: Delen van het onderzoek, waaronder de conclusie en de beleidsaspecten, zullen van invloed zijn op de uitkomsten van dit onderzoek. De resultaten worden meegenomen in dit onderzoek.
- Dit onderzoek wordt een deelonderzoek van het project "Nieuwe ICT Werkomgeving" (NIW). In het project NIW wordt een nieuwe ICT omgeving aangeboden om plaats- en tijdsonafhankelijk te werken. Dit onderzoek levert een advies voor het vervolgtraject van NIW, door de toegang tot Avans applicaties plaats onafhankelijk te maken. Het huidige traject van NIW wordt afgerond in Augustus 2012. De resultaten van dit onderzoek moeten voor deze tijd bekend zijn.

4.3 Relatie van de opdracht tot de hoofdfase van de opleiding

De volgende aspecten zoals behandeld in de hoofdfase van de opleiding Systeembeheer Duaal aan de Hogeschool Utrecht, zullen terugkomen in het project:

- **Beveiliging**: De oplossing die voortkomt uit het afstudeeronderzoek dient te voldoen aan het Informatiebeveiliging beleid van Avans Het toepassen van courante beveiligingstechnieken komen aan bod in de afstudeeropdracht.
- **ICT- Architectuur**: De oplossing die voortkomt uit het afstudeeronderzoek dient volgens de architectuur-principes van Avans te zijn opgezet. Er zal tijdens de uitvoering van het onderzoek ook rekening moeten worden gehouden met de bedrijfsprocessen die zijn gemoeid met de oplossing die voortkomt uit het afstudeeronderzoek.
- **CCNA/CCNP**: Aangezien bij Avans wordt gewerkt met Cisco apparatuur, zal de opgedane kennis van deze modulen worden toegepast.
- **Consultancy**: De kennis opgedaan voor het opzetten van een onderzoeks- en adviesrapport zal hierbij worden toegepast.
- **Methoden en technieken**: Hierbij is kennis opgedaan voor het opzetten van een onderzoek, waarbij gebruik kan worden gemaakt van verschillende onderzoeksmethoden. Eén van de onderzoeksmethoden zal de basis vormen voor het afstudeeronderzoek.
- **Systeemintegratie**: De oplossing die voortkomt uit het afstudeeronderzoek zal gevolgen hebben voor de service die in aanmerking komt voor betere beveiliging. De huidige koppeling van die service met de rest van de infrastructuur zal veranderen.
- **Projectmanagement**: Het afstudeerproject zal worden opgezet volgens de technieken die bij het vak projectmanagement zijn gegeven.
- **Security**: Binnen het afstudeeronderzoek zal rekening gehouden moeten worden met beveiligingsmodellen en best-practices die gangbaar zijn binnen het vakgebied.

5 – Aanpak van het onderzoek

In dit hoofdstuk wordt een globale aanpak omschreven die in het onderzoek gebruik gaat worden. Deze is als volgt:

- Als eerste wordt de huidige situatie van het beveiligingsmodel in kaart gebracht. Hierbij zal duidelijk worden gemaakt hoe de gelaagde beveiliging van Avans er nu uit ziet. Hierbij wordt gebruik gemaakt van de interne documentatie van Avans.
- Inventariseren van de applicaties en services die in aanmerking komen voor persoonsgebonden beveiliging. Door hier een inventarisatie van te maken, kan later technisch worden beoordeeld of er nog aanpassingen per applicatie/service nodig zijn om persoonsgebonden beveiliging mogelijk te maken. Hierbij wordt gebruik gemaakt van de interne documentatie van Avans.
- Er wordt een inventarisatie gedaan van de aanwezige technieken binnen Avans die persoonsgebonden beveiliging mogelijk kunnen maken. Op deze technieken wordt vervolgens literatuuronderzoek uitgevoerd, om de (on)mogelijkheden van alle technieken glashelder te krijgen. Voor het literatuuronderzoek wordt gebruik gemaakt van gecontroleerde bronnen en voor zover noodzakelijk van interne documentatie van Avans.
- Na het literatuuronderzoek vindt er een selectiemoment plaats waarbij de techniek wordt uitgekozen die verder wordt uitgewerkt in het adviesrapport. De selectie zal plaats vinden op basis van het literatuuronderzoek.
- Naar aanleiding van de gemaakte keuze voor een oplossing, wordt onderzocht welke gevolgen de geselecteerde optie heeft voor ICT-beheer ten opzichte van de huidige oplossing.
- Inventariseren beveiligingsmodel en –beleid per applicatie/service die in aanmerking komt voor persoonsgebonden beveiliging, zodat een beleidsadvies kan worden opgesteld voor de beleidsveranderingen die nodig zijn voor de implementatie van de gekozen oplossing.
- De gekozen oplossing wordt getoetst op een voorbeeldsituatie, bijvoorbeel de koppeling tussen Osiris en Corsa.
- Nadat de applicaties die in aanmerking komen voor persoonsgebonden beveiliging en de te gebruiken technieken bekend zijn, zullen deze worden bekeken in een Proof of Concept (PoC). Hierbij wordt getest of de theoretische oplossing in de praktijk ook echt werkt en of deze beheersbaar is.
- De resultaten van de bovenstaande stappen worden uitgewerkt in een adviesrapport. Dit adviesrapport zal ook het eindrapport zijn voor mijn afstudeeropdracht.

6 - Op te leveren producten

- Als eerste zal er een projectvoorstel worden opgeleverd. Hierin staat een globale opdrachtomschrijving en een globale planning. Deze zal moeten worden goedgekeurd, alvorens met het project van start te kunnen gaan. Het projectvoorstel is het huidige document.
- Voor het daadwerkelijke onderzoek van start gaat, wordt er een plan van aanpak opgeleverd. Het plan van aanpak omschrijft gedetailleerd het onderzoeksproject.
- Een beschrijving van het huidige beveiligingsmodel zoals dit wordt gehanteerd binnen Avans. Hierdoor wordt een helder (technisch) beeld gegeven van de huidige manier van beveiligen van Avans. Dit is noodzakelijk om een duidelijk implementatie advies te kunnen geven en om de PoC op te kunnen bouwen (uitgangssituatie)
- Een overzicht van de selectie van de Avans applicaties die in aanmerking komen voor persoonsgebonden beveiliging.
- Een beschrijving naar aanleiding van de inventarisatie van de technische (on)mogelijkheden van de bestaande technische infrastructuur van Avans met betrekking tot de beveiliging.
- Selectierapportage met betrekking tot de te gebruiken technieken voor persoonsgebonden beveiliging.
- Beleidsadvies voor de beleidsveranderingen die nodig zijn voor de implementatie van de gekozen oplossing.
- Een beschrijving die de gevolgen voor de beheerslast beschrijft.
- Een uitwerking voor de toepasbaarheid van de gekozen oplossing op het gekozen voorbeeld.
- Een beschrijving van de Proof of Concept en de conclusies hiervan.
- Het uiteindelijke onderzoek- en adviesrapport, waarin het gehele project is uitgewerkt en alle opgeleverde producten worden opgenomen.

7 - Globale Planning

In dit hoofdstuk wordt een globale planning van het project weergegeven. Deze zal in het plan van aanpak gedetailleerder zijn uitgewerkt.

Projectvoorstel Afstuderen	Oktober 2011 tot 1 januari 2012
Goedkeuring Projectvoorstel afstuderen	Uiterlijk 13 januari 2012
Plan van aanpak	Uiterlijk 16 maart 2012
Voor- en Literatuuronderzoek	Start afstuderen tot 1 mei 2012
Proof Of Concept	1 mei 2012 tot 1 juni 2012
Uitwerken onderzoek en adviesrapport	1 juni 2012

8 – Uitdaging

De uitdaging van het onderzoek zit hem voor mij in drie onderwerpen:

1. Het projectmanagement. Ik ben in mijn huidige positie geen projectleider, maar ik zie het als een uitdaging om die functie op mij te nemen. Zeker om dat je als projectleider bij alle facetten van een project betrokken bent en dan heb ik het vooral over de niet-technische onderdelen. De belangrijkste leerpunten zullen zijn:
    a. Project coördinatie. Dit is redelijk buiten mijn "comfort-zone" en daarnaast kom ik te werken in een organisatieonderdeel waar ik nog niet eerder werkzaam ben geweest,
    b. "Helikopterview" behouden over het project. Het is belangrijk om de grote lijnen te blijven zien. Ik kan mezelf nog wel eens verliezen in de details.
    c. Voortgangsbewaking en planning. Ik kan mezelf nog wel eens verliezen in de tijd, omdat ik iets voor mijn gevoel nog niet 100% heb afgerond.
2. Het technische deel van de opdracht, omdat het een verdieping van mijn huidige kennis zal zijn op het gebied van netwerktechnologie en beveiliging en daarnaast de ICT- en beveiligingsarchitectuur van Avans.
3. Het toepassen van de opgedane kennis tijdens de gehele opleiding. Terugkijkend op de opleiding zijn er vele vakken gevolgd en vele rapporten geschreven, waarbij ik aan mezelf wel merk dat ik in kennis en kunde ben gegroeid. Door de kennis en kunde toe te passen op het afstudeeronderzoek, wil ik ook laten zien dat wat er tijdens de opleiding aan kennis is verworven, ook kan worden toegepast.

Bijlage 2 - Evaluatie eigen functioneren

Terugkijkend op het afstudeeronderzoek dat ik heb uitgevoerd, kan ik zeggen dat ik er tevreden over ben. Ik vind het onderzoek inhoudelijk goed en goed onderbouwd. Tijdens het onderzoek heb ik de focus gelegd op de inhoud van het onderzoek en het binnen de kaders blijven van de opdracht. De opdracht kan ook heel breed worden opgezet, maar juist door het kaderen heeft het onderzoek binnen de gestelde tijd kunnen plaatsvinden.

Het houden aan de planning tijdens het onderzoek is goed gelukt. Het eindrapport was binnen de tijd af en ook het onderzoek zelf is naar tevredenheid van mij en de bedrijfsbegeleider verlopen.

Tijdens het afstudeeronderzoek is er periodiek contact geweest tussen mij en de twee bedrijfsbegeleiders over de voortgang van het onderzoek, waarin de onzekerheden van mij of onzekerheden in het onderzoek konden worden weggenomen. Een persoonlijk leermoment van deze gesprekken en het gehele onderzoek is dat ik meer mag vertrouwen in mijn eigen kunnen en beslissingen. Hierin ben ik soms nog wat onzeker.

Andere leerpunten zijn geweest:

- De projectcoördinatie. Een project coördineren is relatief nieuw voor mij. Binnen het afstudeeronderzoek ben ik zelf verantwoordelijk geweest voor het halen van de planning en de sturing van het project. Hierin ben ik zijdelings wel bijgestaan door mijn bedrijfsbegeider.
- Het toepassen van de kennis die is opgedaan tijdens de opleiding: Ik merk aan mezelf dat ik met meer aspecten rekening houd tijdens een onderzoek dan voorheen. Voorheen had ik sterk de neiging om naar alleen een oplossing te zoeken en daarbij niet naar de bijkomende zaken zoals beleid of juridische aspecten mee te nemen. Daarnaast ook veel geleerd over het verkrijgen van inzicht in bepaalde zaken door te motiveren welke keuzes om welke reden zijn gemaakt.

Tijdens het afstudeeronderzoek heb ik zowel mijn kennis verbreed als meer inzicht in mezelf verkregen.

Bijlage 3 - Omschrijvingen applicaties die in aanmerking komen voor persoonsgebonden toegang

Clientele

Clientele is het call-registratie systeem van de Dienst ICT en Facilitair. Clientele is gebouwd rond een multi-tier architectuur. De client voor Clientele is een desktop applicatie. De clientele omgeving is ingericht in het afgeschermde BedrijfsProcessen netwerk (BP) en daarom alleen toegankelijk voor beheerde medewerkers-werkplekken. Niet alle medewerkers zijn geautoriseerd voor het gebruik van deze applicatie. Het kan wenselijk zijn om de applicatie ook via andere netwerken te ontsluiten, bijvoorbeeld Wifi. Clientele is geen webapplicatie en kan niet worden ontsloten door de reeds bij Avans actieve ontsluitingsmethodieken.

Osiris(11)

Osiris is het inschrijf- en studievolgsysteem van Avans Hogeschool. In dit systeem kan men zich inschrijven voor cursussen en toetsen en worden de behaalde resultaten verwerkt en opgeslagen. Osiris bevat tevens alle NAW-gegevens van de studenten en verzorgt de aanlevering van de collegegelden en financiële gegevens aan het financieel pakket van Avans, FMS. Osiris is gebouwd rond een multi-tier architectuur. Daarnaast is Osiris modulair opgebouwd. Elke module heeft zijn eigen groep gebruikers:

- Osiris Student voor de studenten; Studenten kunnen via Osiris student zichzelf inschrijven en hun studieloopbaan volgen.
- Osiris Begeleider voor de studieloopbaan adviseurs en de docenten.
- Osiris Manager is gekoppeld aan een Business Objects systeem van waaruit er verschillende rapportages worden aangeboden.
- Osiris Studievolg: Back Office omgeving gericht op het beheer van studieresultaten, cursussen en toetsen binnen Osiris, welke wordt uitgevoerd door de administratieve medewerkers op de academies en de centrale diensten.
- Osiris Inschrijving: Module die zorgt voor de koppeling met het inschrijfsysteem Studielink. De NAW gegevens van studenten die zich inschrijven via studielink, worden via deze koppeling naar Osiris overgedragen. Osiris is daarmee de bron voor alle studentengegevens. Vanuit deze module worden de gegevens van de studenten doorgezet naar de integration broker. De integration broker is de koppeling tussen de diverse systemen van Avans. De gegevens die van Osiris naar de integration broker worden verstuurd, worden bijvoorbeeld gebruikt om accounts aan te maken.

Zoals is te zien in bovenstaand overzicht, wordt Osiris door diverse gebruikersgroepen benaderd. Daarnaast is er ook nog een koppeling naar Corsa, waarop sterke authenticatie wordt toegepast. Het kan wenselijk zijn om de diverse componenten van Osiris via persoonsgebonden authenticatie/autorisatie te realiseren.

Corsa

Corsa is een document registratie systeem dat binnen Avans wordt gebruikt voor het verwerken van studenten dossiers, digitalisering van post- en archiefstukken en de registratie van factuurstromen. Corsa is opgebouwd rond een multi-tier architectuur. De gebruikers van Corsa behoren tot de gebruikersgroep medewerkers. De medewerkers kunnen gebruik maken van 3 typen clients:

- Corsa Webaccess: Webbased client omgeving voor Corsa
- MyCorsa: Een thin-client voor Corsa waar beperkte taken kunnen worden uitgevoerd.
- Corsa: Een fat-client, waarmee alle taken binnen Corsa kunnen worden uitgevoerd.

De servers zijn in het bedrijfsprocessen netwerk geplaatst. Door de gevoelige informatie in Corsa, wordt er gewerkt voor de Webaccess client met two-factor authenticatie, wat inhoud dat naast gebruikersnaam en wachtwoord er ook met een sms-token moet worden ingelogd. Dit wordt gerealiseerd door de Novell Access Manager omgeving. Binnen Corsa wordt er gewerkt met vertrouwelijkheidsgroepen, welke binnen Corsa bepalen wat er door de betreffende entiteit kan worden gezien. Het financieel management systeem (FMS) heeft een beveiligde koppeling met Corsa.

Untis

Untis is de software die wordt gebruikt voor het samenstellen van de lesroosters. Untis software bestaat uit een basisprogramma en diverse opties. De kern van het programma is een krachtige automaat, die een geoptimaliseerd lesrooster samenstelt. Untis is een backoffice programma, waar alleen medewerkers van het roosterbureau gebruik van maken. Untis is opgebouwd rond een multi-tier architectuur en bestaat uit een database, applicatieserver en client. Het kan wenselijk zijn om Untis via persoonsgebonden authenticatie/autorisatie te realiseren, zodat er ook bijvoorbeeld vanuit huis kan worden gewerkt.

Superoffice

Superoffice is een CRM pakket dat voor gebruikt gaat worden voor het beheren van gegevens van entiteiten waar Avans een band mee heeft en alle communicatie daar omheen. Superoffice is opgebouwd rond een multi-tier architectuur. Superoffice zal worden gebruikt door medewerkers van DMCS, medewerkers van alle academies en externen. Deze interne medewerkers maken gebruik van een client op hun werkstation. De authenticatie hiervan verloopt via Active Directory. Hierdoor is Single Sign-on mogelijk. De externen zijn beperkt tot het gebruik van de webclient en loggen in met een lokaal in Superoffice aangemaakt account. De autorisatie wordt per gebruiker(sgroep) geregeld binnen Superoffice.

PICA LBS4

LBS 4 is een bibliotheeksysteem dat er voor zorgt dat er boeken, scripties en andere werken van de mediatheek kunnen worden geregistreerd en uitgeleend. De serveromgeving van LBS4 draait bij het bedrijf OCLC in Leiden. Van de architectuur kan worden gesteld dat deze een client-server architectuur is. De serveromgeving die in Leiden functioneert, kan enkel worden benaderd door gebruikers die zich in een medewerkersnetwerk bevinden. Ook wordt de omgeving gebruikt door 'hardware' zoals uitleenautomaten. Het kan interessant zijn om de betreffende applicatie via persoonsgebonden toegang te ontsluiten, zodat de serveromgeving alleen kan worden benaderd door personen die daarvoor geautoriseerd zijn.