Secure Access en Secure Networking Solutions Overview

Eenvoud in ICT

Author(s) : Martijn Doedens

Version: 1.0

Date: Januari 2011

CONTENT

1. INTRODUCTIE

Bent u op zoek naar een onafhankelijk overzicht van de oplossingen voor Secure Access- en Secure Networking? Wilt u weten waarom Secure Access- en Secure Networking belangrijk is en wat de ontwikkelingen zijn? Dan moet u zeker deze whitepaper lezen!

In de huidige markt bestaat een toenemende vraag naar onbevooroordeelde informatie over oplossingen op het gebied van Secure Access en Secure Networking. Deze whitepaper is gericht op oplossingen waarvan wordt verwacht dat zij een belangrijke rol gaan spelen in de inzet van veilige toegang tot informatie systemen.

1.1 DOELSTELLINGEN

Het uiteindelijk doel van deze whitepaper is:

- Een overzicht te bieden van oplossingen op het gebied van Secure Access en Secure Networking.
- De verschillende vendors van en oplossingen voor Secure Access en Secure Networking benoemen.

1.1 DOELGROEP

Dit document is bedoeld voor IT-managers, architecten, analisten, systeembeheerders en IT-professionals in het algemeen die verantwoordelijk zijn voor en/of geïnteresseerd zijn in het ontwerpen, implementeren en onderhouden van infrastructuren voor Secure Access en Secure Networking.

1.2 CONTACTPERSOON

PQR B.V. Tel: +31 (0)30 6629729

www.PQR.com; info@pqr.nl

Wij streven ernaar juiste, duidelijke, volledige en bruikbare informatie te leveren. Wij stellen uw feedback op prijs. Mocht u op- of aanmerkingen, correcties, of suggesties hebben ter verbetering van dit document, dan horen wij graag van u! Stuur uw e-mailbericht naar Martijn Doedens (mdo@pqr.nl) of Ruben Spruijt (rsp@pqr.nl), onder vermelding van de productnaam en het versienummer, plus de titel van het document.

2. ABOUT

2.1 OVER PQR

PQR is dé specialist voor professionele ICT-infrastructuren met focus op Server & Storage, Virtualisatie en Applicatiebeschikbaarheid. PQR voorziet haar klanten van innovatieve ICT-oplossingen die ervoor zorgen dat applicatiebeschikbaarheid en beheerbaarheid optimaal zijn, zonder dat processen complexer worden. Eenvoud in ICT, dat is waar PQR voor staat.

PQR is Citrix Platinum Solution Advisor, HP GOLD Preferred Partner 2011, Microsoft Gold Partner Advanced Infrastructures & Security, NetApp Platinum Partner, RES Platinum Partner, VMware Premier Partner en Gold Authorized Consultant Partner, Cisco Premier Certified Partner, CommVault CASP Value Added Reseller, Dell Enterprise Architecture Certified Partner, HDS Platinum Partner, HP ProCurve Master Partner, Juniper J-Partner, Novell Platespin Platinum Partner, Veeam Gold ProPartner, Quest Software Platinum Partner en Wyse Premier Partner.

PQR beschikt over aantoonbare referenties en brede expertise op het vakgebied, getuige de vele hoogste partnerstatussen en certificeringen. Klanten van PQR zijn actief in alle sectoren van de samenleving en zijn te typeren als middelgrote tot grote organisaties waarbij de ICT-voorziening van essentieel belang is voor de bedrijfsvoering. Een significant deel van de omzet wordt gerealiseerd bij non-profit organisaties, de gezondheidszorg, educatie, lokale en rijksoverheid.

Als Trusted Advisor informeert PQR over nieuwe technologieën waarmee de klant nog eenvoudiger zijn ICT-omgeving draaiende kan houden, waarbij optimale performance belangrijk is en waarbij de gebruiker altijd en overal bij zijn informatie kan. Door middel van consolidatie en virtualisatie streeft PQR er naar het beheer zo eenvoudig mogelijk te laten zijn. Dit geldt niet alleen voor de systeembeheerder, maar komt ook ten goede aan perfomance en gebruikersgemak. Door het toepassen van bijvoorbeeld applicatie- en desktopvirtualisatie ondervindt de gebruiker het gemak en de snelheid waarmee hij toegang heeft tot de applicaties en de bijbehorende data die hij nodig heeft.

PQR creëert oplossingen die bijdragen tot verhoging van de productiviteit van de medewerkers van onze klanten. PQR biedt een ICT-omgeving die beheerbaar en overzichtelijk is en bovendien een aanzienlijke kostenverlaging met zich meebrengt, niet alleen in beheer, maar ook in energieverbruik. Daarnaast dragen deze oplossingen bij aan een aanmerkelijke reductie van CO2-uitstoot. Hiermee zorgt PQR voor een ICT-infrastructuur die stabiel, flexibel en toekomstvast is.

Ook met het ontwerpen en inrichten van storage-omgevingen heeft PQR ruime ervaring. Van oudsher zijn de grotere opslagomgevingen PQR's specialisme en dat zorgt ervoor dat wij efficiënt te werk gaan. De PQR-aanpak is bij alle trajecten helder. Gedurende het gehele traject, van ontwerp tot en met implementatie, neemt PQR de verantwoordelijkheid voor de tijdige oplevering van de deelprojecten en het eindresultaat, veelal tegen een van tevoren afgesproken prijs en bijbehorende garanties. Zo weet de klant altijd van tevoren waar zij aan toe is. Eenvoud in ICT noemt PQR dit. En dát is de PQR-aanpak die succes oplevert, al sinds de oprichting in 1990.

PQR is gevestigd in De Meern en telt ruim 100 medewerkers. In het boekjaar 2008/2009 is een omzet geboekt van € 84,6 miljoen en een nettowinst na belastingen van € 4,2 miljoen

2.2 SUGGESTIES EN VERBETERINGEN

Wij hebben bij het onderzoek en het beschrijven van de verschillende oplossingen onze uiterste best gedaan waarheidsgetrouw en zorgvuldig te zijn. Mocht u verbeteringen hebben dan stellen wij die zeer op prijs. Eeuwige dank zal u ten deel vallen ☺. Onze hartelijke dank voor uw bijdrage ter verbetering van deze whitepaper. Stuur uw e-mail naar mdo@pqr.nl of rsp@pqr.nl

3. INLEIDING

PQR solution schema's zijn ontwikkeld om ICT-infrastructuurconcepten en technische oplossingen op een overzichtelijke, logische en functionele manier te kunnen presenteren.

Het 'Application & Desktop Delivery' solutions overview (ADD) is door PQR ontwikkeld om in één oogopslag een compleet beeld te geven van de verschillende applicatie en desktop delivery oplossingen. Deze oplossingen zorgen ervoor dat gebruikers toegang krijgen tot applicaties, online, offline, onsite en offsite waarbij werkplek, locatie en netwerkonafhankelijkheid essentieel is.

Het 'Data & System Availability' solutions overview' (DSA) is door PQR ontwikkeld om in één oogopslag een compleet beeld te geven van alle componenten waaruit het datacenter is opgebouwd en van de relaties tussen deze componenten. Hoewel oplossingen voor opslag en virtualisatie in veel gevallen een doel op zich kunnen zijn, is het met betrekking tot beschikbaarheid geen eenvoudige taak om een oplossing voor de beschikbaarheid van datacenters te ontwerpen. Alle aspecten van een datacenter zijn op elkaar van invloed.

Het 'Secure Access en Secure Networking' solutions overview (SASN) is de essentiële schakel tussen de gebruikers- en zijn applicaties (ADD) en de informatie- en backendsystemen in het datacenter. Secure Access en Secure Networking is het cement en de wapening tussen ADD en DSA.

Het 'Secure Access en Secure Networking' solution schema, waarbij de focus ligt op het veilig en betrouwbaar verbinding maken met applicaties en resources, is vooral gericht op de onderste lagen van het OSI model. Het SASN solutions overview geeft grafisch de verschillende concepten en oplossingen weer. Daarnaast is het doel van dit document om de verschillende oplossingen, leverancier onafhankelijk en inhoudelijk te beschrijven zodat helder is wat SASN is, welke concepten er zijn en wat de functionaliteit en toepassing is.

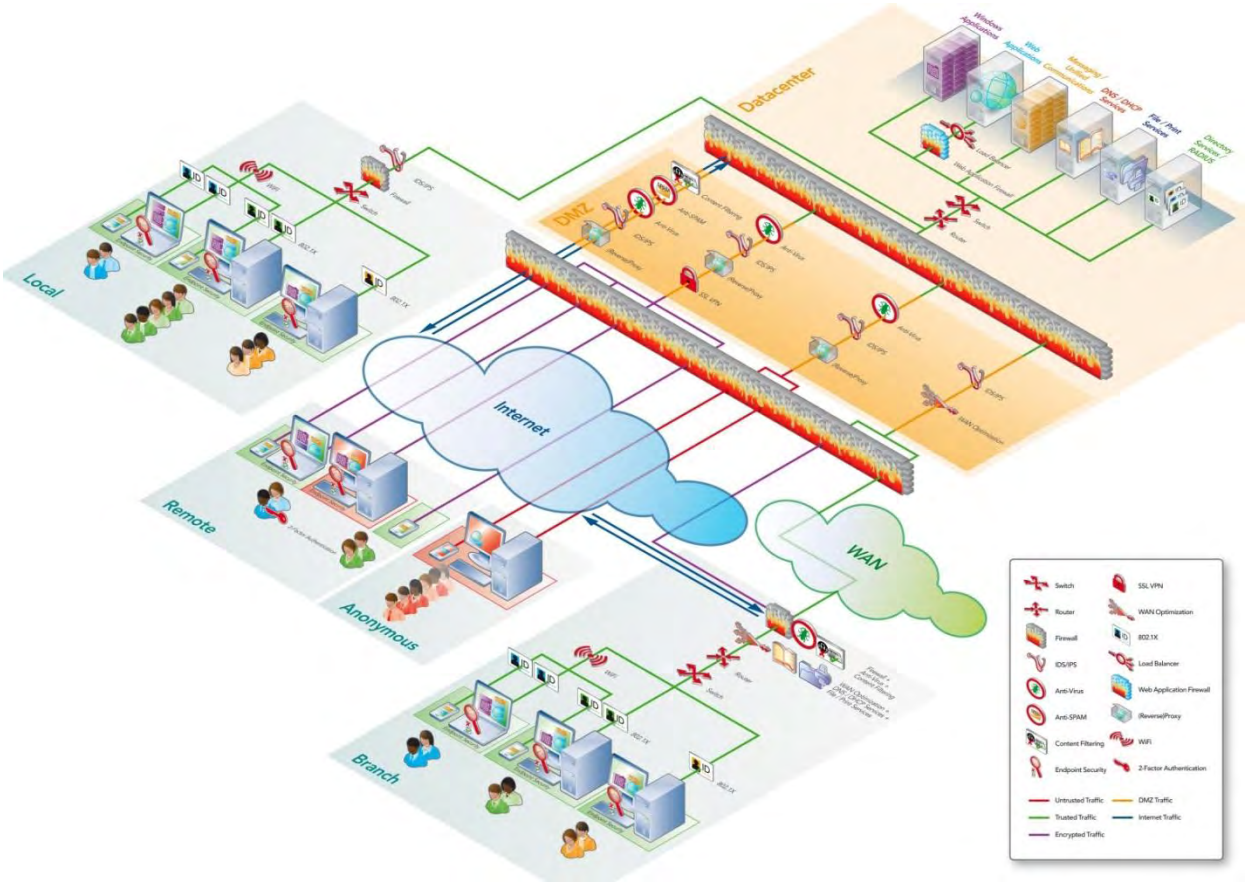
Doel van het schema en van de whitepaper is te informeren over de verschillende mogelijkheden en deze in een duidelijk schema weer te geven. Voor wie is het schema bedoeld: Mensen met basis netwerkkennis begrijpen het solution schema en kunnen door er gebruik van te maken meer inzicht krijgen in de functionaliteit en gerelateerde technieken. Een ervaren netwerkbeheerder of netwerkarchitect kan het schema gebruiken om collega's die op andere gebieden gespecialiseerd zijn duidelijk te maken wat Secure Access en Secure Networking (SASN) inhoudt.

4. SOLUTION SCHEMA

Het Secure Access en Secure Networking (SASN) schema is gebaseerd op de praktijkervaringen in ontwerp- en implementatietrajecten van verschillende, grote en middelgrote klanten. Alle functionaliteiten die mogelijk zijn om een bepaalde gebruiker op een bepaalde locatie met een bepaald apparaat veilige toegang te geven tot de applicatie of resource zijn in dit schema weergegeven. Het schema geeft een beeld van de functionele mogelijkheden, welke oplossing het beste is en welke leverancier hierbij past. Hoe het technisch infrastructuur ontwerp eruit ziet valt buiten de scope van het schema en de whitepaper.

Het schema is opgebouwd uit verschillende 'vlakken', namelijk:

- het datacenter met alle resources waar de gebruiker bij moet kunnen,
- de locatie welke beschikt over een LAN-verbinding met het datacenter,
- een locatie waarbij de gebruikers gebruik maken van een eigen of niet beheerde internetverbinding en
- een locatie waarbij de gebruiker door middel van een eigen WAN-verbinding of via een Virtual Private Network (VPN) via het internet verbinding maakt met het datacenter.



5. GEBRUIKERS, APPLICATIES EN WERKPLEKKEN

Zoals aangegeven bestaat het schema uit een aantal vlakken die gevuld zijn met functionaliteiten. Naast de functionele symbolen zijn er ook symbolen gemaakt voor andere onderdelen in het schema zoals de gebruikers en de werkplekken. In dit hoofdstuk worden de verschillende gebruikers, applicaties en werkplekken beschreven.

5.1 GEBRUIKERS

Gebruikers zijn uniek, maar als we naar de verschillende rollen en werkzaamheden kijken is het mogelijk ze in groepen te verdelen. Een gebruiker heeft bijvoorbeeld een bepaald type werkplek, heeft toegang tot bepaalde applicaties en kan gebruik maken van bepaalde resources.

Naast de typen gebruikers verschilt ook het aantal gebruikers dat aanwezig is op een vestiging. In het schema zijn de verschillende typen gebruikers in kleuren opgedeeld: blauw, groen, oranje en rood. Iedere kleur correspondeert met een rol. We onderscheiden de volgende rollen:

KNOWLEDGE WORKER

Een Knowledge Worker is een medewerker die werkt aan ontwikkelingen of die intensief gebruik maakt van kennis die is vastgelegd in informatiesystemen. Een Knowledge Worker stelt hoge eisen aan zijn ICT-werkplek, omdat hij bijvoorbeeld grafische applicaties (bijv. AutoCAD) gebruikt, zelf software moet kunnen installeren voor ontwikkeling, etc. De Knowledge Worker werkt met ideeën en is verantwoordelijk voor teams. Voorbeeld van deze gebruiker is een consultant of een team manager.

STRUCTURED TASK WORKER

Een Structured Task Worker is een medewerker die, in tegenstelling tot de Knowledge Worker, alleen werkt met informatie en data en niet met ideeën. De gebruiker moet snel over informatie kunnen beschikken. Voorbeeld van deze gebruiker is een boekhouder of controller.

DATA ENTRY WORKER

De Data Entry Worker is een medewerker die ICT-middelen gebruikt om de werkproductiviteit te verhogen. De Data Entry Worker gebruikt data en moet hier voornamelijk makkelijk bij kunnen via gestructureerde processen. Voorbeelden van dit type gebruiker is receptie of een secretaresse.

5.1.1 Blauw

De 'blauwe gebruiker' in het solution schema is een Knowledge Worker. Deze gebruiker kan op elke mogelijke locatie werken en maakt gebruik van de beheerde laptop en beheerde smartphone maar ook, als de gebruiker bijvoorbeeld thuis werkt, van een eigen computer die de gebruiker zelf beheert.

De verschillende applicaties zijn zichtbaar op de werkplek van de gebruiker, aangeduid met de verschillende blokken op het scherm van het apparaat. Bijv. de paarse Windows applicaties en de blauwe web-based applicaties. Afhankelijk van de context: de locatie, type verbinding, soort authenticatie en type werkplek, wordt bepaald welke applicatie beschikbaar is. We noemen dit een Access Scenario.

5.1.2 Groen

De 'groene gebruiker' is een Structured Task Worker en werkt met een beheerde desktop computer en een beheerde smartphone. De smartphone wordt alleen gebruik

om mail te ontvangen en om gebruik te maken van Unified Communications functionaliteiten. De vaste werkplek is aanwezig op het verbindingsprofiel Local (met een LAN-verbinding), Branch (met een WAN-verbinding) en via het internet (alleen met de beheerde smartphone).

De groene gebruiker heeft minder applicaties beschikbaar (een Knowledge Worker maakt bijvoorbeeld gebruik van AutoCAD terwijl Structured Task Worker dit niet nodig heeft). Van het type gebruiker Structured Task Worker zijn over het algemeen meer op een locatie aanwezig dan van het type Knowledge Worker (blauw).

5.1.3 Oranje

De Data Eentry Worker beschikt alleen over een beheerde desktop werkplek en is te vinden in het Local en het Branch type verbinding. Deze gebruiker werkt niet thuis en heeft slechts een beperkt aantal applicaties nodig om te werken. Deze medewerker wordt als 'oranje gebruiker' in het schema weergegeven.

5.1.4 Rood

De 'rode gebruiker' is een anonieme gebruiker en benut de open verbinding, het internet. Deze gebruiker is niet aanwezig in een directory service en heeft een onbeheerde smartphone en zit op een onbeheerde werkplek (dit kan ook zowel een desktop als een laptop zijn). De Rich Internet Applicaties (bijvoorbeeld een iPhone applicatie) en web based applicaties, zoals een webshop of een track&tracé-applicatie, worden op de onbeheerde devices beschikbaar gesteld.

5.2 APPLICATIES

De verschillende typen gebruikers maken gebruik van allerhande applicaties en resources. Deze zijn ook met kleuren te onderscheiden en komen overeen met de kleur van de applicatie of resource zoals deze in het datacenter van het solution schema staat.

5.2.1 Paars

Paarse blokken op de schermen van de verschillende apparaten geven Windows applicaties weer die in het datacenter gehost worden. Donkerpaars wijst op een offline Windows applicatie.

5.2.2 Blauw

Blauwe blokken op de schermen van de verschillende apparaten staan voor web-architected applicaties die in het datacenter gehost worden.

5.2.3 Oranje

Oranje blokken op de schermen van de verschillende apparaten zijn Messaging/Unified Communications applicaties die in het datacenter gehost wordt.

Overige applicaties en resources (zoals deze in het datacenter beschikbaar zijn) hebben geen relatie tot de gebruiker en de werkplek, maar hebben wel een relatie tot een functionaliteit zoals deze geboden wordt in het schema.

5.3 WERKPLEKKEN

Waar in het vorige hoofdstuk beschreven wordt welke gebruikers in het schema weergegeven zijn en de rollen die deze gebruikers hebben, beschrijft dit hoofdstuk met welke apparaten deze gebruikers werken. Er wordt onderscheid gemaakt tussen beheerde en niet-beheerde apparaten (trusted en untrusted devices) door middel van de kleur op de achtergrond van het scherm van het apparaat: groen is trusted en rood is untrusted. Afhankelijk van het apparaat (beheerd of niet-beheerd) is de applicatie of resource beschikbaar.

5.3.1 Smartphone

De smartphone of tablet PC maakt gebruik van een WiFi of andere soort verbinding, zoals 3G of 4G, om toegang te krijgen tot de applicatie of resource waar de gebruiker met dit apparaat recht op heeft. In het solution schema staan alleen Messaging/Unified Communications en Rich Internet Applications. Daarnaast is het ook mogelijk om met technieken als de Citrix Receiver of VMware View Client op de iPad of Android tablet applicaties beschikbaar te stellen, echter zijn deze in het schema niet functioneel weergegeven. Naast de messaging functionaliteit (oranje blok in het scherm) is er ook een web applicatie beschikbaar (blauw blok).

De untrusted smartphone maakt gebruik van dezelfde mogelijkheden echter zijn deze in het schema beperkt tot een webapplicatie. De untrusted smartphone is te herkennen aan de rode achtergrond.

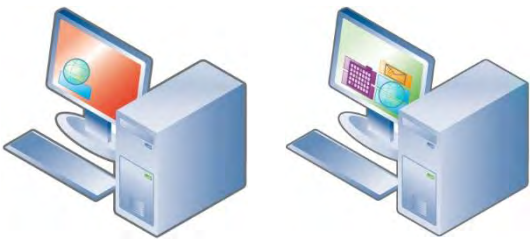
5.3.2 Laptop

De laptop wordt gebruikt door de blauwe gebruiker om altijd en overal een trusted apparaat te hebben en te kunnen beschikken over de applicaties en resources die de Knowledge Worker nodig heeft. Ook hier zijn de applicaties en resources als blokken in het scherm weergegeven. Op de laptop van de Knowledge Worker die een remote verbinding maakt met het datacenter is te zien dat hij een windows applicatie offline aangeboden krijgt (donkerpaarse applicatie).

5.3.3 Desktop

De desktop wordt als trusted apparaat gebruikt door de groene en oranje gebruiker. De desktop blijft op zijn plek staan op de locatie waar de gebruiker werkt; dit kan een local of branch netwerk zijn.

De untrusted desktop wordt door de rode (anonieme gebruiker) en door de Knowledge Worker gebruikt om een webapplicatie te benaderen die in het datacenter gehost wordt.



6. VERBINDINGEN EN VERKEER

Binnen het solution schema worden scenario's door middel van lijnen en wolken weergegeven. In dit hoofdstuk worden deze symbolen nader toegelicht om de gedachtegang hierachter te verduidelijken. De locaties en functionaliteiten worden in hoofdstuk vijf en zes toegelicht.

6.1 INTERNET

Het internet wordt gebruikt om gebruikers vanaf de remote locatie (gebruikers die thuis werken), de anonymous gebruikers en, indien gebruik gemaakt wordt van de site-to-site VPN connectie, gebruikers op de branch locatie, toegang te geven tot het datacenter. Het internet is een volledig untrusted verbinding en verbindingen met het datacenter via het internet dienen derhalve goed beveiligd te zijn.

6.2 WAN

De WAN connectie wordt gebruikt om gebruikers op de branch locatie toegang te geven tot het datacenter. WAN-connecties kunnen zowel als trusted als untrusted gezien worden, trusted omdat het een eigen verbinding is die gehuurd wordt van een WAN service provider maar ook untrusted omdat niet duidelijk is wat er precies met het verkeer gebeurd. In het solution schema zijn firewalls geplaatst aan beide zijden.

6.3 DATASTROMEN

Binnen het solution schema zijn veel verschillende communicatielijnen aanwezig. Deze lijnen geven geen connecties of verbindingen weer, maar datastromen waarvoor bepaalde functionaliteit aanwezig is. Functionaliteiten hoeven niet in-line, dat wil zeggen in het pad van het verkeer, geplaatst te zijn maar moeten wel iets met de datastroom doen.

6.3.1 Groen

De groene lijn geeft betrouwbaar, unencrypted verkeer weer.

6.3.2 Paars

De paarse lijn geeft betrouwbaar, door middel van een (IPSEC of SSL) VPN encrypted verkeer weer.

6.3.3 Rood

De rode lijn geeft onbetrouwbaar verkeer weer, zowel encrypted als unencrypted.

6.3.4 Blauw

Normaal internet verkeer (web browsing, mail) wordt weergegeven door blauwe lijnen met pijlen aan de uiteinden.

6.3.5 Oranje

Al het verkeer binnen de DMZ wordt met oranje lijnen weergegeven.

7. LOCATIES

De verschillende gebruikers en apparaten bevinden zich op allerlei locaties. Deze locaties worden gekarakteriseerd door zowel het type en de snelheid van de verbinding met het datacenter als door het aantal medewerkers. In het solution schema worden de gebruikers en apparaten verdeeld over een 'local' blok, een 'remote' blok, een 'anonymous' locatie en een 'branch' blok. Binnen deze blokken zijn de verschillende functionaliteiten beschreven die nodig zijn om het betreffende type gebruiker met het betreffende apparaat op een veilige en goede manier toegang te geven tot de applicaties en resources in het datacenter.

In onderstaande paragrafen wordt per locatie beschreven welke functionaliteiten daar aanwezig zijn en waarom bepaalde functionaliteiten daar niet aanwezig zijn. De functionaliteiten worden in hoofdstuk 8 nader toegelicht.

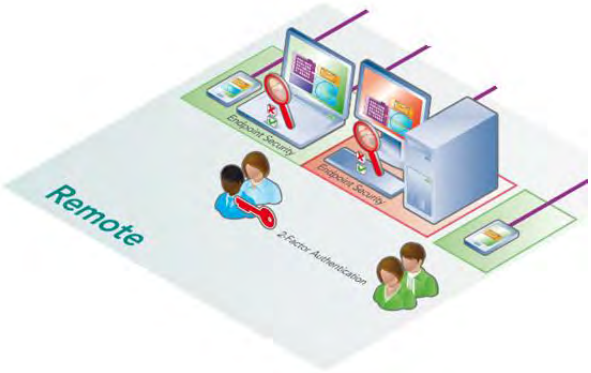
7.1 LOCAL

In het 'local' locatie vlak wordt uitgegaan van een LAN-verbinding. Bandbreedte is voldoende aanwezig aangezien de gebruiker op dezelfde locatie als het datacenter werkt. Als de gebruiker op dezelfde locatie werkt als waar het datacenter gehost wordt is dit meestal de grootste locatie. Hier zijn dus ook de meeste medewerkers aanwezig. Aangezien alle mensen die vanuit het local locatie vlak bekend zijn, zijn de anonieme gebruikers (rood) hier niet weergegeven.

Gebruikers met laptops en smartphones hebben een WiFi-verbinding nodig; gebruikers met een desktop een vaste verbinding met de switch. Op alle laptops en desktops is end-point security functionaliteit toegepast. Deze functionaliteit wordt technisch als Network Access Control (NAC) of Network Access Protection (NAP) aangeduid. Naast end-point security wordt door middel van 802.1x authenticatie bepaald of de gebruiker met zijn of haar credentials verbinding mag maken met het netwerk (zowel wireless als wired). Een firewall en een IDP/IDS functionaliteit is geplaatst tussen het gebruikers netwerk en het datacenter netwerk om het security risico verder te verkleinen.

7.2 REMOTE

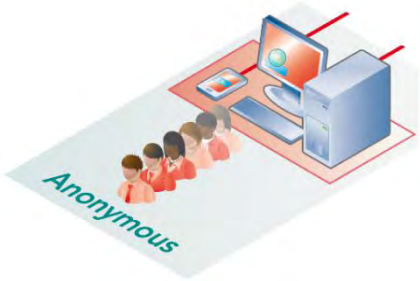
Medewerkers die remote bezig zijn, moeten gezien worden op alle locaties behalve local of branch. Zij maken gebruik van een internetvverbinding via een niet beheerde netwerk infrastructuur. De enige invloed die uitgeoefend kan worden op zo'n gebruiker is de end-point security op het apparaat.



Alleen de blauwe (Knowledge Worker) en groene (Structured Task Worker) gebruikers hebben de mogelijkheid om vanuit het remote locatie vlak verbinding te maken met het datacenter, waarbij de groene gebruiker alleen de messaging/unified communications functionaliteit op de smartphone benut. De blauwe gebruiker maakt gebruik van token authenticatie om een extra authenticatie factor toe te voegen. De gebruiker heeft in dit locatie vlak de smartphone en laptop welke trusted zijn (met de daarbij horende applicaties) en een untrusted desktop computer. Te zien is dat als de blauwe gebruiker meer applicaties beschikbaar heeft met een trusted laptop, dan wanneer hij gebruik maakt van een untrusted desktop.

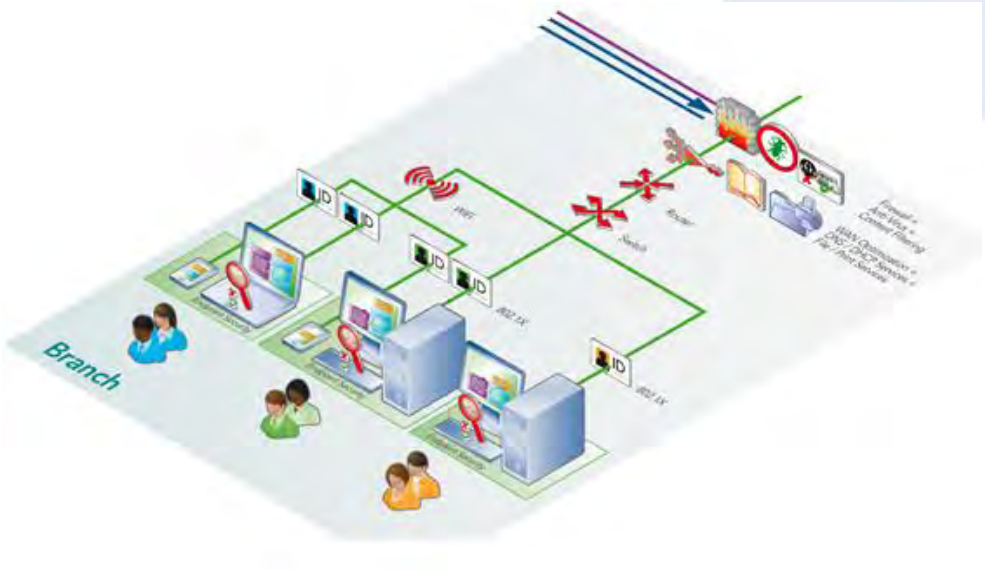
7.3 ANONYMOUS

De rode gebruikers zijn 'anonymous' en daarom niet in een aantal uit te drukken, de gebruiker maakt alleen gebruik van een web applicatie (bijv. track&trace, webshop) welke in het datacenter gehost wordt.



7.4 BRANCH

Karakteristiek voor het branch locatie vlak is de verbinding. Aangezien de branch locatie gebruik maakt van een Wide Area Network (WAN) verbinding en/of gebruik maakt van een site-to-site VPN via het internet is bandbreedte en functionaliteit van deze verbinding beperkt. Het is bijvoorbeeld bij bepaalde vormen van WAN verbindingen niet mogelijk een ethernetverbinding op OSI-laag twee te maken met het datacenter. In het SASN solution schema is uitgegaan van een gerouteerde verbinding, aangezien deze het meest voorkomt. Zowel de WAN-verbinding als de site-to-site VPN-verbinding is opgenomen aangezien deze vaak naast elkaar toegepast worden voor redundantie.



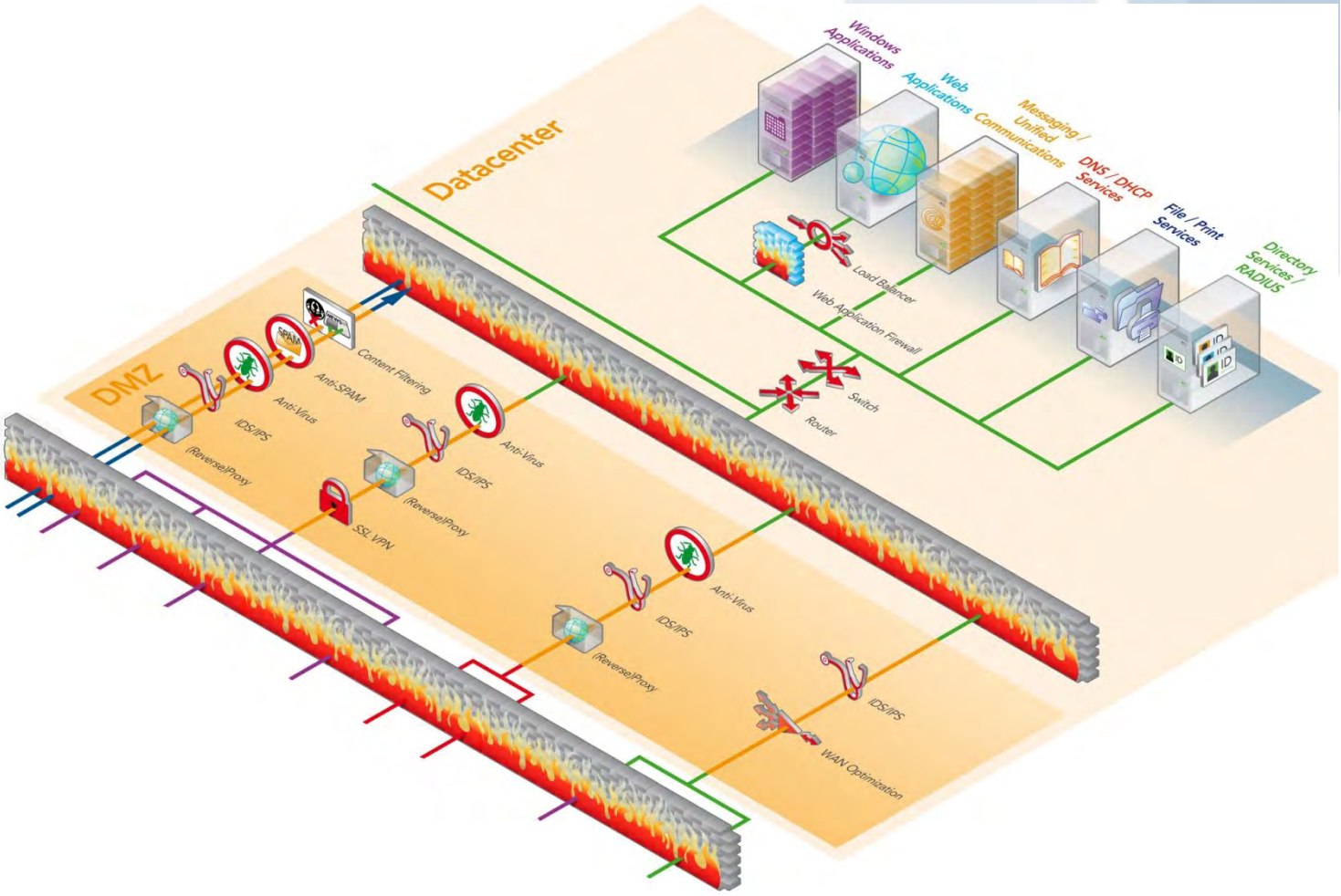
Op het branch locatie vlak zijn minder mensen aanwezig dan op het local locatie vlak omdat een branch locatie een nevenvestiging is terwijl een locatie op het local locatie vlak op dezelfde locatie als het datacenter de hoofdvestiging is. In het geval van een extern datacenter (hosted omgeving of private cloud) kan elke locatie waar mensen werken gezien worden als branch locatie. Aangezien applicaties of resources afhankelijk kunnen zijn van beschikbare bandbreedte kan een groene gebruiker op het branch locatie vlak minder applicaties of resources benaderen dan wanneer de groene gebruiker op een local locatie vlak zit. Naast de end-point security, 802.1x, WiFi en Switch functionaliteit wordt op het branch locatie vlak gebruik gemaakt van een router aangezien de verbinding met het datacenter zoals eerder aangegeven een verbinding op laag drie (waar routering plaatsvind) is.

Om de gebruiker op de branch locatie een goede werkomgeving te bieden worden de door het type verbinding beperkende factoren (met name lagere bandbreedte en hogere latency) door middel van een WAN-optimization-oplossing opgelost. Tevens kunnen in deze functionaliteit andere functionaliteiten ondergebracht worden die voordelen bieden om op de locatie zelf uit te voeren zoals DNS/DHCP services en File/Print services.

De branch locatie maakt gebruik van een eigen internetconnectie die naast voor de site-to-site VPN verbinding ook gebruikt wordt voor internetverkeer. Dit om de WAN of site-to-site VPN-verbinding niet onnodig te belasten. Hiervoor is een Unified Threat Management (UTM) firewall symbool aanwezig om de gebruiker op de branch locatie op een veilige manier gebruik te laten maken van het internet. Unified Threat Management (UTM) houdt in dat meerdere functionaliteiten in de firewall samengebracht zijn om dit te bewerkstelligen, in dit geval is dit Anti-Virus en Content Filtering.

7.5 DATACENTER

In het datacenter zijn alle resources en applicaties aanwezig die door de gebruikers op verschillende locaties gebruikt worden. De verschillende resources en applicaties zijn met kleuren te onderscheiden, die overeenkomen met de kleuren op de schermen van de apparaten van de verschillende gebruikers.

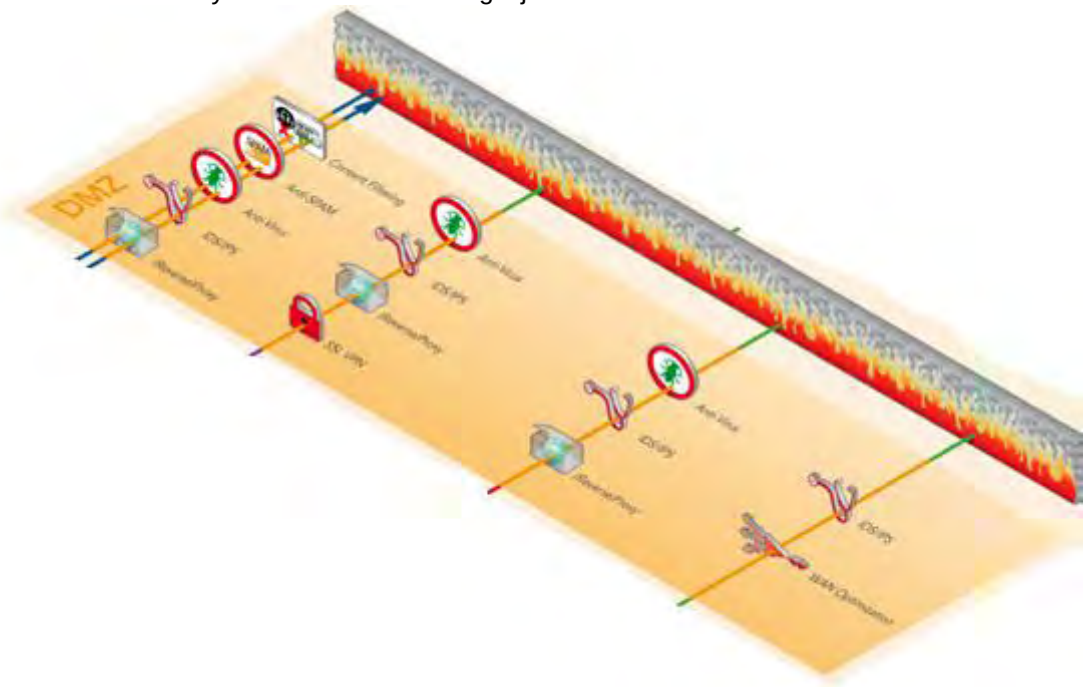


Functionaliteiten in het datacenter zijn een load balancer welke hier voor de web application server geplaatst is. Web-architected applications zijn bij uitstek geschikt om door middel van een load balancer hoog beschikbaar en schaalbaar te maken. Een web application firewall beveiligt deze web applications door te controleren op applicatie niveau (http) wat de gebruiker precies met de web applicatie doet.

De functionaliteiten load balancer en web application firewall kunnen in één apparaat gecombineerd worden, echter zijn ze in het solution schema als verschillende functionaliteiten getekend. Switching functionaliteit is uiteraard aanwezig alsook router functionaliteit. De verkeersstroom van de locatie local komt rechtstreeks binnen in het datacenter, zonder gebruik te maken van een DMZ. Dit omdat binnen 'local' reeds een firewall en IDS/IPS functionaliteit aanwezig is.

7.6 DMZ

Een firewall schermt de datacenter resources en applicaties af van de DMZ waarin een aantal security functionaliteiten geplaatst zijn. De DMZ is op zijn beurt weer door middel van een firewall afgeschermd van het internet en van de WAN-connectie om ook hier te controleren welk verkeer wel en welk verkeer niet is toegestaan. De verschillende datastromen vanaf het internet en vanaf de WAN-connectie komen binnen uit de buitenste firewall waarna een aantal security functionaliteiten gebruikt worden om de omgeving te beveiligen. Tevens is de internetconnectie voor bijvoorbeeld uitgaande en inkomende mail hier als datastroom aanwezig omdat ook hier security functionaliteiten nodig zijn.



Vanuit de branch locatie, waar WAN-optimalisatie plaatsvindt, is ook binnen de DMZ in de datastroom een WAN optimization functionaliteit geplaatst. Tevens is hier, net als bij de local locatie, een IDS/IPS functionaliteit geplaatst. Aangezien het verkeer in deze stroom betrouwbaar is (het komt vanaf een trusted locatie met alleen maar trusted apparaten waar ook nog op de locatie zelf een aantal security functionaliteiten aanwezig zijn), zijn hier geen verdere functionaliteiten geplaatst.

Op de datastroom van anonymous gebruikers die alleen gebruik maken van een web applicatie is reverse proxy functionaliteit geplaatst zodat mogelijke encryptie (door middel van SSL) getermineerd kan worden (SSL offloading). Het verkeer ná de reverse proxy is te analyseren door de IDS/IPS functionaliteit die na de reverse proxy geplaatst is en is te scannen door de Anti-Virus gateway.

Bekende gebruikers die vanaf de remote locatie gebruik willen maken van de resources en applicaties in het datacenter maken een verbinding met de SSL VPN functionaliteit zodat verkeer encrypted is. Na de SSL VPN functionaliteit is reverse proxy functionaliteit geplaatst om gegevens te cachen en indien nodig SSL offloading te doen. Al het verkeer wordt door een IDS/IPS controleerd en door een Anti-Virus gateway gescand.

Op het reguliere internet verkeer worden de meeste security functionaliteiten toegepast. De proxy (hier als forwarding proxy), IDS/IPS functionaliteit, Anti-Virus, Anti-SPAM en Content filtering. Er kan gekozen worden bepaalde functionaliteiten in een bepaalde richting wel of niet te gebruiken (bijvoorbeeld inkomend verkeer alles controleren maar uitgaand verkeer niet).

8. FUNCTIONALITEITEN

In dit hoofdstuk worden alle functionele symbolen uitgelegd en wordt er een koppeling gelegd met technische invulling van de verschillende functionalieiten.

8.1 SWITCH

Het switch symbool wordt in alle trusted locaties gebruikt in het schema om een verbinding te maken met het apparaat of verbinding te maken met de WiFi-functionaliteit. De switch functionaliteit in het schema wordt in alle scenario's toegepast.

De switch functionaliteit vindt plaats op laag twee van het OSI-model. Ethernet frames worden naar de juiste bestemming gestuurd op basis van het MAC-adres dat in een tabel van de switch staat (MAC-tabel). De switch ziet welk systeem, dus welk MAC-adres, achter een bepaalde poort aanwezig is en beperkt zo het zogenaamde collissiondomein. Frames komen alleen aan bij het systeem waar de frames voor bedoeld zijn en niet, zoals bij een hub, bij alle systemen binnen het collissiondomein.

Binnen de switch functionaliteit zijn tal van technieken geïntroduceerd ten behoeve van snelheid, schaalbaarheid en redundantie. Belangrijkste voorbeeld hiervan is Spanning-Tree. Het Spanning-Tree protocol zorgt ervoor dat redundante verbindingen gelegd kunnen worden zonder dat een broadcast storm ontstaat doordat er een loop in het netwerk ontstaat. Hiervoor worden verbindingen dicht gezet (blocking) en op het moment dat een redundant pad nodig is wordt de verbinding open gezet (forwarding). Dit gebeurt op basis van een hiërarchie met een root switch en een backup root switch. Binnen spanning-tree zijn verschillende versies actief die het mogelijk maken verbindingen te load balancen per VLAN. Bijvoorbeeld, poort 24 is forwarding voor VLAN 1 en blocking voor VLAN 2 en poort 23 (de redundante verbinding) is blocking voor VLAN 1 en forwarding voor VLAN 2.

Om alle poorten in forwarding mode te zetten is het nodig om logisch gezien geen loops in het netwerk te krijgen. Oplossing hiervoor is van verschillende fysieke switches één logische switch te maken die binnen de logische switch redundant is opgebouwd.

Proprieteray technieken om van verschillende fysieke switches één logische switch te maken zijn Stackwise en Virtual Switch System (VSS) van Cisco, Intelligent Resilient Framework (IRF) van HP Networking, Virtual Chassis van Juniper Networks en knowledge worker van Brocade (voorheen Foundry). Bekende fabrikanten van switching functionaliteit zijn Cisco, HP Networking, Juniper Networks en Brocade.

8.2 ROUTER

Verkeer wordt op laag drie van het OSI-model gerouteerd. Waarbij een switch gebruikt maakt van MAC–adressen, gebruikt een router IP-adressering. Op basis van het IP-adres wordt een packet naar de juiste bestemming gestuurd. Dit kan een systeem zijn binnen het subnet van een poort van de router (dan gaat het packet rechtstreeks naar zijn bestemming) of een systeem dat achter een volgende router te vinden is (dan wordt het packet naar de volgende router gestuurd die dan weer een beslissing neemt waar het packet heen moet. De router gebruikt hiervoor een routering en forwarding tabel. In deze tabel zijn alle verbonden IP-subnetten weergegeven en kunnen routes naar andere IP-subnetten geplaatst worden welke achter een andere router te vinden zijn. De beslissing wordt genomen op basis van best match: een route die het meest specifiek in de tabel staat voor een bepaald packet wordt gebruikt. Bekend voorbeeld hiervan is de default route met subnet adres 0.0.0.0 en als subnet masker 0.0.0.0 naar een volgende router. Al het verkeer dat niet gespecificeerd staat in de routing table wordt naar de volgende router gestuurd. Vaak is dit de internet router. Routing tables kunnen statisch gevuld worden maar ook dynamisch door gebruik te maken van een routing protocol. Voorbeelden hiervan zijn het Border Gateway Protocol (BGP), Open Shortest Path First

(OSPF) en het Cisco proprietary Enhanced Interior Gateway Protocol (EIGRP). BGP wordt over het algemeen niet binnen lokale netwerken gebruikt maar binnen het internet en WAN-oplossingen. Bekende fabrikanten van routers zijn bijvoorbeeld Cisco en Juniper Networks.

8.3 FIREWALL

Waar switching en routing functionaliteit gebaseerd is op het doorsturen van informatie (bij een switch ethernet frames, bij een router IP packets), is een firewall bedoeld om verkeer te blokkeren mits het wordt toegestaan. Firewalls nemen een dergelijke beslissing op basis van een aantal gegevens. In het geval van een traditionele firewall gebeurt dit op laag vier van het OSI-model. Op basis van bron IP-adres, bestemming IP-adres, TCP en UDP poort nummer wordt bepaald of het verkeer toegestaan is (permit) of niet (deny). In de nieuwe generatie firewalls (next-gen firewalls) wordt hier de gebruiker en de applicatie aan toegevoegd. Bijvoorbeeld wordt MSN messenger toegestaan maar file transfer via het MSN Messenger protocol geblokkeerd. Bekende fabrikanten van firewall functionaliteit zijn onder andere Juniper Networks, Watchguard, Microsoft ForeFront Threat Management Gateway (TMG) en Fortinet. Palo Alto is een nieuwe firewall fabrikant volledig gericht op de 'next-gen' firewalls waar de andere firewall fabrikanten de 'next-gen' functionaliteit aan de traditionele firewall toegevoegd hebben.

8.4 IDS/IPS

IDS/IPS functionaliteit is enigszins vergelijkbaar met de next-gen firewall functionaliteit. Op applicatieniveau wordt gekeken naar het verkeer, bekende aanvallen worden herkend en verkeer kan worden geblokkeerd. Een database met signatures is aanwezig en verkeer wordt vergeleken met deze signatures. Verschil tussen Intrusion Detection Systems (IDS) en Intrusion Prevention System (IPS) is dat de IDS alleen aanvallen herkend en de IPS de aanvallen ook tegenhoudt. Bekende fabrikanten van IDS/IPS functionaliteit zijn Cisco (IDS), Juniper Networks (IDP) en HP Networking (Tipping Point).

8.5 ANTI-VIRUS

Binnen alle ICT-infrastructuren wordt wel Anti-Virus software gebruikt. Er zijn uitzonderingen (zoals Terminal Servers, VDI-omgevingen) maar dan wordt hier expliciet voor gekozen. Anti-Virus functionaliteit in het SASN solution schema is niet de Anti-Virus software op de werkplek maar de gateway functionaliteit. Onder andere verkeer van en naar het internet wordt gecontroleerd op virussen. Dit kunnen bijvoorbeeld downloads zijn maar ook attachments in e-mailverkeer. Vaak wordt anti-virus functionaliteit op het gebied van mail geïntegreerd met anti-SPAM functionaliteit. Bekende fabrikanten van anti-virus software- en hardwarefunctionaliteit zijn McAfee, Microsoft en Trend Micro. Deze producten worden geïntegreerd in de totaaloplossing (mits deze aanwezig is). Barracuda en PineApp hebben anti-virus producten specifiek voor mailverkeer. Bluecoat is een fabrikant met een product specifiek voor webverkeer. Dit werkt samen met de proxy-oplossing.

8.6 ANTI-SPAM

Van de e-mail die naar een organisatie verzonden wordt is het overgrote deel SPAM, vaak met virussen of trojan software. Anti-SPAM functionaliteit is dus een vereiste voor SASN. Anti-SPAM functionaliteit maakt gebruik van blacklists, analyse van berichten en meer technieken. De functionaliteit kan in de mailapplicatie zelf (Microsoft Exchange) geïntegreerd zijn, maar ook als externe gateway. Bekende fabrikanten van Anti-SPAM functionaliteit zijn Barracuda, PineApp en Microsoft met ForeFront threat management gateway (TMG) functionaliteit.

8.7 CONTENT FILTERING

Gebruikers maken veel gebruik van internet, echter niet altijd om zakelijke redenen. Content filtering functionaliteit kan gebruikt worden om gebruik van internet te beperken door toegang in te delen in categorieën. Ook kan hier een tijdvariabele aan gekoppeld worden (bijvoorbeeld een gebruiker mag van 9:00 uur tot 18:00 uur geen gebruik maken van www.facebook.com).

Een bekende fabrikant van content filtering functionaliteit is Websense. Bluecoat heeft een content filtering functionaliteit als toevoeging op de proxy-oplossing.

8.8 ENDPOINT SECURITY

Controle over het apparaat dat gebruikt wordt om toegang te krijgen tot resources en applicaties is een belangrijk onderdeel van SASN. Als pure thin clients gebruikt worden is dit een risico minder, er kan immers minder op geïnstalleerd worden. Voor laptops en andere apparaten heeft de gebruiker meer mogelijkheden waardoor een dergelijk apparaat meer risico zal lopen. Door endpoint security te gebruiken kan gecontroleerd worden of een apparaat aan de security eisen voldoet die door de organisatie gesteld zijn. Dit geldt voor wired en wireless gebruikers door Network Access Control of Network Access Protection (NAC/NAP) te gebruiken, maar ook voor remote gebruikers doordat de SSL VPN endpoint security ondersteunt. Op deze manier kan bijvoorbeeld gecontroleerd worden of op het apparaat waarmee verbinding gemaakt wordt anti-virus software geïnstalleerd is en of het patch niveau van Windows op het juiste niveau is. Bekende fabrikanten van NAC-functionaliteit zijn bijvoorbeeld Cisco, HP Networking, Juniper Networks en Quarantainenet. Microsoft heeft NAC functionaliteit in het portfolio die Network Access Protection (NAP genoemd wordt.

8.9 SSL VPN

Om via een onbeheerde en onveilige verbinding zoals het internet connectie te maken met het datacenter is een encrypted sessie nodig. Door een Virtual Private Network (VPN) te gebruiken wordt dit gerealiseerd. Er wordt een encrypted authenticatie gedaan waarna al het verkeer van de client naar het datacenter encrypted is. Voorheen werd een client gebruikt welke een VPN-verbinding maakt met de firewall (IPSEC VPN). Hiermee wordt een netwerkverbinding gemaakt op laag drie waarna de firewall zo nodig verkeer kan toestaan of weigeren. Bij een SSL VPN wordt de authenticatie en het verkeer versleuteld door middel van een SSL certificaat dat op een appliance staat (of op een gecombineerd apparaat zoals een firewall). Aan de gebruiker wordt een portal gepresenteerd met daarop de applicaties en resources welke voor de gebruiker relevant zijn. Er kan hier op basis van gebruiker bepaald worden waar de gebruiker bij kan komen. Indien nodig kan ook met een SSL VPN oplossing een netwerkverbinding opgezet worden. Bekende fabrikanten van SSL VPN functionaliteit zijn onder andere Juniper (SA), Citrix (Access Gateway), F5 (Firepass), Cisco (ASA) en Microsoft (UAG).

8.10 WAN OPTIMIZATION

Gebruikers op de branch locatie maken gebruik van een over het algemeen tragere verbinding dan de LAN-verbinding. Dit kan een WAN-verbinding zijn of een site-to-site VPN (of beiden). WAN optimzation oplossingen kunnen de gebruikerservaring op een dergelijke locatie verbeteren door een aantal technieken toe te passen. Hiervoor dient een WAN optimization oplossing aan beide kanten van het verkeer geplaatst te worden, dus op de branch locatie zelf en in het datacenter. WAN optimization functionaliteit maakt gebruik van TCP optimalisatie, caching van bekende protocollen en kan op de branch locatie services aanbieden (DNS/DHCP/File/Print) waardoor hier geen server aanwezig hoeft te zijn. Bekende oplossingen zijn van Riverbed, Expand, Cisco (WAAS), Juniper (WXC) en Citrix (Repeater).

8.11 802.1x

Voordat een gebruiker verbinding met het bedrade of draadloze (WiFi) network maakt moet hij zich authenticeren op het netwerk. Op grote draadloze netwerken met centrale authenticatie wordt hiervoor vaak de standaard WPA(2)-Enterprise. Deze authenticatie past het 802.1x protocol toe dat op zijn beurt weer gebruik maakt van een RADIUS service. De RADIUS service kent de directory services (bijv. Active Directory) zodat de gebruiker de credentials zoals deze in de directory service bekend zijn kan benutten. Het 802.1x protocol kan ook toegepast worden op bedrade netwerken zodat niet iedere gebruiker een apparaat kan koppelen op het bedrade netwerk waarna een verbinding tot stand gebracht kan worden. Alle managed switches van bekende fabrikanten (zoals eerder genoemd in de whitepaper) ondersteunen 802.1x.

8.12 LOAD BALANCER

Een server kan maar een bepaald aantal gelijktijdige netwerk connecties aan. Dit is afhankelijk van de kracht van de server en de service die gehanteerd wordt. Ook is het vaak nodig om een server redundant uit te voeren terwijl hier geen clustering techniek voor toegepast kan worden door beperkingen en gedrag van deze techniek. Door load balancer functionaliteit vóór deze server te plaatsen kan dit opgelost worden. De load balancer presenteert een virtual IP-adres in het netwerk welke opgenomen wordt in de DNS functionaliteit waarna de load balancer de sessies verdeeld over een aantal echte servers. De load balancer kan verschillende technieken aanwenden om te load balancen (OSI laag 3, laag 4 en laag 7). Sessies van apparaat A naar service X moeten tijdens de sessie wel bij dezelfde echte server aankomen, hiervoor wordt persistence toegepast. Bijvoorbeeld op basis van het client IP-adres wordt deze altijd naar dezelfde echte server doorverwezen. Dit kan ook door bijvoorbeeld een http cookie weg te schrijven op de client. De load balancer functionaliteit kan 'zien' of een echte server aanwezig is en of de benodigde service (bijvoorbeeld http) actief is. Op de server kan gebruik gemaakt worden van het Simple Network Management Protocol (SNMP), een TCP port check of een banner grab van bijvoorbeeld een http service, deze oplossingen zorgen ervoor dat de beschikbaarheid van de service gemonitored kan worden. Bekende Load Balancer fabrikanten zijn F5 (BigIP), A10 Networks, Cisco (ACE), Citrix (Netscaler) en KEMP.

8.13 WEB APPLICATION FIREWALL

Een Web Application Firewall (WAF) is specifiek bedoeld voor webapplicaties. Door de http sessie te analyseren en bepaalde commando's wel of niet toe te staan wordt de webapplicaties beschermd tegen ongewenst gedrag. Bekende fabrikanten van Web Application Firewalls zijn onder andere Cisco (functionaliteit in de ACE), F5 (ASM), Citrix (functionaliteit in de Netscaler).

8.14 (REVERSE) PROXY

Toen internetverbindingen nog overwegend traag waren werden proxy servers gebruikt om gegevens te cachen zodat data niet onnodig meerdere keren over de internet verbinding ging. Tegenwoordig wordt proxy functionaliteit in twee richtingen toegepast: in de forwarding proxy en de reverse proxy. De proxy functionaliteit wordt gebruikt als beveiligoplossing voor zowel gebruikers die het internet (forwarding proxy) raadplegen, als voor gebruikers die vanaf het internet gebruik maken van een applicatie of resource (reverse proxy). De proxy doet in beide gevallen een 'man in the middle'. De sessie wordt niet meer vanaf de gebruiker naar de service opgezet, maar de proxy doet dit voor de gebruiker. Hierdoor kunnen verschillende functionaliteiten toegepast worden zoals Anti-Virus en Content Filtering op het verkeer. Indien de gebruiker een encrypted sessie (SSL) wil gebruiken kan de proxy ook hier het verkeer analyseren doordat de proxy de SSL encryptie afhandelt (in het geval van reverse proxy SSL offloading). Bekende fabrikanten van proxy functionaliteit zijn Microsoft (TMG) en Bluecoat (ProxySG).

8.15 WiFi

Draadloze netwerken zijn bijna overal aanwezig en er zijn veel fabrikanten die oplossingen leveren. Onderscheidend is het centraal beheer van grote draadloze netwerken en hoe flexibel met access points omgegaan kan worden. Bekende fabrikanten van WiFi-functionaliteit zijn bijvoorbeeld Cisco, HP Networking, Aruba en Trapeze.

8.16 2-Factor Authentication

Een gebruiker die via SSL VPN functionaliteit applicaties en resources gebruikt, moet zich eerst authenticeren. Waar dit bij 802.1x gebeurt op basis van credentials zoals deze bekend zijn in de directory service, is dit bij een SSL VPN verbinding niet voldoende. Gebruikers die zich hier authenticeren maken gebruik van een one-time-password (token) om een extra authenticatie toe te voegen. Naast de bekende credentials voert de gebruiker een tweede wachtwoord in dat door een fysiek of SMS token gegenereerd wordt. Bekende fabrikanten van 2-Factor authentication zijn bijvoorbeeld RSA, Cryptocard en ActivIdentity.

9. VERVOLG

Alle onderdelen van het solution schema zijn uitgelegd. De mogelijkheden ontwikkelen zich snel op alle gebieden. Secure Access en Secure Networking zal hierin mee moeten. Technieken als Virtualisatie kunnen gebruikt worden om SASN functionaliteit te virtualiseren. Met de intrede van cloud computing ontstaan nieuwe beveiligingsvraagstukken waardoor functionaliteit toegevoegd zal moeten worden.

10. AUTEUR(S)

Martijn Doedens (1981) is sinds 2007 werkzaam bij PQR op het gebied van networking en security oplossingen. Na zijn studie Hogere Informatica is hij bij PQR gaan werken als Engineer en kort daarna als Consultant. Naast het ontwerpen houdt hij zich ook nog steeds bezig met het daadwerkelijk inrichten van complexe datacenter netwerken. Martijn is vooral actief op het gebied van routing en switching designs, firewalls, intrusion detection & prevention en andere security oplossingen. Hij is breed gecertificeerd op Cisco, HP en Juniper oplossingen en heeft daarnaast ook fabrikant-onafhankelijke certificeringen waaronder Certified Ethical Hacker.

PQR B.V.
Rijnzathe 7
3454 PV De Meern
The Netherlands

Tel: +31 (0)30 6629729
Fax: +31 (0)30 6665905
E-mail: info@pqr.nl
www.PQR.com

as