Publicatiedatum: september 2017

Veilige externe toegang tot bedrijfsnetwerk

Ik stonk er weer in. Ik kwam via via op een site terecht met zeer bruikbare technische achtergrond informatie waarin DirectAccess werd vergeleken met traditionele VPN oplossingen.
Gegrepen door deze schat aan informatie begon ik enthousiast aan mijn volgende blog in de 'vrije momentjes'. Echter hoe verder ik vorderde met het artikel kwam bij mij, gelukkig op tijd, de gedachtenomslag dat het helemaal niet om de techniek draait. De techniek en oplossingen zijn slechts ondersteunend aan het grotere (bedrijfs)plaatje.

Wat zit er dan in dat (bedrijfs)plaatje?
1. Techniek moet het werk doen zonder (extra) eindgebruikers interactie
2. IT veiligheid op het hoogst mogelijke en noodzakelijke niveau brengen zonder dat de eindgebruiker daar hinder van ondervind

Daarbij komen aspecten als:
- Het bedrijfsbeleid op IT vlak (ook wat betreft toegang of afstand)
- Eindgebruikers middelen
- Kwalificatie en beveiliging van data/content

Samengevat: Makkelijk (in gebruik en in onderhoud) , veilig en flexibel!
In een organisatie waar IT in dienst staat van het gehele bedrijf als facilitator zullen bovenstaande punten vaak de revue passeren bij het maken van keuzes.
Door het '(bedrijfs)plaatje' als uitgangspunt te nemen krijgen de aspecten van de potentiele mogelijkheden een andere waardering.

Het ideale (bedrijfs)plaatje
De tot nu toe genoemde aspecten schuren tegen het idee van een ideale IT omgeving aan.
Maar waarom zouden we dat niet zo dicht mogelijk willen benaderen?
Het maakt het vergroten van het draagvlak aan alle kanten binnen een organisatie makkelijker. En is het dan duurder?
Ik denk dat op de lange termijn het veel goedkoper is ondanks dat de behaalde winst niet op alle punten in geld is uit te drukken. En wat tellen we wel mee in een Business Case? Vallen daar ook HR en frustratiekosten onder?
Geld is een middel en niet een doel om de juiste keuze te kunnen onderbouwen.

Maar terug naar de titel...
Zoals dat vaak gaat vallen, in de tijd gezien, dan de puzzelstukjes in elkaar.
Gisteren was er een webinar van de Amerikaanse goeroe van DirectAccess Richard Hicks.
Misschien heeft u meegekeken en geluisterd. Ook voor mij was het spannend want ik weet niet wat hij heeft behandeld terwijl ik dit stuk (het technische deel daarvan) al zo goed als mogelijk had afgerond.

Het doel van de webinar
Het doel van deze webinar is verbreding van de horizon van IT mensen.
Er is meer dan je weet en dan je kent.
De meeste IT mensen zijn van nature erg nieuwsgierig naar de (nieuwe) mogelijkheden.

Er zijn maar 2 smaken: of VPN of DirectAccess
Richard Hicks zit al 20 jaar in het vak. Tot voor kort had hij nooit van NetMotion gehoord en beperkte zijn blikveld zich tot of een VPN of Direct Access om van buiten af veilige toegang tot het netwerk te kunnen faciliteren.
Doordat hij kennis heeft gemaakt met NetMotion Mobility beschikt hij opeens over een extra keuze die hij aan zijn klanten kan voorleggen om het gewenste bedrijfsplaatje op het vlak van externe toegang te kunnen invullen.

Een alternatief met het beste van beide werelden?
Waar er eerst een alternatief was voor een traditionele VPN in de vorm van DirectAccess weet ik dat de Mobility oplossing in vele situaties vele malen krachtiger en flexibeler is.

De unieke en sterke punten van Mobility (bovenop die van traditionele VPN en DA):
- Applicatie persistentie ("in stand houdend") bij het wisselen van netwerk verbindingen (wifi-wifi/wifi-wwan/wifi-lan)
- Applicatie persistentie ("in stand houdend") bij netwerk onderbrekingen
- Gebruikersvriendelijke en automatische veilige toegang en gebruik van 'captive portals'
- Policy controle. Split tunnel mogelijk "on the fly" maar bijvoorbeeld ook applicaties en/of updates wel of niet toegestaan op bepaalde type verbindingen/tijden of prioriseren met Quality of Service (kortweg:QoS)
- Groter bereik bij mobiele verbindingen (wifi en 2G/3G/4G) door slimme data-afhandeling
- Dataverkeer besparing mogelijk bij vele applicaties
- VoIP en video verkeer zeer goed bruikbaar tot aan 30% packet loss over de verbindingen.
- Real-time inzicht en historische rapportage over alle zaken die we in onze vaste netwerken al jaren gewend zijn. Denk aan het dataverbruik per applicatie, hoe vaak applicaties worden gestart, welke versies van applicaties actief zijn, de connectiestatus van elk device en nog meer.

Het is tijd om te kijken of Mobility in uw (bedrijfs)plaatje past. Werken zonder gedoe is mogelijk.

Voor degene die meer diepgaande informatie willen hebben, hieronder een bloemlezing van de diverse blog's van Richard Hicks.

Met een 'op afstand' digitale groet,

Richard Stemfoort

Bloemlezing: Veilige externe toegang tot bedrijfsnetwerk (technische vergelijking)

In de uitwerking beperk ik me hier tot die oplossingen die een verbinding tussen een eindgebruiker en de centrale infrastructuur van een bedrijf opzetten.

'Traditionele' VPN
Een 'Virtual Private Networking' (VPN) bestaat al jaren en is een volwassen, en beproefde techniek en wordt breed toegepast. Het is 'de standaard' manier voor veilige externe toegang tot bedrijfsnetwerken. Bovendien ondersteunt het vrijwel altijd de nieuwe protocollen en kan het draaien op verschillende platformen (Operating systemen) en zijn goed te integreren met multifactor authenticatie platformen.

VPN randvoorwaarden
De meeste traditionele Client gebaseerde VPN's hebben de nodige aandachtspunten. VPN verbindingen moeten door de eindgebruiker worden geactiveerd en zijn dus optioneel te gebruiken. De gebruiker beslist wanneer hij of zijn de VPN gebruikt en wanneer niet. De meeste VPN oplossingen hebben extra software nodig. Dit vereist aandacht bij de uitrol en daarna onderhoud. Het opzetten van verbindingen kan potentieel ook problemen opleveren omdat de VPN protocollen niet firewall vriendelijk zijn en niet op alle locaties derhalve functioneren.

VPN uitdagingen
Vanuit veiligheidsoogpunt is sterke authenticatie vereist. Dit omdat iedereen kan proberen een VPN verbinding op te bouwen vanaf een willekeurige client. Het integreren van een multifactor authenticatie maakt het complexer en moeilijker te onderhouden. Bovendien vereist het meestal ook extra hardware, licenties en support kosten. VPN omgevingen kunnen prijzig zijn om te implementeren en te onderhouden. Algemeen gebruikelijk is dat ze fabrikant specifieke hardware vereisen en afwijkende management vaardigheden. Veel VPN oplossingen vereisen extra licenties. Het schalen van VPN producten vereist bovendien bijna altijd extra hardware. Alles opgeteld kan de totale investeringsom voor een VPN oplossing aardig oplopen.

DirectAccess
DirectAccess is een relatieve nieuwkomer in de wereld van veilig op afstand toegang krijgen tot een netwerk. DirectAccess (kortweg DA) verschilt fundamenteel van VPN door een naadloos en transparant 'altijd aan' verbinding. DirectAccess verbindingen worden door de machine 'beheerd' en niet door de eindgebruiker. DA verbindingen zijn veilig en geauthentiseerd en worden automatisch., wanneer er een actieve internet verbinding is, verbonden. DA verbindingen zijn altijd bi-directioneel wat een belangrijk verschil is. De mogelijkheid om 'uitgaand' verbinding met een client te maken geeft IT beheerders nieuwe mogelijkheden.

De sterke punten van DA
DA verbindingen zijn van nature veiliger dan traditionele VPN's. DA clients moeten lid zijn van een domein, en in de meeste configuraties, moeten ze ook een certificaat hebben uitgegeven door het bedrijfs- interne Public Key Infrastructure (PKI). Hierdoor wordt een vorm van multifactor toegepast met als gevolg een veel hogere zekerheid op legitieme

clients die toegang krijgen tot het netwerk. DA kan ook integreren met veel bestaande multifactor oplossingen en authenticatie aanbieders om de gebruikers authenticatie op een hoger niveau te tillen indien dat gewenst is. DA is vriendelijk voor firewalls en het beheer daarvan. DA werkt overal waar een actieve internet verbinding voor handen is. Er hoeft geen extra software te worden geïnstalleerd. Het is gemakkelijker in gebruik dan een traditionele VPN. Alles bij elkaar opgeteld zal de productiviteit bij gebruikers omhoog gaan en is de management kostenpost overzichtelijk. DA is een beter betaalbaar alternatief voor traditionele VPN's. DA kan worden uitgerold op bestaande infrastructuur (fysiek of virtueel) en vereist geen dure specifieke hardware. Met DA is schaalbaarheid makkelijker en goedkoper dan traditionele VPN. DA kan beheerd worden met bestaande systeem management tools en Windows Administrator kennis.

De beperkingen van DA
DA is niet een alomvattende 'remote access' oplossing. Het is alleen ontwikkeld voor aangemelde domein Windows clients. Als aanvulling DA moet worden uitgerold met de zakelijke beschikbare Windows licentie pool. Er zijn enkele gevallen bekend waarin applicaties niet compatibel zijn met DA. Er is geen ondersteuning voor DA op 'niet gemanagede' Windows apparaten, particuliere Windows licenties en alle niet Windows draaiende OS-en. Dat maakt dat een traditionele VPN nog steeds noodzakelijk kan zijn. Bij verstoringen is een brede en diepgaande kennis vereist van de opbouw om het probleem te kunnen oplossen.

Ontwikkelingen rondom DA
Ondanks dat DA een relatief nieuw product is lijkt het er op dat Microsoft in de niet verre toekomst afscheid wil nemen van DA. Microsoft adviseert zijn klanten om over te stappen op 'always on VPN' van Microsoft. Een overstap brengt wat voordelen maar brengt zeker ook nieuwe nadelen met zich mee. Nu worden alle W10 licentie varianten ondersteund. Het kan nu ook IPv4 ondersteunen en heeft wat meer mogelijkheden op netwerk access control (NAC). Het werkt dus alleen nog maar met Windows 10 en het kan niet meer beheerd worden met Active Directory en group policies. Het moet nu worden beheerd en geconfigureerd met Microsoft System Center Configuration Manager (SCCM), Microsoft Intune, or PowerShell.

DirectAccess or VPN?
Wat moet ik nu kiezen: DA of een VPN? Waarom niet beide?
Het gebruik van de ene sluit de andere niet uit. Ze kunnen naast elkaar bestaan en vullen elkaar op menig vlak aan. DA kan gebruikt worden voor veilige toegang op afstand voor apparaten onder beheer van de IT afdeling terwijl de VPN kan worden gebruikt voor de niet gemanaged apparaten.
Hoewel je met DA de traditionele VPN niet volledig kan elimineren kan het zeker helpen de het aantal VPN verbindingen naar beneden te brengen. Hierdoor wordt bespaart op dure hardware en bijbehorende licenties en het onderhoud van de traditionele VPN omgeving.

door Richard Hicks samengevat
DA is niet simpelweg een andere VPN oplossing. Het heeft standaard meer veiligheid aan boord en is meer kosten effectief als traditionele VPN oplossingen. DA heeft geen concurrentie als het aan komt op standaard veiligheid en gebruiksgemak. Productiviteit en beperkte infrastructuurkosten helpen hier aan mee.
DA kan worden opgebouwd op fysieke en virtuele machines en kan worden beheerd met standaard Windows management tools.

Tot zover de behoorlijk complete vertaling van de inhoud van de diverse blog pagina's. Maar dit verhaal is zeker niet af en zeker niet compleet.

NetMotion Mobility in plaats van DA en traditionele VPN?
Beste van beide werelden
Ook hier blijkt dat de onbekendheid van NetMotion Mobility een groot nadeel is. Nu is NetMotion Mobility zeker geen traditionele VPN en is het in de eerste plaats een connectiviteitsproduct. Dat betekend dat alle geschetste voordelen van DA ook van toepassing zijn op NetMotion Mobility. Bovendien kan Mobility andere OS-en (iOS, OSX en Android tot teruggaande WindowsMobile 5) aan en steunt het op netwerkvlak zowel IPv4 en IPv6. Alle geschetste nadelen van een traditionele VPN vallen bijna allemaal af.

Samengevat
Hieronder haal ik de aspecten aan die ik uit de bloemlezing hierboven heb gehaald. Ik ben me bewust dat ik aan de traditionele VPN kant niet het gehele speelveld kan overzien. Hierdoor kunnen bepaalde punten per fabrikant totaal verschillend zijn.

DirectAccess t.o.v. traditionele VPN
- 'Always on'
- Makkelijk in gebruik voor eindgebruiker
- Geen extra client/agent software
- IPV6 ready
- PKI vereist (multi factor)
- Bi-directionele tunnel
- Geen fabrikant specifieke VPN hardware vereist
- Virtueel of fysiek op te bouwen
- Geen extra VPN licenties nodig (maar wel Microsoft, afhankelijk van licentie overeenkomst)
- standaard split tunneling aan
- Beperkte OS ondersteuning (alleen (specifieke) Windows)
- Niet alle applicaties zijn te gebruiken
- Alleen beheerde apparaten mogelijk
- Toekomst ongewis

Gedeelde aspecten DirectAccess en Mobility
- 'Always on'
- Makkelijk in gebruik voor eindgebruiker
- IPV6 ready
- Bi-directionele tunnel
- Geen fabrikant specifieke VPN hardware vereist
- Virtueel of fysiek op te bouwen

Traditionele VPN t.o.v. DirectAccess
- Zeer beproefd/uitgerijpt concept
- Alle protocollen
- Meer(dere) Operating Systemen ondersteuning
- Vereist bijna altijd fabrikant specifieke hardware
- Vereist client/agent op eindgebruiker systemen
- Vereist 'niet-Microsoft' licenties

Gedeelde aspecten traditionele VPN en Mobility
- Zeer beproefd/uitgerijpt concept
- Alle protocollen
- Meer(dere) Operating Systemen ondersteuning
- Vereist client/agent op eindgebruiker systemen
- Vereist 'niet-Microsoft' licenties

Unieke aspecten Mobility t.o.v. traditionele VPN en DirectAccess
Naast de al genoemde gedeelde aspecten van DA, traditionele VPN en Mobility:
- 'Always on'
- Makkelijk in gebruik voor eindgebruiker
- IPV6 ready
- Bi-directionele tunnel
- Geen fabrikant specifieke VPN hardware vereist
- Virtueel of fysiek op te bouwen
- Zeer beproefd/uitgerijpt concept
- Alle protocollen
- Meer(dere) Operating Systemen ondersteuning
- Vereist client/agent op eindgebruiker systemen
- Vereist 'niet-Microsoft' licenties

*Bezit Mobility de volgende **unieke aspecten:***
- Elke applicatie werkt (zolang die maar over een TCP/IP interface verbinding maakt)
- Elke applicatie wordt overeind gehouden bij netwerkwissel en bij verbindingsverlies of onderbreking
- Automatische, veilige en gebruiksvriendelijke captive portal functie
- Centrale beheer console (webinterface) met standaard rapportages voor snelle analyse en onderzoek
- Meerdere authenticatie vormen naast elkaar (NTLM, Radius, PKI, RSA)
- Policy module. Split tunnel mogelijk "on the fly" maar bijvoorbeeld ook applicaties en of updates wel of niet toegestaan op bepaalde type verbindingen/tijden op prioriteren met Quality of Service.
- NAC voor externe partijen die toegang willen tot netwerk/applicaties
- Databesparing. Compressie mogelijk en instelbaar op interface snelheid en blokkering applicaties/(netwerk)routes op bepaalde type (duurdere) verbindingen
- Groter bereik bij mobiele verbindingen (wifi en 2G/3G/4G) door slimme data-afhandeling
- VoIP en video verkeer blijven zeer goed bruikbaar tot aan 30% packet loss over de verbindingen.

Ik heb dit artikel naar eer en geweten samengesteld en ik dank mijn naamgenoot voor het mogen putten uit zijn kennis en blogs.
Ondanks de grote zorg die ik heb besteed aan dit artikel kan het altijd voorkomen dat er onjuistheden in zijn geslopen.

Publicatiedatum: september 2017.