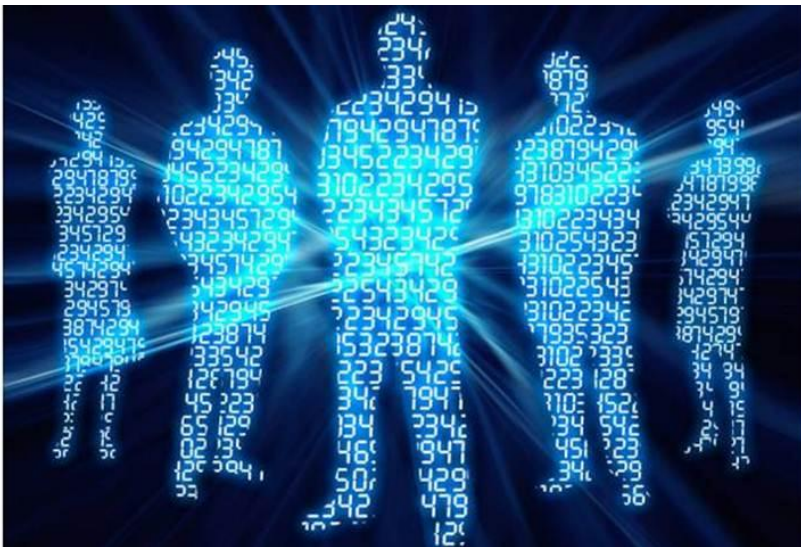


WHITEPAPER 802.1X

SERIOUS BUSINESS FOR YOUR NETWORK

802.1x betekent een sterk verhoogde veiligheid van uw netwerk. **802.1x** is volledig transparant voor alle applicaties. Mits voldaan aan de voorwaarden zorgt **802.1x** voor weinig beheer. De kosten voor het invoeren van **802.1x** zijn laag. Genoeg redenen om verder te lezen.

In deze whitepaper leest u: wat is 802.1x? Waarom zou ik het implementeren en wat zijn de voordelen en de nadelen? Hoe kan 802.1x mij helpen in het kader van Bring Your Own Device (BYOD)?



Inleiding

Technisch gezien is het IP-netwerk (Local Area Network of LAN) van een bedrijf het fundament van het 'ICT Huis'. Een goed ingericht netwerk is randvoorwaardelijk om vervolgens servers, telefonie en applicaties te kunnen draaien. Deze applicaties ondersteunen dan weer de primaire bedrijfsprocessen.

Het is 'common sense' om een netwerk te segmenteren in VLAN's (Virtual LAN). Eigenlijk is dit het indelen van het netwerk in denkbeeldige losstaande LAN's.

Kleine IP-subnetten / VLAN's brengen de volgende voordelen met zich mee:

- *Beperkt failure domain*: een groep van layer-2 switches wordt een layer-2 switched domain genoemd. Een layer-2 switched domain kan worden gezien als failure domain. Wanneer bijvoorbeeld een slechte netwerkkaart 'errors' veroorzaakt, dan heeft het gehele domain daar last van.
- *Broadcast domain*: MAC-layer broadcasts vloeien door het gehele layer-2 switched domain. Teneinde de scope van broadcast domains te beperken worden layer-3 switches ingezet die, bijvoorbeeld DHCP-broadcasts omzetten naar het unicast adres van de DHCP server.

- *Common access policy*: Een groep servers ondergebracht in hetzelfde VLAN, kan met behulp van access control lists (ACL) worden geassocieerd met een gemeenschappelijke access policy. Bijvoorbeeld het verbieden van toegang tot het voice-VLAN voor andere toepassingen dan strikt noodzakelijk is voor IP telefonie.
- *Multicast controle*: Voor de controle en distributie van multicast verkeer draait op layer-3 switches het Protocol Independent Multicast (PIM) routing protocol en op layer-2 switches het Internet Group Membership Protocol (IGMP snooping). De combinatie van beide protocollen zorgt ervoor dat een multicast alleen gestuurd wordt naar de poort die is aangemeld voor de multicast video stream. Een goed gesegmenteerd netwerk biedt een optimale basis voor Multicast controle.
- *Beheer (overzicht/troubleshooten)*: Bij een bepaald IP-adres is onmiddellijk de bijbehorende switch te achterhalen. Voorts bieden kleine subnets het voordeel om snel een subnetscan uit te kunnen voeren bij problemen. Ook distributiesoftware maakt gebruik van subnetscanners.
- Een 'broadcast storm' of 'Denial of Service aanval' in een bepaald VLAN veroorzaakt geen verstoring in de overige VLAN's.

VLAN's worden toegewezen per poort op een netwerk switch. Een standaard toegangspoort in een netwerk verschaft in de regel toegang tot het data VLAN voor kantoorautomatisering en het voice VLAN voor IP telefonie. Deze poorten worden Multi-VLAN poorten genoemd. Om er voor te zorgen dat enkel geregistreerde apparatuur en geregistreerde gebruikers toegang hebben tot het netwerk en het juiste VLAN, kan gebruik worden gemaakt van IEEE 802.1x. 'Dot1x' zorgt er voor dat een telefoon geauthentiseerd wordt in het voice VLAN en een werkstation in het data VLAN.

Wat is 802.1x?

De IEEE 802.1x standaard bevat zowel een architectuur en functionele elementen als protocollen die wederzijdse authenticatie ondersteunen. Middels deze standaard wordt toegang beheerd en geverifieerd voor draadloze en bekabelde ethernet netwerken.

Dot1x is initieel ontworpen voor het controleren van toegang tot draadloze netwerken, maar kan dus ook uitstekend worden toegepast voor bekabelde netwerken.

Wanneer een apparaat op een switchpoort wordt aangesloten of wireless verbinding wil maken, dient het apparaat zich te authenticeren. Afhankelijk van deze authenticatie kan het apparaat verbinding maken met het achterliggende netwerk.

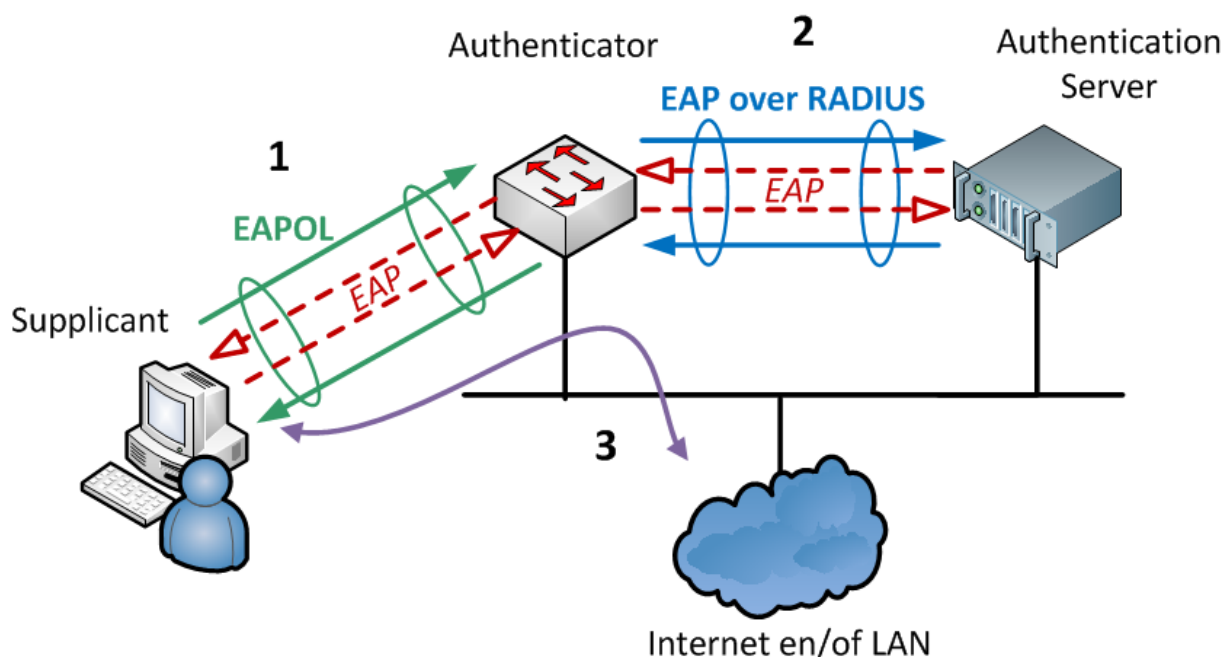
Architectuur

Er zijn drie basiscomponenten binnen 802.1x:

- de aanvrager of supplicant (de clientsoftware)
- de vericator of authenticator (het draadloos Access Point of de switch)
- de authentication server (een RADIUS-server)

Er wordt een verzoek om toegang gestuurd door de cliënt/supplicant naar de authenticator. Deze authenticator vraagt de cliënt zich te identificeren. Hierop verzendt de cliënt een identiteitspakket dat wordt doorgegeven aan de authenticationserver. Deze authenticationserver kan de gebruiker (via wachtwoorden of certificaten) en/of het systeem (via certificaten of MAC-adres) verifiëren. Vervolgens stuurt hij een acceptatiepakket terug naar de authenticator die vervolgens de cliënt instelt als geautoriseerd. De cliënt kan nu op het netwerk. Indien niet succesvol dan kan het device in een 'authentication fail' VLAN of in een gast VLAN worden geplaatst.

De authenticator is eigenlijk een doorgeefluik tussen de RADIUS-server en de supplicant.



Figuur 1: 802.1x Basiscomponenten

Een voorbeeld: een gebruiker wil met een pc, pda of ander apparaat gebruik maken van het netwerk. De switch of draadloos Access Point accepteert in eerste instantie enkel het verzoek om toegang tot het netwerk. Als antwoord vraagt de switch of het draadloos Access Point naar de identiteit van de gebruiker of het apparaat. Deze gegevens worden vervolgens doorgestuurd naar een Radius-server, die bepaalt of de gebruiker of apparaat inderdaad is wie hij zegt te zijn en welke rechten de betreffende gebruiker heeft. Op basis van deze gegevens en eventueel extra criteria wordt de gebruiker al dan niet toegelaten en in het juiste VLAN opgenomen.

Protocollen

Het protocol dat gebruikt wordt voor authenticatie in de IEEE 802.1x-standaard is EAP of Extensible Authentication Protocol.

Het EAP protocol wordt op twee manieren getransporteerd over het IP-netwerk:

- EAP over LAN (EAPOL) tussen Supplicant en Authenticator;
- EAP over RADIUS (EAP in een RADIUS pakket) tussen Authenticator en de RADIUS server.

Wanneer 802.1x wordt ingeschakeld op een netwerkpoort, zal er door deze poort enkel EAP verkeer worden toegelaten. Default zal een switch tot 3 maal (om de 30 sec.) een EAP request versturen naar het aangesloten device. Binnen die termijn zal er een EAP respons ontvangen moeten worden waarin het device zich identificeert. De switch zal dit in een RADIUS request versturen naar de RADIUS server welke de ontvangen credentials of certificaat zal controleren. Op basis daarvan zal de authenticatie succesvol zijn of niet.

EAP is de absolute kern van 802.1x. Het bevat verschillende modules of methodes om de manier van authenticeren te regelen: EAP-MD5, PEAP, LEAP, EAP-FAST, EAP-PSK, EAP-TLS, EAP-TTLS enz. We bespreken kort de meest gangbare methodes.

EAP-MD5

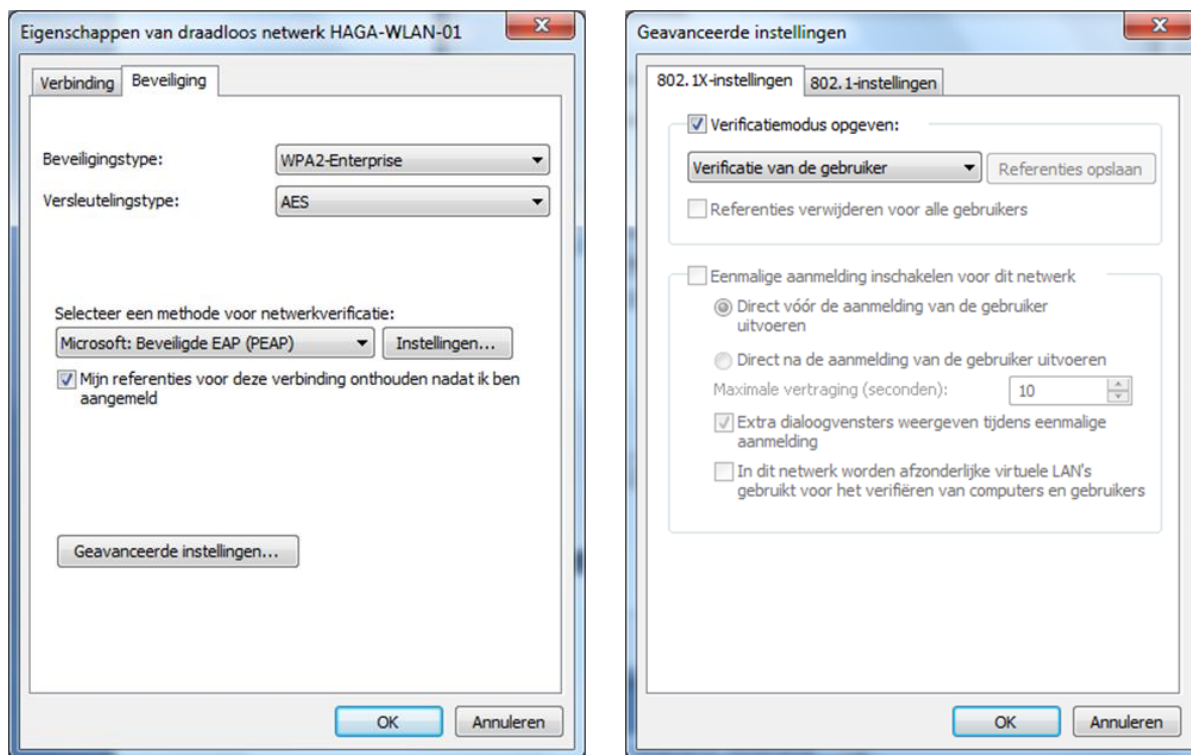
EAP-MD5 is een eenvoudige variant waarvan veel apparatuur, waaronder IP telefoons gebruik maken. Er wordt hier gebruik gemaakt van een username en password. In het geval van een IP telefoon is de username vaak het MAC adres van de telefoon en het password een bepaalde pincode (bijv. 1234). Een nadeel van deze methode is in dit geval de beheerimpact. Elk MAC adres met bijbehorende pincode dient centraal te worden ingevoerd op de RADIUS server. De pincode wordt vaak voor elke telefoon gelijk gekozen, waardoor de beveiliging niet echt optimaal is. Bovendien is EAP-MD5 een éénrichting authenticatie, waarbij de identiteit van de authentication server niet gecontroleerd wordt.

PEAP

PEAP biedt een prima oplossing voor Microsoft cliënten. Er wordt hier gebruik gemaakt van de centrale Active Directory database. In eerste instantie kan hiermee device (of machine) authenticatie worden uitgevoerd. Het device dient dan ook te zijn opgevoerd in Active Directory. Naast device of machine authenticatie kan er ook gebruik worden gemaakt van user authenticatie. Het moge duidelijk zijn dat in dit geval ook de user dient te zijn opgevoerd in MS-AD.

In de regel wordt er voor deze oplossing een LDAP (Lightweight Directory Access Protocol) koppeling gemaakt tussen de RADIUS server en de Domain Controller.

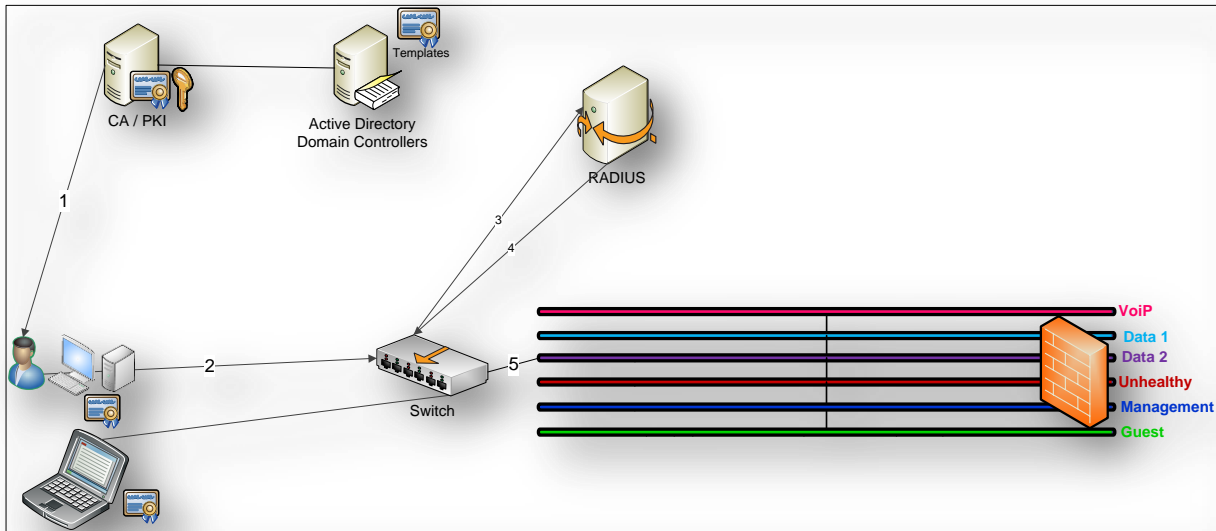
Er wordt op de RADIUS server nu geen gebruik gemaakt van zijn lokale database maar van de externe AD database. In het geval van een Microsoft RADIUS server, is de AD integratie heel gemakkelijk te configureren.



Figuur 2 Voorbeeld PEAP-MSCHAP

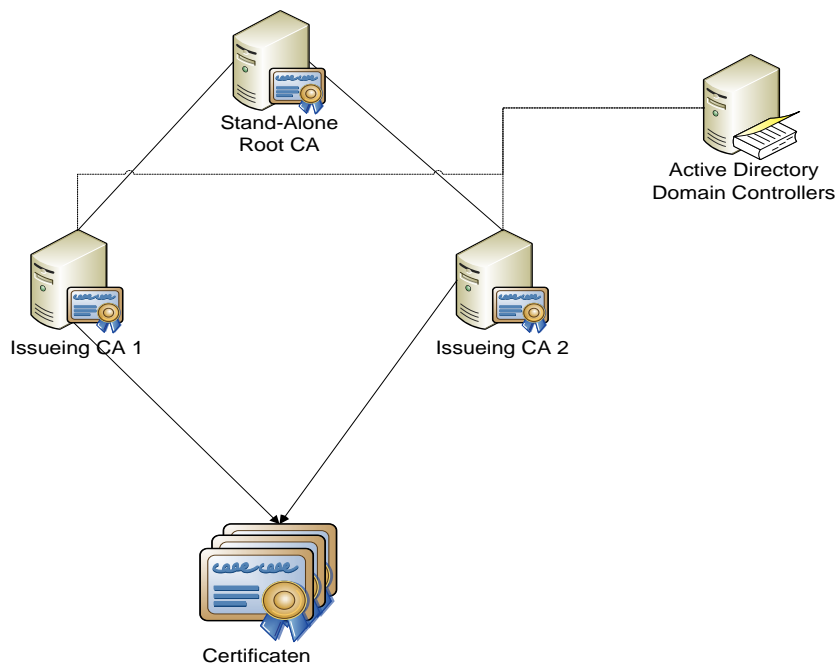
EAP-TLS

Eén van de veiligste EAP standaarden is EAP-TLS. Het wordt door heel veel leveranciers van hardware en software ondersteund. EAP-TLS maakt gebruik van certificaten. Alle cliënten en ook de RADIUS server worden voorzien van een certificaat dat intern wordt uitgegeven door een Public Key Infrastructure (een groep certificaat servers). Hierdoor vertrouwen de server en de cliënten elkaar. De hoogst mogelijke beveiliging krijg je wanneer de keys van de cliënt op een smartcard worden gezet. Deze kaart (en een kaartlezer) zijn dan nodig om toegang te kunnen krijgen tot ICT services en eventueel fysieke gebouwen.



Figuur 3 802.1x met EAP-TLS

Een Public Key Infrastructure (PKI) is een systeem waarmee het uitgeven en het beheer van digitale certificaten wordt gerealiseerd. Een certificaat dat door een certificaatautoriteit (CA) uitgegeven is, kan voor verschillende doeleinden gebruikt worden. De CA waarborgt de integriteit en authenticiteit van het certificaat en staat dus in voor de identiteit van de certificaatbezitter. Aangezien een CA de kopieën van de verstrekte certificaten bevat, alsook gegevens van de identiteiten aan wie ze zijn verstrekt, is beveiliging van de gehele PKI-infrastructuur van groot belang.



Figuur 3 PKI Infrastructuur

Voor devices die geen EAP-TLS ondersteuning bieden, kunnen andere EAP methodes geconfigureerd worden op de RADIUS server.

Voor apparaten die helemaal geen 802.1x ondersteunen, zoals sommige printers, wireless AP's en thin clients¹, kan er gebruik worden gemaakt van Mac Authentication Bypass (MAB). Indien dit (additioneel) op een poort is geconfigureerd, zal er na drie verstuurd EAP requests een poging worden gedaan om het MAC-adres of hardware-adres² van de client te gebruiken voor authenticatie. Dit MAC-adres wordt naar de authentication server gestuurd die het vervolgens opzoekt in een locale database. Deze database dient actueel gehouden te worden en veroorzaakt extra beheer. Mac Authentication Bypass is dus een laatste redmiddel om ook devices aan te sluiten die geen 802.1x ondersteunen.

Voordelen

1. Veiligheid

802.1x betekent een sterk verhoogde veiligheid van het netwerk. Middels 802.1x is het niet meer mogelijk om zomaar een willekeurige ethernet kabel te nemen om toegang te krijgen tot het netwerk. Een device dat niet van het bedrijf is, kan automatisch de toegang geweigerd worden.

2. Transparant

802.1x is volledig transparant voor alle applicaties. Nadat toegang is verschaft tot het netwerk heeft het geen enkele invloed op applicaties. Standaard vindt er elk uur (onderwater) een herauthenticatie plaats. Ook hiervan merkt een gebruiker niets. Het enige punt van aandacht zijn zaken als PxE boot, hetgeen veel gebruikt wordt voor het imagen van werkstations en Wakeup On LAN (WOL). Hiervoor is enige tuning noodzakelijk, hetgeen normaliter in een pré-productie omgeving wordt uitgevoerd.

3. Beheer

Mits goed voorbereid in een préproductie-omgeving en goed gedocumenteerd blijft de impact op het beheer beperkt tot de volgende zaken:

- Invoeren van username en password voor nieuwe gebruikers / devices bij gebruik van EAP-MD5 en MAB indien gebruikt.
- Beheer van de PKI omgeving bij gebruik van EAP-TLS. Deze zaken zijn echter vaak eenvoudig toe te wijzen aan de afdeling systeembeheer binnen een organisatie.
- Configuratie van Access Switches en draadloze toegang zijn eenmalige acties, welke eenmaal geconfigureerd, niet meer gewijzigd hoeven te worden.

4. Lage kosten

802.1x is een feature welke in de meeste gevallen standaard aanwezig is in netwerkapparatuur. De kosten voor het invoeren van 802.1x zijn dan ook beperkt tot de volgende zaken:

- Aanschaf van een redundant RADIUS server of gebruik van Microsoft RADIUS server welke standaard in een Microsoft Server licentie zit.
- Opzetten pré-productie omgeving
- Detail design en plan van aanpak
- Configuratie van draadloze en bedrade netwerkgeving
- Configuratie RADIUS server evt. met LDAP koppeling
- Desgewenst opzet van een PKI omgeving

¹ De meeste thin clients ondersteunen momenteel eveneens wired 802.1x. Dit moet nader onderzocht worden.

² Een MAC-adres is een uniek nummer per hardware device.

Mogelijke nadelen

1. Complexiteit

De implementatie van 802.1x is complex. Het vereist een gedegen kennis van alle onderdelen in de keten. Zonder een goed design en Plan van Aanpak is het bovendien niet mogelijk om 802.1x succesvol in te zetten. Alle mogelijke cliënts of supplicants dienen bekeken en getest te worden of en zo ja, welke methodes van EAP zij ondersteunen. Tenslotte dient er een redundante opstelling van zowel RADIUS servers als eventuele PKI infrastructuur opgezet te worden. De consultants van Innervate hebben echter uitgebreide ervaring om u bij al deze stappen te ondersteunen.

2. 802.1x en telefonie

Een 'best practice' in Voice-implementaties is het aansluiten van werkstations achter IP telefoons. Hierdoor is er slechts één poort per IP-toestel en werkstation nodig. De IEEE 802.1x standaard is echter geschreven voor maximaal één device per poort. Het risico bestaat hierdoor dat de telefoon wordt geauthenticeerd en daarmee gelijktijdig ook het apparaat achter de telefoon. Proprietary oplossingen van leveranciers als Cisco Multi Domain Authentication (MDA) maken het mogelijk dat beide apparaten elk op hun eigen methode geauthenticeerd worden. De PC bijvoorbeeld op basis van EAP-TLS in het data domein en de telefoon bijvoorbeeld op basis van EAP-MD5 in het voice domein.

Een randvoorwaarde waaraan voldaan dient te worden om bedraad 802.1x te kunnen gebruiken is het configureren van switchpoorten als multi-VLAN poort. Een IP Telefoon krijgt daarbij zijn voice VLAN meegedeeld door de switch via CDP of LLDP, of in zijn DHCP offer tijdens opstarten in het data VLAN.

3. Is BYOD niet meer mogelijk?

Initieel lijkt het erop dat Bring Your Own Device (BYOD) niet meer mogelijk is. Er wordt immers geen certificaat op een apparaat gezet dat niet in beheer is bij het bedrijf. Hierdoor kan dit apparaat geen rechtstreekse verbinding maken met het netwerk. Dit is echter de gewenste situatie. Hieronder beschrijven we hoe 802.1x juist faciliterend kan werken voor BYOD.

Gastentoeegang en BYOD

Hoewel Bring Your Own Device (BYOD) voor veel gebruikers als muziek in de oren zal klinken, kost het de gemiddelde IT-manager de nodige kopzorgen. Waar deze vroeger verantwoordelijk was voor een park met goed beveiligde, strak ingerichte, nauwelijks door de gebruiker zelf te veranderen computers, worden met BYOD opeens allemaal 'vreemde' systemen op het bedrijfsnetwerk toegelaten, met alle gevolgen van dien. Op basis van beveiligingsrichtlijnen (zoals NEN7510) zal het bieden van rechtstreekse toegang tot het bedrijfsnetwerk niet toelaatbaar zijn en is het raadzaam deze devices enkel tot een Internet VLAN voor gasten toe te laten. Dit is automatisch in te regelen middels 802.1x.

Op deze manier kunnen centrale web-based bedrijfsapplicaties worden benaderd, welke niet op een privé-laptop van een eindgebruiker geïnstalleerd kunnen worden vanwege beveiliging of kostenoverwegingen.

Met name voor derden, zoals partners, leveranciers, Consultants en contractors, alsmede medewerkers die hun privé device (BYOD) willen gebruiken binnen de domeinen van het bedrijf, is wireless en desgewenst ook wired gast toegang wenselijk.

Er dient een gescheiden Internet VLAN beschikbaar te zijn dat geschikt is voor het bieden van internettoegang aan haar gasten. Gasten kunnen via dit VLAN ongehinderd naar buiten. Leveranciers kunnen via het web beheerservers binnen het bedrijfsnetwerk benaderen als ze remote werken. Medewerkers kunnen met hun privé device bijvoorbeeld inloggen op de webmail. Een voorwaarde daarvoor is evenwel dat er een separate internet toegang is voor gasten omdat de meeste firewall's het niet accepteren dat gebruikers via de inside interface van een firewall naar buiten gaan om vervolgens via de outside interface van de zelfde firewall weer naar binnen te treden.

Netwerktechnisch, hetzij wired dan wel wireless, hoeven we er eigenlijk alleen maar voor te zorgen dat deze gebruikers in dit VLAN terecht komen om van daaruit op het internet te kunnen geraken. Voor wireless gasttoegang is het noodzakelijk dat er een extra SSID wordt aangemaakt, welk wordt 'gemapped' op dit VLAN. Voor wired gasttoegang dient er een extra regel te worden opgenomen in de 802.1x configuratie van elke poort.³

Indien de beschreven gast oplossing op basis van internet access niet te realiseren is, bijvoorbeeld omdat de bedrijfsapplicatie niet centraal web-based te benaderen is, kan er desgewenst naar een oplossing worden gekeken waarbij bij wijze van uitzondering het device wel rechtstreeks toegang krijgt tot het bedrijfsnetwerk.

En verder?

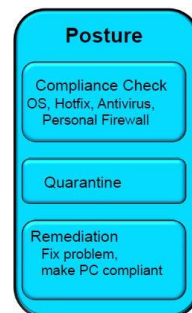
Wanneer netwerkbeveiliging middels 802.1x ingeregeld is, zijn er heel wat extra stappen mogelijk die ook absolute voordelen bieden voor gebruikers.

Indien gebruikers middels certificaten (EAP-TLS) geauthentiseerd worden op het netwerk, is het een relatief kleine stap om een gemakkelijkere manier van inloggen te voorzien. Je kan het gebruikerscertificaat op een smartcard plaatsen, idealiter dezelfde kaart als waarmee men het gebouw binnen kan komen. Deze kaart wordt dan in een kaartlezer gestopt en na het invoeren van een pincode logt de gebruiker automatisch in. Wanneer de smartcard verwijderd wordt uit de kaartlezer, kan het scherm automatisch 'gelocked' worden of kan de gebruiker weer uitgelogd worden. Een gebruiker dient hierdoor niet meer zijn gebruikersnaam en password te onthouden of op gezette tijdstippen telkens te veranderen. Hierdoor vermijdt men situaties waarbij gebruikers het password ergens noteren. Een win-win situatie dus. Wanneer dit inloggen met een smartcard ook nog eens gecombineerd wordt met een Single Sign-On oplossing dient de gebruiker slechts éénmaal in te loggen voor alle applicaties en services waar hij gebruik van mag maken.

De rol van de RADIUS server in de vorige hoofdstukken is enkel beschreven vanuit het perspectief van Authentication server. Het is echter mogelijk om heel wat extra functies van de RADIUS server te gebruiken, bijvoorbeeld accounting en rapportages. De RADIUS server houdt immers een log bij wie op welk device wanneer inlogt.

Een stap verder nog dan 802.1x gaat het toepassen van posture assessment technieken.

Microsoft biedt dit met Network Access Protection (NAP) en Cisco Systems met Network Access Control (NAC). Hiermee kan een device gecontroleerd worden op een aantal minimum vereisten:



Figuur 4 NAC

³ Om met name wired gast VLAN's gescheiden van de productieomgeving te kunnen implementeren binnen een organisatie, zijn technieken als MPLS-VPN en VRF-Lite beschikbaar. De consultants van Innervate beschikken over een schat aan ervaring met deze technieken.

of de encryptiesoftware wel is ingesteld, of de antivirusscanner aanwezig is en up-to-date is, of de juiste Windows versie en service pack geïnstalleerd is, enz. Het beschrijven van deze technieken gaat echter buiten de scope van dit whitepaper.

Waarom Innervate?

Innervate is een eredivisiespeler in het vakgebied van informatietechnologie en ICT infrastructuur. De professionals van Innervate zijn allemaal spelers met hun eigen specifieke expertise en praktijkervaring. Hierdoor is een succesvol 802.1x project gegarandeerd. Met een multidisciplinair team overzien we immers elke stap in de keten van 802.1x authenticatie. Concreet kunnen we helpen om het design te maken van zowel de 802.1x authenticatie als de PKI omgeving, om vervolgens alle onderdelen te configureren en af te stemmen op elkaar: cliënts, netwerk, PKI, Windows domein en RADIUS server.

Voor meer informatie:

Innervate

Aziëlaan 14
6199 AG Maastricht-Airport

Innervate Midden Nederland

De Corridor 21 A
3621 ZA Breukelen

T +31 (0) 43 358 1880

E info@innervate.nl

W www.innervate.nl

Volg ons op **LinkedIn**:

<http://nl.linkedin.com/innervate>

Volg ons op **Twitter** :

#InnervateNL

Volg ons op **Facebook**:

Innervate NL

Nawoord

Deze whitepaper is opgesteld door Jef Vleugels, Senior Consultant, en Peter Verstegen, Principal Consultant van Innervate, gebaseerd op recente projectervaringen op het gebied van 802.1x en Office Automation.