SURFnet

Innovatieflyer

802.1X

Het internet is zich aan het ontwikkelen tot een alomtegenwoordig medium. Binnen instellingen, maar ook daarbuiten, wordt dit gerealiseerd door bijvoorbeeld de aanleg van draadloze netwerken. Ook gastgebruikers met een laptop kunnen van deze netwerken gebruik maken indien de bezochte instelling dit toelaat. Met één set credentials (inloggegevens) is het mogelijk om op vele locaties gebruik te maken van het internet en zo van de applicaties van de eigen instelling.

Op deze manier ontstaat een instellingsoverschrijdende authenticatie-infrastructuur. Bovendien is de toegang (‘access’) tot de netwerken beveiligd. Daarnaast is het gewenst dat, afhankelijk van wie een laptop inplugt in een vast of draadloos netwerk, bevoegdheden op dat netwerk worden toegekend, zonder dat daarvoor fysieke aanpassingen nodig zijn. SURFnet doet onderzoek naar geschikte technologie om deze vormen van access op een veilige manier te realiseren en heeft daarbij gekozen voor IEEE 802.1X, een standaard van the Institute of Electrical and Electronics Engineers (IEEE).

Er is onderzoek gedaan naar meerdere oplossingen om instellingsoverschrijdende toegang tot het internet te kunnen bieden. Open toegang, WEP-gebaseerde oplossingen, MAC-gebaseerde oplossingen, oplossingen gebaseerd op VPN- en web-gateways en 802.1X zijn uitgebreid beoordeeld. Het bleek dat 802.1X van de mogelijke oplossingen de beste combinatie van beveiliging en schaalbaarheid biedt. SURFnet heeft daarom besloten om met deze technologie verder te gaan.

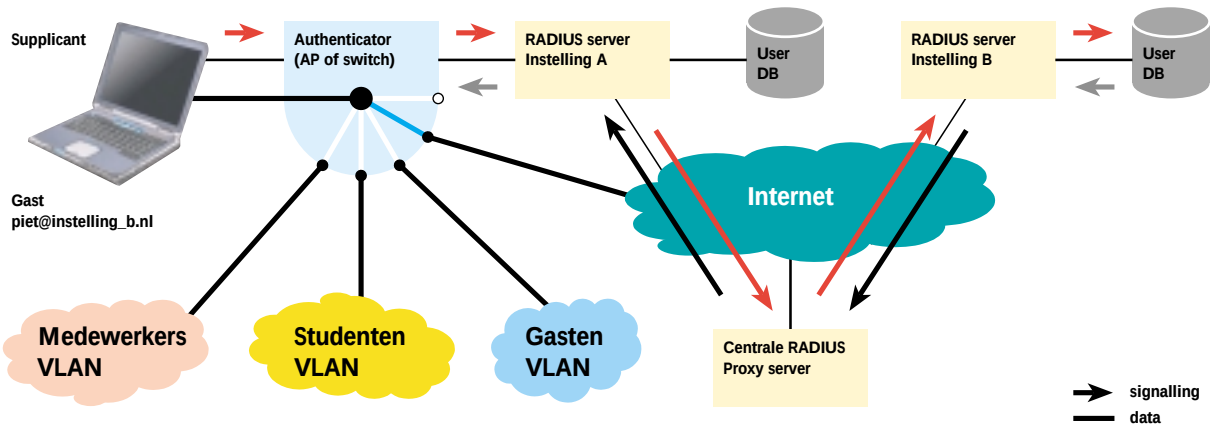
De standaard 802.1X

802.1X is een standaard voor poortgebaseerde authenticatie op laag 2 van het OSI-model en wordt gebruikt tussen een computer (pc, laptop of ander apparaat), in 802.1X termen de ‘Supplicant’, en een wireless Access Point of switch, in 802.1X termen de ‘Authenticator’. Authenticatie is gebaseerd op het Extensible Authentication Protocol (EAP), waardoor diverse vormen van authenticatie mogelijk zijn.
De communicatie tussen supplicant en authenticator verloopt via EAP over LAN. De authenticator zet het authenticatieverzoek in een RADIUS-pakketje en stuurt het door naar een RADIUS server. Deze server kan het pakketje desgewenst doorsturen naar een andere RADIUS server (in het geval van gastgebruik).
Door gebruik te maken van 802.1X zowel voor vaste als draadloze toegang kan probleemloos tussen vaste en draadloze netwerken worden ‘geroamed’.

De standaard is nog niet wijd geïmplementeerd, wat als een (tijdelijk) nadeel kan worden gezien. Ook is het momenteel voor de meeste besturingssystemen nog noodzakelijk om client software te installeren.

802.1X in praktijk

Een complete 802.1X infrastructuur ziet er bij gebruik voor wireless LAN toegang als volgt uit:



Voorbeeld van authenticatietraject, waarbij een gast-gebruiker wordt verbonden met het SURFnet-netwerk.

In feite introduceert 802.1X geen nieuwe componenten in het netwerk. Om 802.1X te laten werken, moet het aangezet worden in het Access Point, op de laptops van gebruikers en in een vaak al aanwezige RADIUS server. Een gebruiker maakt hierin verbinding met het netwerk via een Access Point, waarbij hij de credentials van zijn eigen instelling gebruikt (jan@instelling_b.nl). In geval van draadloze toegang tot het eigen netwerk, kan de RADIUS server van de betreffende instelling de gebruiker direct authenticeren, waarna verkeer kan worden doorgelaten. In geval van gastgebruik van het netwerk zal de RADIUS server van de gastinstelling de credentials via de SURFnet RADIUS infrastructuur doorspelen naar de RADIUS server van de instelling van de gebruiker, waar deze gebruiker wordt geauthenticeerd. Een melding of de authenticatie succesvol was wordt vervolgens weer doorgegeven aan de RADIUS server van de gastinstelling, waarna ook in dit geval verkeer wordt doorgelaten en de gebruiker in het juiste VLAN wordt geplaatst.

SURFnet heeft deze opstelling van november 2002 tot op heden in een testomgeving geïmplementeerd. Alfa & Ariss, de Universiteit Twente, de Hogeschool van Amsterdam en het SURFnet kantoor in Utrecht participeren hierin. Bij de test is gekeken naar de mobiele apparaten, access points, RADIUS servers, switches en naar de bruikbaarheid van het geheel. In de pilot is gekozen om te kijken naar de EAP authenticatietypen TLS (Transport Layer Security) en TTLS (Tunneled Transport Layer Security). Beide authenticatiemethoden gaan uit van het principe dat er eerst een veilige (TLS-) tunnel wordt opgezet naar de RADIUS server waarna binnen deze tunnel de eigenlijke authenticatie plaats vindt. De beide typen onderscheiden zich door het feit dat TLS zowel client als server authenticatie vereist (en daarmee een PKI) terwijl TTLS alleen servercertificaten nodig heeft.
Alfa & Ariss heeft in opdracht van SURFnet een freeware TTLS client ontwikkeld, die kan worden toegepast in een Windows-omgeving. Naar PEAP (Protected EAP) is in de testomgeving wel gekeken, maar dit protocol van Microsoft en Cisco komt niet in aanmerking voor uitrol op korte termijn.

Eerste resultaten

Er is in de pilot voor 802.1X gekeken naar de clients, access points, RADIUS servers, switches en naar de bruikbaarheid van het geheel. Gebleken is dat 802.1X uitkomst biedt voor veel wensen op het gebied van netwerktoegang op draadloze netwerken, voor zowel eigen gebruikers als gastgebruikers:
- Elke instelling kan één of meerdere authenticatiemethoden kiezen zonder aanpassingen in het netwerk;
- Het is mogelijk om als gast gebruik te maken van het netwerk van een andere instelling;
- De authenticatie van de gebruiker vindt plaats bij de eigen instelling;
- Het authenticatieproces is voldoende beveiligd;
- Het gebruik van 802.1X verloopt voor de eindgebruiker zonder grote hindernissen;
- Er kunnen na aanmelding op het netwerk door de RADIUS server extra attributen, zoals een VLAN of een IP-adres, worden toegekend aan de eindgebruiker;
- Wanneer een gebruiker het netwerk misbruikt, kan eenvoudig worden nagegaan waar en wanneer hij heeft ingelogd.

In de pilot zijn de volgende zaken met succes getest:
- Client: Funk, Meetinghouse en de TTLS client van Alfa & Ariss
- Access Point: Cisco (350 en 1200) en Orinoco (AP2000)
- RADIUS server: Radiator 3.3.1, FreeRADIUS (TLS)
- Switch: HP
- TTLS module: Alfa & Ariss

Met 802.1X is in voldoende mate te bewerkstelligen dat alleen geautoriseerde gebruikers toegang krijgen tot het netwerk van de instelling.

Meer informatie

De afdeling Innovatie Management van SURFnet doet onderzoek naar verschillende netwerktechnologieën en applicaties. Voor meer informatie over de implementatie van 802.1X kunt u contact opnemen met:
Klaas Wierenga, Innovatie Manager
Klaas.Wierenga@SURFnet.nl
Telefoon (030) 2 305 305

www.surfnet.nl/innovatie/wlan/

Ontwerp: Vos Ontwerp bv