Vägledning för anslutning mot eduroam

Innehåll

Introduktion

eduroam är ett samarbete mellan högskolor och universitet världen över för att underlätta nyttjandet av varandras trådlösa nätverk. En student eller anställd vars universitet är medlem i eduroam kan, med sitt användarnamn från sitt lärosäte, logga på det trådlösa nätverket på alla andra högskolor och universitet som är anslutna till eduroam.

Mottot lyder “Open your laptop and be online”.

Vem gör vad?

Precis som i annan federationsteknik skiljer man inom eduroam på IdP och SP.

Identity Provider (IdP) innebär att gör det möjligt för en skolas användare kan ansluta till eduroam i resten av världen. Autentisering sker via eduroam och skolan hanterar själv all autentisering av sina egna användare.

Service Provider (SP) innebär man öppnar upp för besökare med eduroam-konto att ansluta till Internet via skolans trådlösa nät. Skolan upplåter nätåtkomst och behöver inte känna till de enskilda användarna eftersom all autentisering av besökarna sker via eduroam. Besökarna är spårbara vid eventuella problem.

De flesta skolor som ansluter sig väljer att vara både IdP och SP, men det går också bra att bara ansluta sig som SP. Att bara ansluta sig som IdP går däremot inte för sig – man måste dela ut sina egna nätresurser om man vill få möjlighet att använda andras.

Hur fungerar det?

eduroam använder sig av RADIUS och standarden IEEE 802.1x för att förmedla information om användaren från identitetsutfärdaren (användarens hemvist) till tjänsteleverantören (lärosätet som står för det trådlösa nätverket).

Skolfederation förmedlar RADIUS-frågor mellan skolor inom Skolfederation och SUNET, som i sin tur hanterar kommunikationen med resten av världen.

eduroam Identity Provider (IdP)

För att göra det möjligt för sina egna användare att ansluta via eduroam behöver man en eduroam IdP i form av en RADIUS-server.

Denna server, som via Skolfederation tar emot autentiseringsfrågor från eduroam SP:s runt om i världen, har två huvuduppgifter – autentisering och loggning.

All autentisering sker av användarens hemmaorganisation, dvs skolan. Hur användaren autentiseras är upp till skolan och vad man bör tänka på i samband med detta beskrivs nedan. Loggning beskrivs i ett separat stycke senare i denna vägledning.

Autentisering av användare

Autentisering i eduroam sker med protokollet EAP – *Extensible Authentication Protocol*. Över det trådlösa nätet transporteras EAP över IEEE 802.1X och sedan vidare inom eduroam-infrastrukturen inneslutet i RADIUS.

EAP ger möjlighet till flera olika autentiseringsmetoder, men i praktiken används inom eduroam två metoder:

- Användarnamn & lösenord (EAP-PEAPv0/MSCHAPv2)
- Klientcertifikat (EAP-TLS)

Som de något kryptiska beteckningarna antyder bygger båda dessa metoder på TLS – *Transpoort Layer Security*. För att TLS ska fungera på ett säkert sätt måste en klient kunna autentisera den server man kommunicerar med. I fallet med EAP är servern som ska autentiseras användarens IdP, i praktiken skolans RADIUS-server. Mer information om detta hittar du under rubriken *autentisering av servrar* nedan.

Om användarna autentiseras med hjälp av **användarnamn och lösenord** kontrolleras dessa ofta mot en central katalog.

Då uppkoppling sker över många främmande accesspunkter, kan det inte uteslutas att en användare kan komma att försöka göras en uppkoppling över en “falsk” accesspunkt med namnet (SSID) eduroam. Följande frågeställningar bör därför beaktas vid användning av användarnamn och lösenord:

- Lösenord för trådlös åtkomst lagras i praktiken alltid i användarens utrustning (dator, surfplatta, telefon) och kan därför vara mer komplicerat och gärna automatiskt genererat. Detta medför i sin tur att man inte behöver ställa krav på periodiskt lösenordsbyte, något som ofta krävs i miljöer där lösenordet skrivs in manuellt flera gånger per dag.
- Beroende på hur användarens utrustning är konfigurerad (t.ex. om profiler används för konfiguration), kan det vara olika lätt för en angripare att avlyssna användarens lösenord. På grund av detta är det en fördel om lösenordet för trådlös åtkomst inte används för verksamhetskritiska system, t.ex. inloggning med *Active Directory*.
- Användarnamnet är i många fall samma som användarens epostadress. Beroende på hur användarens utrustning är konfigurerad kan detta loggas av de nätoperatörer som användaren passerar. Pseudonyma användarnamn, dvs. användarnamn som inte har en direkt (uppenbar) koppling till användaren som person kan därför vara att föredra.

Istället för användarnamn och lösenord kan **klientcertifikat** användas. I detta fall installeras ett certifikat (och tillhörande ett nyckelpar) i användarens utrustning.

Följande frågeställningar bör beaktas vid införande av klientcertifikat som autentiseringsmetod:

- Vem genererar nycklarna och hur distribuerar man ut certifikat och nycklar till användarnas utrustning första gången?
- Certifikat har en begränsad giltighetstid och behöver förnyas efter viss tid. Hur genomförs detta, och finns rutiner och metoder för att automatiskt skicka ut nya certifikat?

Användarens identitet

Alla nät som användaren besöker (eduroam SP) loggar användarens *yttre identitet* (EAP Outer Identity). Denna identitet används för att skicka vidare inloggningen till rätt IdP.

I de flesta klientprogramvaror sätts den yttre identiteten automatiskt till användarnamnet, men beroende på hur programvaran konfigureras kan det gå att sätta denna manuellt. I vissa fall (t.ex. för iOS) finns denna inställning bara tillgänglig via profilhanteraren.

Yttre identitet ska om möjligt sättas till "@" + användarens sfär (domännamn), t.ex. "@iis.se", för att de nätoperatörer man ansluter via inte ska behöva hantera information om vilken verklig identitet som anslutits. Denna information kan vid behov erhållas från IdP, som loggar själva inloggningen baserat på *inre identitet* (EAP Inner Identity).

Autentisering av servrar

Ett vanligt certifikat associerar (binder ihop) ett namn, t.ex. www.skolfederation.se, med en kryptografisk nyckel. Sådana associationer går att lita på genom att de är signerade av kända

certifikatutfärdare (CA). Motsvarande association finns inte för trådlösa nät, framför allt på grund av att datorn som kopplas upp inte har några uppgifter om vad för certifikat den ska förvänta sig från det trådlösa nätet. För att vara mer specifik – vad för certifikat datorn ska förvänta sig från RADIUS-infrastrukturen (en eller flera servrar).

För att användaren inte ska behöva hantera en säkerhetsvarning vid anslutning måste man därför fast konfigurera vilket certifikatnamn och utfärdare som ska användas för RADIUS-infrastrukturen. Detta kan göras med hjälp av konfigurationsprofiler eller genom manuell konfiguration.

Konfiguration

För många typer av klienter kan konfigurationsprofiler användas för att göra det enklare för användarna att ansluta till eduroam på ett säkert sätt.

eduroam Configuration Assistant Tool (CAT) är ett verktyg som kan användas för bygga konfigurationsprofiler. CAT stödjer i dagsläget följande operativsystem:

- Windows 8, 7, Vista, XP
- Apple iOS, OS X
- Linux

Förutom CAT finns flertalet bra andra MDM-system (*Mobile Device Management*). Ett exempel är Apple Configurator som kan tillverka konfigurationsprofiler för iOS och OS X. Dessa profiler kan sedan distribueras via webb, e-post eller direkt till enheter via kabelanslutning.

Rekommendationer

- Fundera på hur användarnas enheter ska konfigureras – görs detta av användarna själva, eller finns det någon form av centralt konfigurationsstöd?
- För att minska exponeringen av lösenord, använd separata användarnamn/lösenord (eller klientcertifikat) för autentisering av användare mot eduroam. Kräv inte att användarnas lösenord byts alltför ofta.
- För att minska exponeringen av användarnas identiteter, skicka inte användarnamnet som yttre identitet. Om detta inte är möjligt bör pseudonyma användarnamn användas istället.
- Säkerställ att användarnas enheter (klienter) kan lita på det certifikat som används för EAP. I praktiken ska certifikatnamn konfigureras fast i klienterna, och om egen certifikatutfärdare används ska alla klienter konfigureras med denna.

eduroam Service Provider (SP)

För att kunna erbjuda anslutning via eduroam behöver man erbjuda Internetåtkomst via ett trådlöst nätverk med namnet (SSID) “eduroam”.

Användare som ansluter till eduroam-nätet behöver autentiseras via en RADIUS-server, som i sin tur skickar vidare autentieringsfrågor om besökare till Skolfederation. Alla anslutningar måste också loggas, se separat stycke om detta senare i denna vägledning.

Vad menas med Internet?

eduroam ska ses som ett externt nät, motsvarande den tjänst som tillhandahålls från en ISP. Fångande portaler (*captive portal*), ibland kallad webbaserad inloggning, som används i många publika nät (*hotspots*) är inte tillåtet i eduroam -– användarna autentiseras alltid endast via 802.1x.

Trafikfiltrering får normalt sett inte tillämpas för besökande användare, men lokala användare (dvs skolans egna användare) kan få särbehandlas om så krävs. Komplett dokumentation över vad som krävs finns tillgängligt från Skolfederation.

Säkerhet

Ansluten organisation ansvarar alltid själv för att filtrera bort eventuella skadliga RADIUS attribut, t.ex. sådana attribut som används för att styra VLAN och roller i det trådlösa nätverket. Det är viktigt att inte underskatta denna risk – missar man att filtrera bort denna information kan besökare få otillbörlig åtkomst!

Loggning

All användning av eduroam loggas. Både IdP och SP förväntas kunna assistera och samarbeta vid incidenter och felsökning.

SP vet i normala fall inte vem användaren är (bara vilken sfär/domän användaren tillhör) och loggar datum och tid för anslutningen, användarens tilldelade IP-adress (IPv4/IPv6), användarens MAC-adress samt vilka åtkomstpunkter som användaren besökt. I de fall användaren har en unik pseudoym identifierare, en så kallad CUI (*Chargeable User Identity*), loggas även denna.

IdP loggar användarens identitet, datum och tid för anslutningen, användarens MAC-adress samt vilken SP som användaren besökt.

Genom att kombinera ovanstående information kan IdP och SP tillsammans lägga loggpusslet och ska förhoppningsvis kunna reda ut eventuella problem eller tveksamheter.

Programvara för RADIUS

Den som ska köra eduroam IdP eller SP behöver minst en RADIUS-server. Skolfederation rekommenderar dock alltid minst två RADIUS-servrar för att få redundans.

Det finns en uppsjö av programvara att välja mellan. Nedan listas några programvaror som visat sig fungera bra tillsammans med eduroam:

- OSC Radiator är en kommersiell RADIUS-server som används av många organisationer runt om i världen. Stöd finns för integration mot många olika datakällor och kataloger, och dokumentationen är mycket bra. Radiator har fullt stöd för RADSEC (se nedan) och fungerar på både UNIX och Windows.
- FreeRADIUS är en programvara som baseras på öppen källkod. Bra dokumentation finns, även om programvaran i många fall kan vara svår att konfigurera första gången. Fungerar i första hand på UNIX, men kan även köras på Windows.
- Cisco ACS är en traditionell Cisco-produkt som levereras med hårdvara eller som en virtuell maskin.
- Microsoft NPS ingår i Microsoft Windows Server 2012. Relativt begränsad funktionalitet jämfört med konkurrenterna.

Arbete pågår med att migrera eduroam från RADIUS-protokollet till en säkrare och mer robust kusin – RADSEC. Skolfederation har stöd för RADSEC. I praktiken innebär RADSEC att man kör det klassiska RADIUS-protokollet över TLS (*Transport Layer Security*). Än så länge är stödet för RADSEC begränsat i de flesta programvaror, med OSC Radiator som det stora undantaget. Vill man köra RADSEC till/från en server som bara har stöd för klassisk RADIUS kan man använda programvaran radsecproxy som översättare.