DIENSTBESCHRIJVING GOVROAM

Februari 2024

Bijlage 2 behorende bij Gebruiksovereenkomst

govroam is…

Community
govroam, geschreven met kleine letters, is een voorziening die Nederlandse organisaties in het openbaar bestuur (zoals gemeenten, ministeries, waterschappen, ZBO's, etc.) in staat stelt hun elektronische netwerken (zoals wifi) op confederatieve basis met elkaar te delen zodat iedereen in het openbaar bestuur overal veilig online kan gaan zonder extra kosten. Aan govroam deelnemende organisaties sluiten daartoe een overeenkomst met de Stichting government roaming Nederland ('stichting govroam'), die govroam in Nederland ontwikkelt en beheert.

Vertrouwen
govroam is een confederatie van organisaties die elkaar vertrouwen. Ze vertrouwen er op dat medewerkers van andere organisaties die bij hen op bezoek zijn, zich niet zullen misgedragen op het internet. En ook andersom: ze vertrouwen erop dat hun eigen medewerkers zich zullen gedragen als ze op bezoek zijn bij collega organisaties. Voorts vertrouwen ze er op dat een gast die zich misdraagt, wordt aangesproken door zijn of haar werkgever.

Standaardisatie
De Nederlandse govroam confederatie is gebaseerd op organisatorische en technische afspraken waar iedere govroam deelnemer mee dient in te stemmen en die beheerd worden door de Stichting govroam in overleg met de gebruikersraad.

Veilig
govroam zorgt voor veilige toegang doordat de hoogste eisen worden gesteld aan de protocollen die worden gebruikt voor authenticatie en encryptie. govroam netwerken zijn dus relatief veilige netwerken. En daarmee is govroam ook een keurmerk voor veilige netwerken.

Technische infrastructuur
govroam is een netwerk van gekoppelde RADIUS-servers die authenticatieverzoeken routeren van de gast organisatie (Service Provider) naar de organisatie waarvoor de gast werkt (Identity Provider). Daarmee is govroam ook een technische infrastructuur.

Vergelijkbaar met eduroam en toch net anders
govroam is qua technische uitvoering gelijk aan eduroam, wat reeds 10 jaar in meer dan 50 landen dagelijks door meer dan 20 miljoen gebruikers in onderwijs- en onderzoeksinstellingen wordt gebruikt. De organisatorische inrichting van govroam gebruikt die inrichting van eduroam als voorbeeld maar is aangepast aan de overheid. Zo is govroam in Nederland vooralsnog beperkt tot Nederlandse organisaties en wordt er terughoudend omgegaan met Service Providers van buiten de

overheid. Maar mogelijkheden tot internationale samenwerking met bijvoorbeeld de ons omringende landen en de internationale organisaties in Nederland, worden verkend.

1. INTRODUCTIE

1.1. INLEIDING

Dit document beschrijft op hooflijnen de technische en organisatorische aspecten van govroam. De beschrijvingen zijn in het Engels en ontleend uit de eduroam Policy Service Definition, version 2.8, 26 july 2012.
De volgende onderwerpen worden behandeld:

- Een algemeen overzicht van de voorziening inclusief de doelstelling, onderdelen en veiligheid.
- Een beschrijving van de techniek, gebruikers en werking.
- De govroam organisatie.

Het woord 'policies' wordt vaak gebruikt in dit document. De 'policies' verwijzen naar een set van technische standaarden en organisatorische regels waar aan voldaan dient te worden om deel te kunnen nemen aan govroam. De policies zijn vastgelegd in het document "govroam NL service policy".

1.2. GOVROAM IN MEER DETAIL

govroam (GOVernment ROAMing) maakt het voor werknemers van deelnemende overheidsinstellingen zoals gemeenten, provincies, ministeries, waterschappen mogelijk om op een eenvoudige en veilige wijze internet toegang te verkrijgen. De architectuur waardoor dit mogelijk is maakt gebruik van een aantal (bewezen) technologieën en onderlinge afspraken, met als resultaat: "*open je laptop en je bent online*".
Het onderliggende basisprincipe van de veiligheid van govroam is dat de authenticatie van een gebruiker uitgevoerd wordt door zijn/haar eigen organisatie, op het domein van die eigen organisatie, en via de specifieke methode van die eigen organisatie. De benodigde autorisatie om toegang te verlenen tot lokale netwerkmiddelen wordt uitgevoerd door het netwerk waar de medewerk te gast is.
De Nederlandse nationale govroam voorziening is confederatief georganiseerd. Deze organisatie houdt in dat de deelnemende organisaties een overeengekomen en samenwerkend geheel vormen. De overeenkomst omvat een set van organisatorische en technische afspraken die het eenvoudig en veilig gebruik van toegang tot internet en eventuele andere toepassingen (bijvoorbeeld printen) waarborgt. De deelnemende organisaties blijven onafhankelijk en zelfstandig verantwoordelijk voor de eigen organisatorische en technische invulling. De govroam dienst en de wijze van organiseren volgt die van govroam.
De technische invulling betreft een hiërarchisch systeem van Remote Authentication Dial-In Service (RADIUS) servers. Wanneer een gebruiker die op een gastlocatie (niet zijn eigen locatie) gebruik wil maken van internet dan zal zijn verzoek om toegang via het authentication request door de RADIUS servers doorgezet worden naar zijn thuislocatie, en het antwoord (authentication response) zal terug gestuurd worden. Iedere deelnemende organisatie zal een eigen RADIUS server inrichten en deze koppelen aan de centrale nationale RADIUS. Wanneer govroam zich zou uitbreiden naar Europa dan zal de Nederlandse nationale govroam RADIUS server gekoppeld worden aan een Europese centrale RADIUS server. govroam volgt hierin dan de hiërarchisch infrastructuur die wereldwijd voor eduroam is toegepast.

Het juist routeren van de authenticatie berichten is mogelijk omdat de gebruikersnamen een vast voorgeschreven format hebben op basis waarvan de RADIUS servers de berichten door de hiërarchie kunnen sturen. Het format van een gebruikersnaam is "user@realm" waarin realm een fully qualified domain name (FQDN). Voorbeelden van geldige gebruikersnamen in dit voorgeschreven format zijn: flip@utrecht.nl of j.r.flipkens@minvenj.nl .
Access points of switches gebruiken de IEEE 802.1X standaard met het Extensible Authentication Protocol (EAP). Instellingen bepalen zelf welke EAP-methode voor hun het beste gehanteerd kan worden. Zo is het mogelijk om via een beveiligde tunnel (bijvoorbeeld EAP-TTLS of PEAP) de authenticatie gegevens (gebruikersnaam/wachtwoorden etc) te versturen. Een andere mogelijkheid is om gebruik te maken van wederzijdse authenticatie via publieke X.509 certificaten. In al deze authenticatiemethoden wordt er gebruik gemaakt van een beveiligde tunnel (secure TLS session) vanaf het toestel van de gebruiker tot en met zijn thuis authenticatie server, zodat de persoonlijke gegevens van de gebruiker niet zichtbaar zijn voor de tussenliggende partijen.
De confederatieve govroam voorziening omvat alle mogelijkheden om een veilige dienstverlening te bewerkstelligen.

2. ONDERDELEN VAN GOVROAM

Dit hoofdstuk beschrijft de infrastructuur waar govroam uit is opgebouwd. Dit houdt onder andere in: de technische infrastructuur en de ondersteunende onderdelen, zoals monitoring, diagnose tools, de govroam website, centrale data opslag en ticketing system voor problemen.

2.1. TECHNISCHE INFRASTRUCTUUR

De confederatieve infrastructuur is gebaseerd op gedistribueerde AAA[1] servers. De huidige opzet gebruikt RADIUS voor het AAA protocol. Er zijn verschillende transport protocollen om RADIUS data pakketten te transporteren: RADIUS/UDP, RADIUS/TCP, RADIUS/DTLS en RADIUS/TLS.
govroam ondersteunt het transport over RADIUS/UDP en RADIUS/TLS en beveelt het gebruik van RADIUS/TLS aan. De routering van RADIUS berichten, onafhankelijk van de wijze van transport, gebeurt op twee manieren: een zogenaamde baseline routing model, gebaseerd op de hiërarchie van RADIUS servers, en een dynamisch routing model, gebaseerd op DNS. Het dynamische routing model wordt alleen ondersteund bij RADIUS/TLS.
De routing modellen en onderdelen van de infrastructuur worden in de volgende paragrafen in meer detail behandeld.

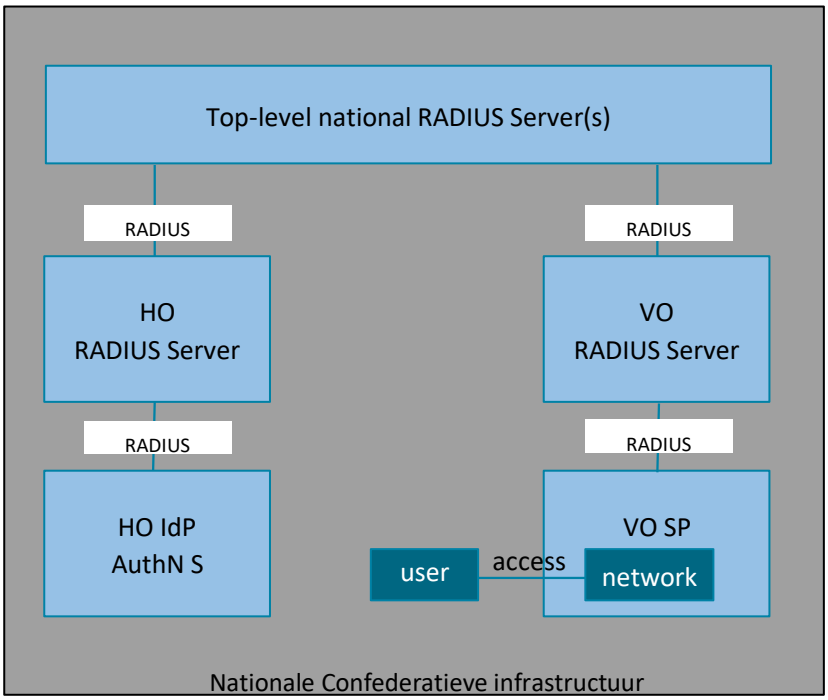
2.2. ROUTING MODELLEN

2.2.1. Baseline RADIUS Routing (Hiërarchie)

De RADIUS hiërarchie van de Nederlandse govroam confederatie bestaat uit verschillende RADIUS servers die bij de deelnemende organisatie staan. Deze zijn direct of indirect aangesloten op de nationale RADIUS proxy server. Zie figuur 2.1.

[1] Authentication, Authorization en Accounting zijn Engelse termen en worden ook wel AAA of triple-A genoemd. Een AAA wordt gebruikt om de toegang te controleren, gedefinieerde regels te hanteren en het gebruik te auditeren.

HO = Home Organisation
VO = Visited Organisation
IdP = Identity Provider
SP = Service Provider



De nationale Top-level RADIUS Server (NTLRS) van govroam verbindt de deelnemende organisaties in govroam. Deze server vindt de juiste RADIUS server van de 'thuis' organisatie (IdP) van de gebruiker, en zorgt voor een veilig transport van alle gebruikers informatie tussen de RADIUS servers. De NTLRS van govroam wordt onderhouden door de Roaming Operator, in dit geval de Stichting govroam. De stichting heeft het beheer uitbesteed aan SURF.

2.2.2. Dynamische RADIUS Routing

Bij dynamische routing maakt de govroam IdP zijn RADIUS server bekend via DNS. govroam Service Providers (SPs), die een gebruiker moeten authentiseren, vinden de juiste RADIUS server door het Domain Name System (DNS) te bevragen voor een specifiek govroam vermelding op de server.
In dit routing model is geen intermediaire RADIUS infrastructuur nodig, maar kan deze kunnen wel parallel aan elkaar werken.

2.2.3. European Top-level RADIUS Servers (ETLRS)

Momenteel is er geen centrale Europese Top-level RADIUS Server (ETLRS) omdat er geen Europese govroam confederatie is.

2.2.4. National-level RADIUS Server (NLRS)

De centrale Nederlandse govroam RADIUS server heeft een lijst met alle aangesloten IdP servers en hun *realms* (het gedeelte na de @ in een emailadres: jansen@*gemeente.nl*). Daarnaast beschikt de NLRS over een lijst met de aangesloten Service Providers (SP). Mogelijk zal deze server in de toekomst met de Europese (ETLRS) server worden verbonden.
De NTLRS ontvangt authenticatie verzoeken van de ETLRS en SPs en stuurt deze door naar de desbetreffende IdP.

2.2.5. govroam Identity Providers (IdPs)

Een govroam IdP's RADIUS server authentiseert zijn eigen gebruikers ('thuis' of als zij te gast zijn bij een andere organisatie uit de govroam community) door de credentials te checken bij het eigen Identity Management System. Het Identity Management System bevat informatie van eindgebruikers (bijvoorbeeld usernames en passwords). Het Identity Management System moet actueel worden gehouden door de Identity Provider.
Let op: de RADIUS server van de govroam Identity Provider's heeft de meest complexe taak. De meeste RADIUS servers sturen authenticatie verzoeken alleen maar door, de server van de Identity Provider's moet gebruikers ook daadwerkelijk authentiseren. Daarom moet deze geschikt zijn om EAP requests af te handelen en informatie op te vragen uit de identity management systemen.

2.2.6. govroam Service Providers (SPs)

De RADIUS server van een govroam Service Provider (SP) is verantwoordelijk voor het doorsturen van authenticatieaanvragen van gasten naar de verantwoordelijke IdP. Nadat een gebruikers is geauthentiseerd kan de RADIUS server van de SP de gebruiker in een daar voor bestemd VLAN plaatsen.
In de meeste gevallen zal een deelnemer aan govroam zowel IdP als SP zijn.

2.2.7. Network Access Elements

govroam is niet afhankelijk van toegangstechnologieën. Gebruikers van govroam kunnen toegang krijgen via draadloze en bedrade netwerken. Toegang via draadloze netwerken is uiteraard de basis van govroam.
In beide gevallen is software nodig op het apparaat waarmee de gebruiker online wil gaan, die de authenticatie verzorgt (*supplicant software*).

2.2.7.1. Supplicants

Het apparaat waarmee de eindgebruikers online wil gaan moet software (supplicant software) hebben die het IEEE 802.1x protocol ondersteunt en het EAP protocol gebruikt om authenticatie informatie te verzenden. Vrijwel altijd is deze software ingebouwd in het besturingssysteem (OS). In sommige gevallen moet er een apart programma worden geïnstalleerd.
Om govroam goed te kunnen gebruiken moet het apparaat via de instellingen van het besturingssysteem of de supplicant software, juist zijn ingesteld.

2.2.7.2. Access Points

Access points zijn alleen nodig voor draadloze toegang tot het netwerk.
Access points moeten IEEE 802.1X ondersteunen. Ze moeten ook toegangsverzoeken van een gebruiker kunnen door doorsturen naar de RADIUS van de SP die deze vervolgens doorstuurt naar de IdP, zodat de gebruiker juist geauthentiseerd kan worden. Mogelijk moeten access points ook gebruikers toewijzen aan specifieke VLANs, gebaseerd op de instructies die het AP ontvangt van de RADIUS server. Verder moeten AP's de benodigde (sleutel)informatie met het apparaat van de eindgebruiker uitwisselen zodat deze niet gehijacked kan worden en om er voor te zorgen dat de data tussen het AP en de gebruiker beveiligd wordt.

2.2.7.3. Switches

Switches worden gebruikt voor toegang tot een bedraad netwerk.

Bedrade netwerken kunnen ook geconfigureerd worden voor IEEE 802.1X. Hierdoor kunnen govroam gebruikers met hun pc of laptop toegang kunnen krijgen tot bedrade netwerken mits de switches IEEE 802.1x ondersteunen en de juiste poorten voor govroam toegang open zijn gezet. Voor een juiste authenticatie en het toewijzen van een specifiek VLAN moeten de switches een toegangsvraag van een gebruiker kunnen doorzetten naar de RADIUS server van de SP en de reactie kunnen afhandelen.

3. USERS

Dit hoofdstuk beschrijft de verschillende soorten gebruikers en de wijze waarop de govroam voorziening daarop ingericht is.

3.1. EINDGEBRUIKERS

Eindgebruikers zijn de individuele personen die govroam gebruiken om toegang te krijgen tot een netwerk. Dat netwerk is het netwerk van de eigen organisatie of dat van de organisatie waar de eindgebruiker te gast is. Gastgebruikers komen meestal niet in het eigen netwerk terecht, maar worden in een VLAN geplaatst dat enkel transparante toegang tot internet geeft.
In het algemeen zijn er twee gradaties in eindgebruikers; technologie bewust en technologie onbewust. De technologiebewuste eindgebruiker zal de govroam documentatie begrijpen en vrijwel zonder hulp in staat zijn het eigen toestel in te stellen om van govroam gebruik te maken. Andere gebruikers zullen meer assistentie nodig hebben. In termen van het huidige dienstenportfolio van govroam wordt er geen onderscheid gemaakt tussen deze gebruikers.

3.2. ADMINISTRATIEF PERSONEEL

Beheerders zijn de gebruikers die delen van de govroam voorziening beheren. Er wordt onderscheid gemaakt in beheerders op nationaal niveau en op organisatie niveau.

3.2.1. Beheer op nationaal niveau

Een klein aantal beheerders kan de nationale govroam servers beheren. Van belang is dat deze beheerders veel kennis van de RADIUS server en technologie hebben. Gezien het beperkte beheer en de vereiste kennis, zal in ieder geval voor de aanvangsperiode met de beheerders van eduroam (samen-)gewerkt worden.

3.2.2. Beheer op organisatie niveau

Op het niveau, en ook het domein, van de deelnemende organisaties dient eveneens beheer plaats te vinden. Het beheer op het niveau van een deelnemende organisatie verschilt aanzienlijk van dat op nationaal niveau. Beheerders van deelnemende organisaties moeten de onderdelen die zorgen voor de authenticatie en identity management systemen, configureren en de correcte werking waarborgen. Iedere organisatie bepaalt zelf met welke apparatuur en op welke wijze deze de infrastructuur inricht. Gegeven de vele mogelijkheden tot invulling, is het voor de stichting govroam niet mogelijk en voor deelnemende organisaties niet wenselijk, om voor iedere wijze van implementatie uitputtende documentatie te verzorgen van hoe deze geconfigureerd dient te worden.