publicroam
#OveralVeiligWifi

TECHNISCHE SPECIFICATIES

Dit document beschrijft de technische specificaties waaraan organisaties die publicroam gebruiken voor het bieden van toegang tot hun wifi-gastnetwerk, moeten voldoen.

1. Definities

1.1 **Aanbieder:** Publicroam B.V.
1.2 **Afnemer:** organisatie die gebruik maakt van de Dienst
1.3 **Dienst:** de authenticatiedienst 'publicroam' waarmee Afnemer de toegang tot zijn gastnetwerk veiliger en gebruiksvriendelijker kan maken.
1.4 **Publicroam-RADIUS:** de centrale RADIUS proxy server van de Dienst.

2. Technische specificaties

Afnemers moeten voldoen aan de volgende technische specificaties:

1. De netwerken van Afnemers moeten 802.1X implementeren met een RADIUS interface om te verbinden aan de Publicroam-RADIUS (minimaal 802.11b en/of 802.11g).
2. Afnemers worden aangemoedigd ongefilterde en onbeperkte internet toegang te bieden. Echter, zij moeten minimaal de mogelijkheid bieden om het web te raadplegen, e-mail te ontvangen en te verzenden, en SSH te gebruiken (bijvoorbeeld uitgaande TCP-poorten 22, 80, 110, 143, 443, 465, 587, 993, and 995). Verder moet het gebruik van reguliere VPNs ondersteund worden waar mogelijk.
3. Als een Afnemer de toegang tot internet filtert (firewall), beperkt (shape, limit bandwidth, etc.) of monitort (loging, intercept, etc.), dan houdt de betreffende Afnemer zich aan de wettelijke regels hieromtrent.
4. Afnemers moeten alle Extensible Authentication Protocol (EAP) berichten routeren naar de Publicroam-RADIUS en mogen zulke berichten niet aanpassen bij overdracht.
5. Afnemers mogen publicroam alleen aanbieden via draadloze netwerken.
6. De draadloze netwerken van Afnemer moet de SSID "publicroam" uitzenden — let op: dit is hooflettergevoelig, het dient geschreven te worden met kleine letters.
7. De netwerken van een Afnemer moeten een IP-adres en DNS-configuratie voor automatische configuratie-infrastructuur bieden.
8. Afnemers moeten routeerbare IP-adressen bieden en mogen Network Address Translation (NAT) bieden.
9. Draadloze netwerken van Afnemer moeten WPA2+AES ondersteunen, en mogen aanvullend WPA/TKIP ondersteunen.
10. Afnemers wordt geadviseerd VLAN-scheiding toe te passen
11. Afnemers moeten de voldoende technische gebruiksgegevens leveren aan Aanbieder om in staat te zijn om een apparaat te authentiseren, minimaal:
    - timestamp of authenticatie-requests en corresponderende responses
    - de outer EAP identity in het authenticatie-request (User-Name attribute)
    - het MAC address van de connecting client (Calling-Station-Id attribute)
    - type van de authenticatie-response (i.e. Accept or Reject)
    - informatie over de relatie tussen het layer 2 (MAC) address van de client en het layer 3 (IP) adres dat is verstrekt na login (bijvoorbeeld, ARP sniffing logs or DHCP logs)
12. Afnemer bewaart technische gebruiksgegevens maximaal drie maanden na het beëindigen van de verbinding met het WiFi-gastnetwerk, tenzij de gegevens langer bewaard moeten worden om misbruik tegen te gaan, of wanneer er een wettelijk verplichting is om deze gegevens langer te bewaren. In het geval dat de gegevens langer bewaard moeten worden om misbruik tegen te gaan, worden de gegevens zo lang bewaard als nodig is om tegen het gesignaleerde misbruik op te treden.
13. Klokken die gebruikt worden voor de timestamps moeten gesynchroniseerd worden via het Network Time Protocol (NTP; SNTP) of alternatieven die acceptabel zijn voor de Aanbieder

Afnemer is zelfstandig verantwoordelijk voor een goede beveiliging van haar eigen ICT-netwerken en-applicaties