

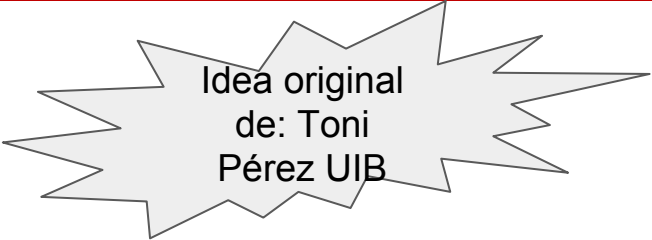
# edurogue vs eduroam CAT Universidad de Salamanca

José Manuel Agudo - [jagudo@usal.es](mailto:jagudo@usal.es)



VNIVERSIDAD  
DSALAMANCA  
1218 - 2018

# edurogue vs eduroam CAT



Idea original  
de: Toni  
Pérez UIB

- Objetivos:
  - Detectar y corregir los usuarios de eduroam configurados de forma insegura.
- Solución propuesta:
  - Establecer la identidad externa / anónima de las conexiones en los instaladores de la herramienta eduroam CAT con el siguiente formato:  
“**cat.<fecha\_instalador>@usal.es**”
  - Verificar en el RADIUS la identidad externa de la siguiente forma:
    - outer-identity = [cat.20170714@usal.es](mailto:cat.20170714@usal.es)
      - El dispositivo está configurado con la última versión de eduroam CAT
      - Acceso normal a la red
    - outer-identity = \*
      - El dispositivo no ha sido configurado por eduroam CAT
      - Redirigimos a un portal cautivo informando al usuario y dando acceso a eduroam CAT

# Cisco WLC - Configuración (I)

**WLANs**

MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'eduroam'

General Security **QoS** Policy-Mapping Advanced

Layer 2 Layer 3 **AAA Servers**

Layer 3 Security Web Policy ▾

- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- On MAC Filter failure<sup>10</sup>

Preauthentication ACL IPv4 None ▾ IPv6 None ▾ WebAuth FlexAcl None ▾

**VPN Pass-Through**

VPN Gateway Address 0.0.0.0

# Cisco WLC - Configuración (II)



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

## Security

### AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
  - DNS
  - Downloaded AVP
- TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
  - Access Control Lists
  - CPU Access Control Lists
  - FlexConnect ACLs
  - Layer2 ACLs
  - URL ACLs

## Access Control Lists > Edit

### General

Access List Name bad-eduroam

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
<a href="#">1</a>	Permit	0.0.0.0 / 0.0.0.0	212.128.130.10 / 255.255.255.254	Any	Any	Any	Any	Inbound	0
<a href="#">2</a>	Permit	0.0.0.0 / 0.0.0.0	212.128.130.140 / 255.255.255.254	UDP	Any	DNS	Any	Inbound	0
<a href="#">3</a>	Permit	0.0.0.0 / 0.0.0.0	212.128.129.69 / 255.255.255.255	TCP	Any	HTTP	Any	Inbound	0
<a href="#">4</a>	Permit	0.0.0.0 / 0.0.0.0	145.100.191.84 / 255.255.255.255	TCP	Any	HTTP	Any	Inbound	0
<a href="#">5</a>	Permit	0.0.0.0 / 0.0.0.0	145.100.191.84 / 255.255.255.255	TCP	Any	HTTPS	Any	Inbound	0
<a href="#">6</a>	Permit	212.128.130.10 / 255.255.255.254	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
<a href="#">7</a>	Permit	212.128.130.140 / 255.255.255.254	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	0
<a href="#">8</a>	Permit	212.128.129.69 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	0
<a href="#">9</a>	Permit	145.100.191.84 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	0
<a href="#">10</a>	Permit	145.100.191.84 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any	Any	Outbound	0
<a href="#">11</a>	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0



# FreeRADIUS - Configuración

- Configurar en el site externo:

```
# Usuarios no configurados con cat.eduroam.org - Redirect
if (Realm == "usal.es" && User-Name != "cat.20170714@usal.es") {
    update reply {
        Cisco-AVPair := "url-redirect=http://lazarillo.usal.es/node/521"
        Cisco-AVPair := "url-redirect-acl=bad-eduroam"
    }
}
```