# USO Y DESPLIEGUE DE TAILSCALE EN IRAM

## Creación de una Red Superpuesta de Malla

William Robertson II (wroberts@iram.es)

tailscale

iram
Institut de
Radioastronomie
Millimétrique

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

red.es

RedIRIS

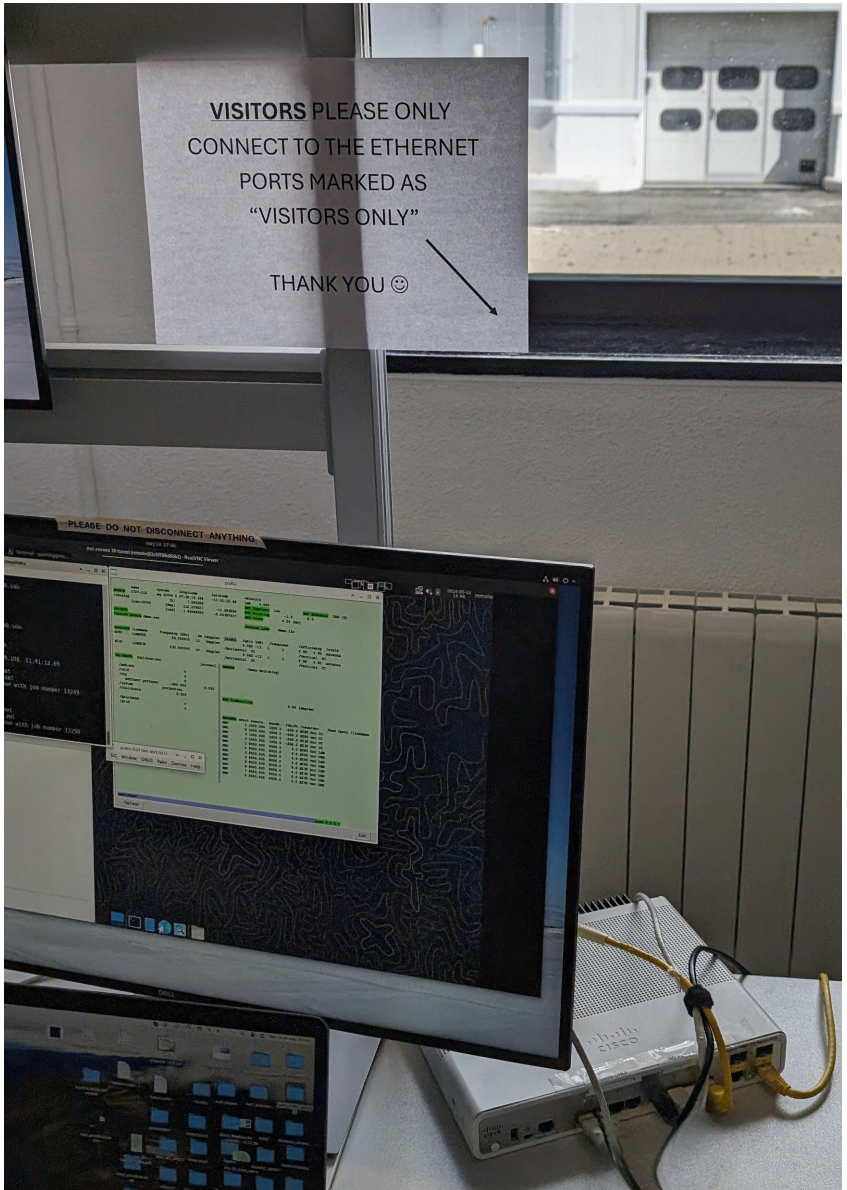
# Motivación

# Nuestro Caso de Uso

- Situación actual: Servidor de OpenVPN autenticando contra LDAP via plugin
  - Sin **MFA** (autenticación con múltiples factores)
  - **AAA** (Autenticación, Autorización, Contabilidad) muy limitada
  - **Rendimiento** bastante bajo (especialmente en clientes)
  - Estrategia de defensa: **castillo y foso**
    - “Exterior crujiente, interior blandito” – Cheswick, 1990
- Cambiarlo a algo **más moderno**

# Más Allá de una VPN

- Mover el problema de confianza en la red a los dispositivos (**Device Trust**)
- Todo esto es primordial en el caso de IRAM 30m:
  - Observadores semanales
  - Dispositivos no conocidos
  - No es posible controlar acceso de forma robusta y granular en la sala de control


VISITORS PLEASE ONLY
CONNECT TO THE ETHERNET
PORTS MARKED AS
“VISITORS ONLY”
THANK YOU ☺
PLEASE DO NOT DISCONNECT ANYTHING

# Contexto

- ALMA: octubre, 2022
- NSF: agosto, 2023
- JCMT: octubre, 2023
- ESO: mayo, 2024 (!!)
- IRAM: ???

# Proceso de Selección

# ~~Requisitos~~ Lista de Deseos

- MFA fuerte
- AAA/registros
- UX refinada
- “Soberanía”/control de datos
- Encriptación moderna

- RBAC (control de acceso basado en roles)
- Rendimiento (servidor y cliente)

# Soluciones Propuestas

- Wireguard “vainilla”
- Nebula
- Tailscale
- Headscale
- ZeroTier

| | MFA | AAA | UX | Control | Modernidad | RBAC | Rendimiento |
|---|---|---|---|---|---|---|---|
| **OpenVPN** | NO | DIFÍCIL | ACEPTABLE | COMPLETO | NO | NO | MEDIO |
| **Wireguard** | NO | DIFÍCIL | DIFÍCIL | COMPLETO | SÍ | NO | ALTO |
| **Nebula** | NO | SÍ* | ACEPTABLE | COMPLETO | SÍ | SÍ | ALTO |
| **Tailscale** | SÍ | SÍ | MUY BUENA | HÍBRIDO | SÍ | SÍ | ALTO |
| **Headscale** | NO | SÍ | DIFÍCIL | COMPLETO | SÍ | SÍ | ALTO** |
| **ZeroTier** | SÍ | SÍ | BUENA | HÍBRIDO | SÍ*** | SÍ | ALTO |

# Selección Final: Tailscale

- Satisface todos los requisitos
- Gestión de DNS fácil (vs. ZeroNSD)
- Criptografía más “estándar” que ZeroTier
  - Wireguard (Noise) vs. NaCl, ZT no tiene **PFS**
- Documentación para usuario final más “accesible”

# Servicios Requisitos y Despliegue

# Servicio de Autenticación

- Tailscale no quiere ofrecer autenticación:
  - Necesitamos proveedor de OIDC (que no teníamos)
  - Opciones: GSuite, M365, etc. o **proveedor propio**
    - Eligimos Authelia con conexión a nuestro LDAP
      - **Fácil** de desplegar con Podman
      - Solución **minimalista**
      - **Mantener control** de la fuente de autenticación/autorización

# Retos y Soluciones en el Despliegue

- Muchos servidores que necesitarán el agente
  - Ansible
- Varios sistemas sin posibilidad de instalar agente
  - Subnet Routers (modelo antiguo de VPN)
- Registros de conexiones
  - GrayLog con Grok Patterns
  - Network Flow Logging es un botón en la consola web

# Retos y Soluciones cont.

- Tailscale dispone IPs distintas
- No romper enlaces antiguos, favoritos de navegador, etc
  - “MagicDNS” == nuevo dominio, no era adecuado
  - Tailscale puede reconfigurar DNS del sistema
  - Implementamos **vistas en BIND**
    - IP fuente de Tailscale == respuesta con IP Tailscale
    - IP fuente “normal” == respuesta con IP “normal” (antigua)

# Filosofía de “Nube Híbrida”

- Tailscale utiliza servidores relays (nombrados “DERP”) para negociar conexiones (cifradas) entre nodos
- También dispone de la posibilidad desplegar y usar servidores **DERP custom**
  - IRAM actualmente usamos dos servidores DERP propios:
    - Observatorio Pico Veleta (MRT)
    - Oficinas en Granada ciudad (GRA)
    - Despliegue automatizado con Ansible y Docker

# Conclusiones y Próximos Pasos

# Incorporación de Usuarios

- Nuestros usuarios han tenido experiencias positivas dándose de alta (casi) sin ayuda
  - Documentación en línea de Tailscale
  - 400 palabras de información extra para darse de alta en nuestro sistema de OIDC (Authelia)
- Pocas solicitudes de soporte == caso de éxito

# Especificación de ACLs

- Menos flexibles, más sencillas que cortafuegos
- Cambios ~inmediatos en los nodos

```
{
    "action": "accept",
    "src":    ["tag:mysqlclient"],
    "proto":  "tcp",
    "dst":    ["tag:mysqlserver:3306"],
}, // MySQL clients can see their servers
{
    "action": "accept",
    "src":    ["tag:postgresclient"],
    "proto":  "tcp",
    "dst":    ["tag:postgresserver:5432"],
}, // PostgreSQL clients see their servers
{
    "action": "accept",
    "src":    ["autogroup:member", "tag:server"],
    "proto":  "tcp",
    "dst":    ["tag:restic:8000"],
}, // Allow all users/servers to send data to restic repositories
```

# Trabajo en el Futuro Próximo

- Aplicar principios de **IaC/GitOps** al desarrollo de ACLs
- Mejorar la **monitorización** de servidores DERP (usando `derpprobe` y Zabbix)
- Endurecer la seguridad del agente usando systemd y SELinux