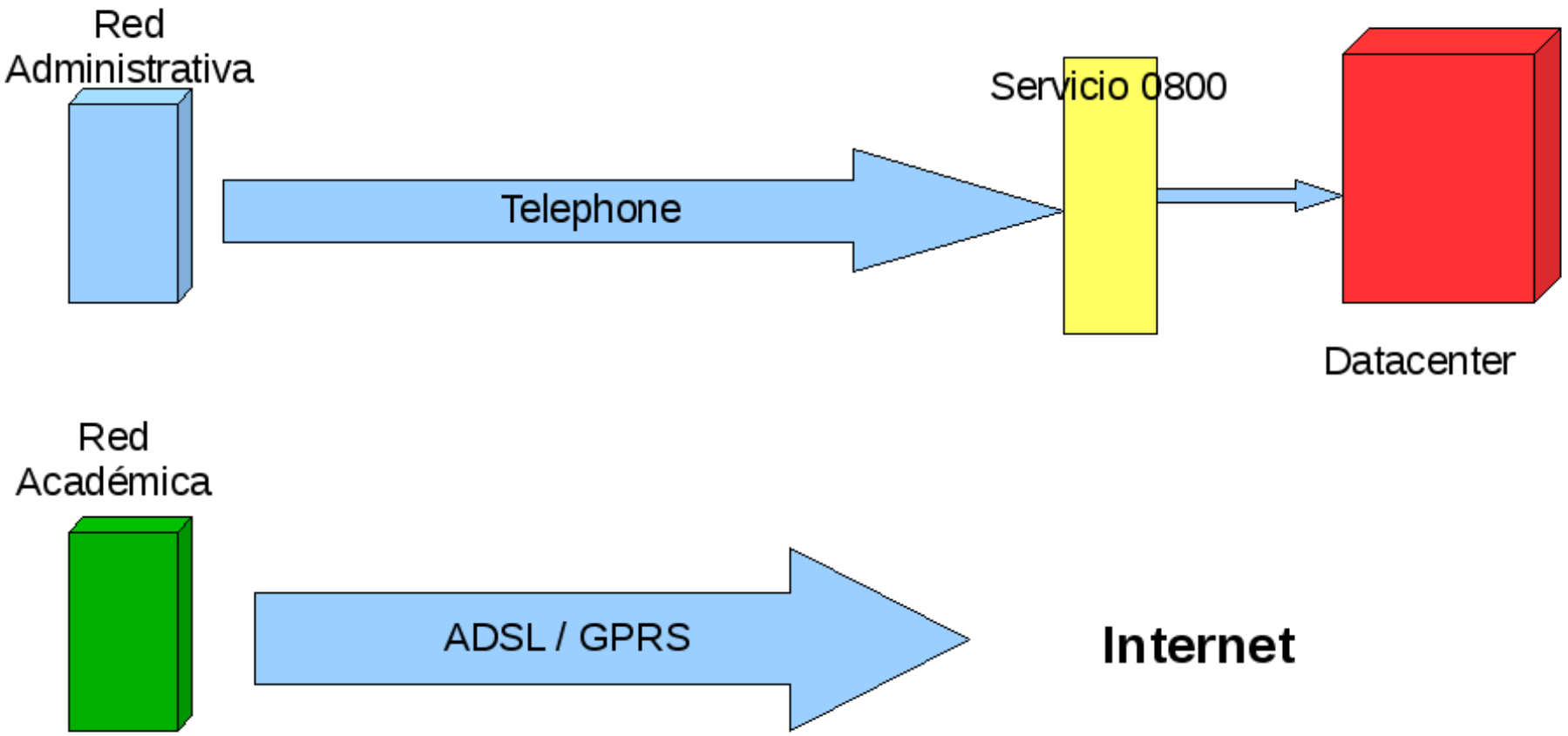
Keeping 200 firewalls on track

Ing. Ernesto Silva
A/PEnrique Verdes

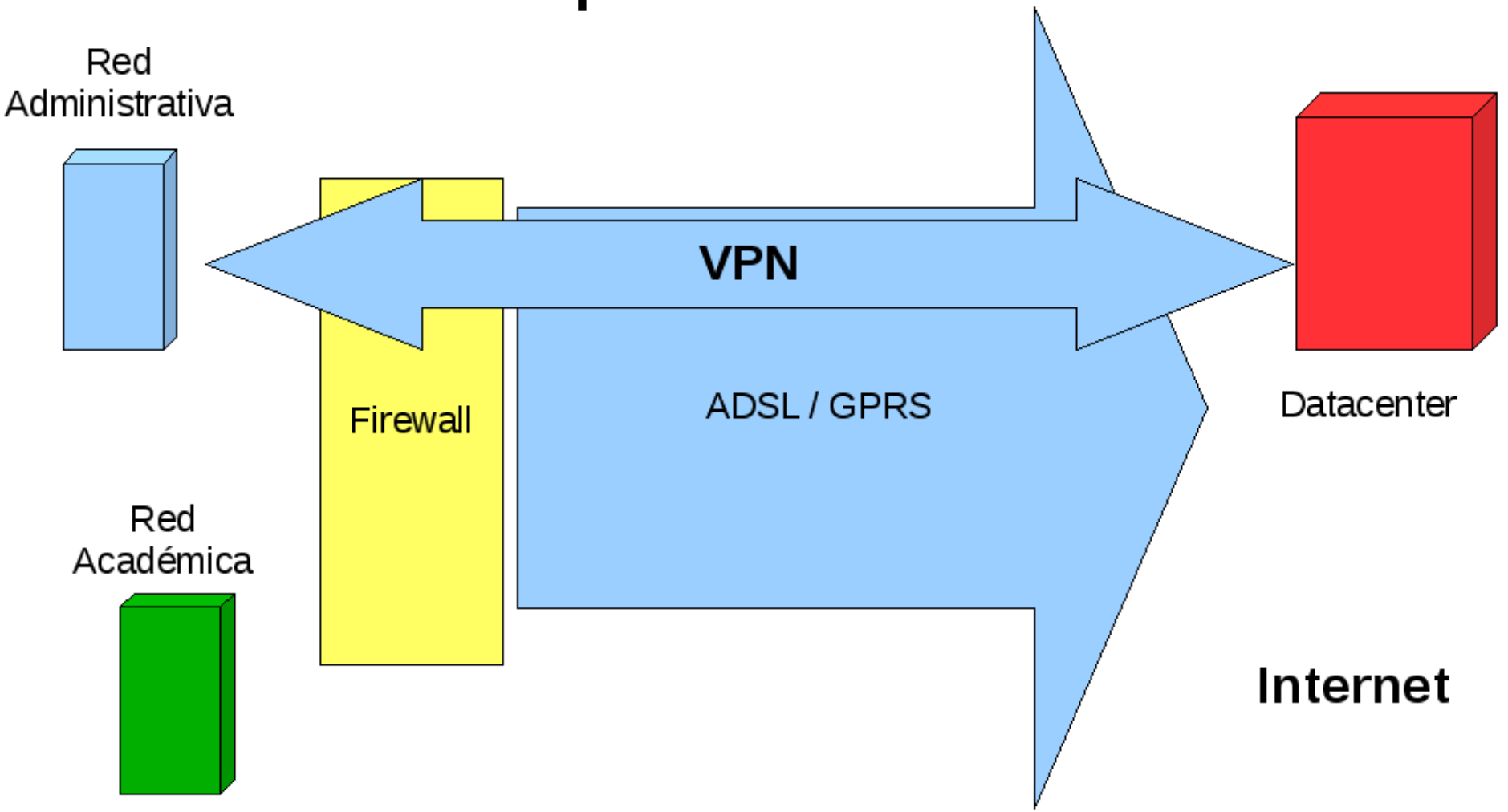
Donde

- Consejo de Educación Secundaria de Uruguay
- 270 liceos en todo el pais. 220 con conexión a Internet (ADSL y GPRS)
- Centro de cómputos:
  - 9 técnicos de soporte nivel 1 con formación muy heterogenea.
  - 2 técnicos de soporte de nivel 2.
- Soporte regional
  - Solo técnicos en hardware.
- Soporte on-site
  - 1 ó 2 por centro de estudios (docentes de informática)

Que tenemos


Red
Administrativa
Telephone
Servicio 0800
Datacenter
Red
Académica
ADSL / GPRS
Internet

Que queremos tener



Metas

- ADSLs de 512 Kbps mínimo en todos los centros y EDGE para centros en áreas rurales.
- Una sola vía de comunicación (Internet).
- VPN para comunicación de datos administrativos.
- Administración centralizada de la infraestructura.

El Firewall

- Hardware:
  - Pentium IV 1,6 Ghz. 256MB RAM recertificados, sin disco, con almacenamiento USB de 2GB.
- Software:
  - IPCop: Actualizaciones de software, buena interfase web y VPN. Solución “llave en mano”. Documentación para instalar en pendrive.Interfase para plugins.
  - Otras alternativas evaluadas no reunian las características deseadas.(Ej. FWBuilder, DevilLinux, ZeroShell)

Mantenimiento y Gerenciamiento.

- Capacidad limitada de almacenamiento en appliances:
  - Servidor central de logs y proxy deshabilitado para evitar desgaste de pendrive USB.
- Ancho de banda limitado (64 Kbps de subida).
- Mantenimiento centralizado de configuración.
- Monitoreo centralizado. No hay técnicos con capacidad para soporte y solución de problemas on-site.

Gestión de logs.

- Los logs son mantenidos en memoria y enviados diariamente al servidor de gerenciamiento en el DataCenter.
- Los eventos críticos son monitoreados en tiempo real en un servidor de logs central.
- El objetivo es evitar o minimizar la escritura en el pendrive USB, sin perder funcionalidad.

Mantenimiento centralizado de configuración

- Debido a la cantidad de equipos debe ser posible realizar cambios masivos en forma automática.
- Se evalúa el uso de cfengine o puppet.
- También podría desarrollarse un script basado en *rsync* y *ssh* que se adapte a las características del software utilizado.

Monitoreo centralizado

- Debido a la falta de personal técnico es necesario que el personal de administración pueda conocer el estado de las conexiones para actuar más proactivamente y asegurar el servicio.
  - Pandora FNMS ofrece capacidad de autoconfiguración, monitoreo (activo y pasivo) y alertas.
  - *swatch* complementa las herramientas de monitoreo con análisis de logs y generación de alertas.

Estado actual del proyecto

- Los firewalls ya son funcionales.
- Estamos resolviendo las cuestiones de monitoreo y gerenciamiento.
- Limitaciones de presupuesto, personal y burocracia han retrasado la puesta en marcha del proyecto.

Preguntas

test -z $PREGUNTAS && echo “Muito Obrigado”