UNITRONICS

I Jornadas de Arquitecturas de Red Seguras en las Universidades

Universidad Pablo Olavide de Sevilla

4 – 5 Marzo de 2003

Israel García Yagüe
igy@unitronics.es

UNITRONICS
COMUNICACIONES

UNITRONICS

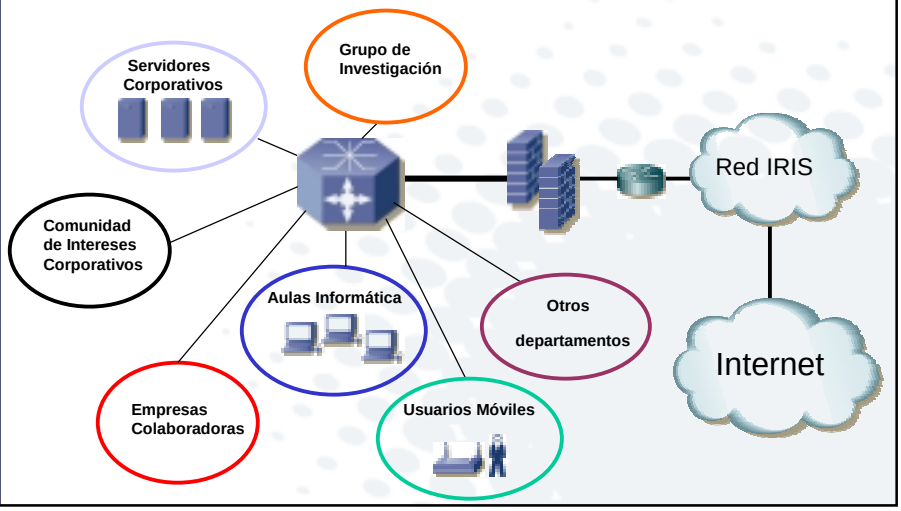
Agenda

- Firewall´s
- Seguridad, Aceleración y Distribución de Contenidos
- Aplicaciones P2P, Mensajería Instantánea
- Antivirus
- Detección de Intrusión
- Acceso Remoto usuarios
- Seguridad en Redes Wireless
- Seguridad en Telefonía IP y Videoconferencia
- Autentificación
- Gestión Centralizada de log´s

UNITRONICS

Escenario de red Universitario

➢ **Grupos de usuarios con distintas políticas de seguridad:** alumnos, grupos de investigación, etc...



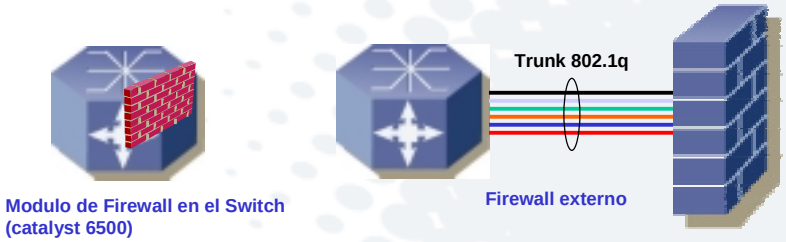
UNITRONICS

Firewall

Grupos de Usuarios con distintas Políticas de Seguridad

- **Firewall con soporte 802.1q**
  - ➢ Firewall entre distintas Vlan´s
  - ➢ Política de Seguridad Flexible
  - ➢ Alto rendimiento

Soluciones:



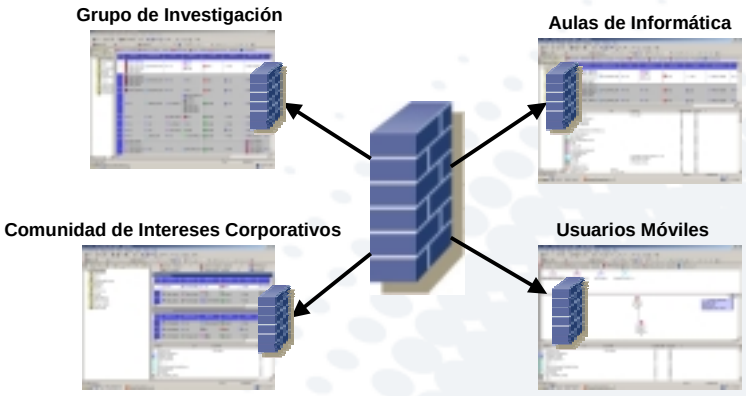
Modulo de Firewall en el Switch (catalyst 6500)

Firewall externo

Firewall

Grupos de Usuarios con distintas Políticas de Seguridad

- Firewall Virtuales: un Firewall físico, múltiples Firewall lógicos con gestión y administración independientes



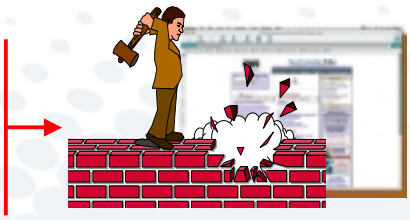
Ampliar la funcionalidades del Firewall a los diferentes grupos de la Universidad

Firewall

Seguridad en los Servidores Web

Existen ciertos tipos de ataques que se saltan la seguridad de los Firewall, aprovechando vulnerabilidades del servidor web o de las aplicaciones:

buffer overflow, manipulación de campos ocultos, alteración de cookies, malformación de url y campos de entrada, cgi, etc..



Es necesario definir otro tipo de protección:

Firewall de aplicación. Establece protección a nivel de aplicación para los servidores web, neutralizando los intentos de intrusión.

Aconsejable su instalación en servidores Web públicos

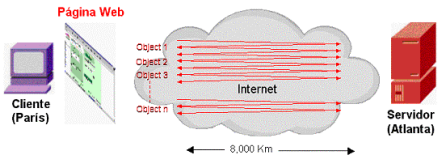
Seguridad, Aceleración y Distribución de Contenidos

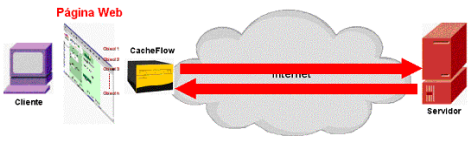
- Caché
- Seguridad
- Aceleración
- Distribución

→ Contenido

Cache de Contenidos

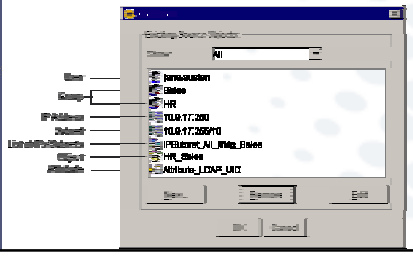
- **CacheOS**
  - Código optimizado
  - Diseño robusto
  - Escalabilidad
- **Caché de contenidos**
  - Object Pipeline
  - Adaptative Refresh

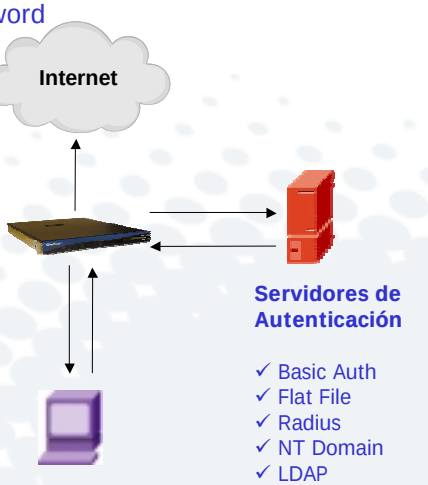




Autenticación, Identificación de usuarios

- Por nombre de usuario + password
- Grupo de usuarios
- Dirección IP, Subred origen
- Por Cookies entregadas por el Security Gateway, duraderas por sesión o TTL configurable



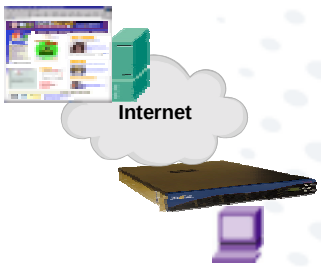


Servidores de Autenticación

- ✓ Basic Auth
- ✓ Flat File
- ✓ Radius
- ✓ NT Domain
- ✓ LDAP
- ✓ Active Directory

Seguridad de Contenido

- **Criterios de Filtrado:**
  - ✓Client IP address
  - ✓Client Subnet
  - ✓Destination Port
  - ✓Domain
  - ✓Protocol
  - ✓URL
  - ✓Wild Card URL
  - ✓User Group
  - ✓User Name
  - ✓Time of the day
  - ✓Day
  - ✓MIME type



- **Políticas:**
  - ✓Allow/Deny
  - ✓Authenticate or no authentication
  - ✓Cache
  - ✓Rewrite URL
  - ✓Rewrite HTTP header
  - ✓Strip ActiveX and Java applications and scripts
- **Control Parental:**

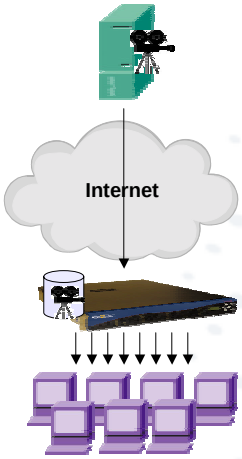
SECURE COMPUTING WEBSENSE

- **Inspección Antivirus ICAP:**

TREND MICRO

Entrega de contenidos multimedia

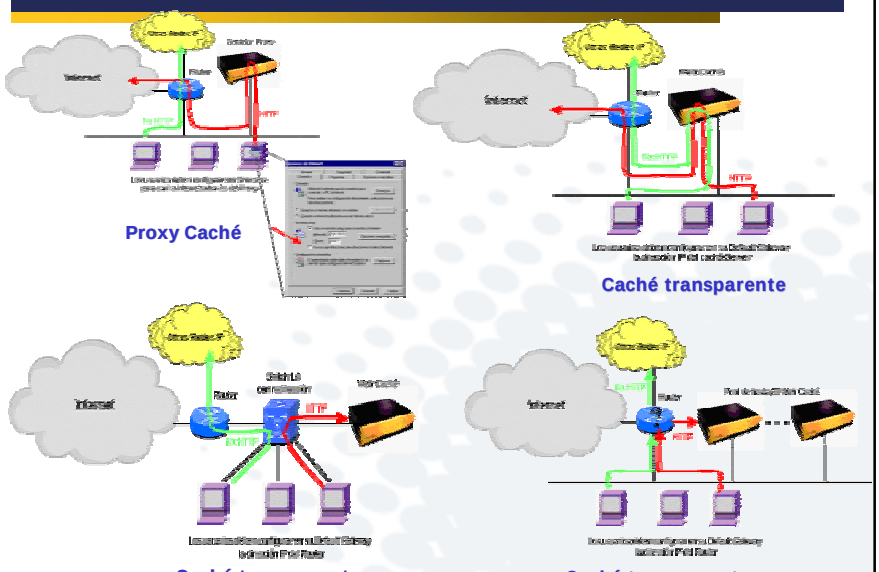
• Entrega de Contenidos multimedia en tiempo real o pregrabados



Capacidades:

- ✓Autenticación
- ✓Caching del contenido
- ✓Spliting de una emisión
- ✓Traslación multicast-unicast
- ✓Traslación unicast-multicast
- ✓Controlar el ancho de banda del flujo multimedia:
  - Windows Media
  - Real Server

Modos de Operación



UNITRONICS

Antivirus e Inspeccion de Contenido

Estrategia de defensa en capas

- **Estrategia de defensa en capas:**
  - Antivirus en el perímetro de Internet
  - Antivirus en los servidores de correo
  - Antivirus en los servidores de ficheros, aplicaciones
  - Antivirus en el puesto de trabajo

- **Gestión centralizada**
- **Diferentes motores de análisis**
  - Dos mejor que uno

UNITRONICS

P2P, Mensajería Instantánea, etc..

➢ Nuevas fuentes de propagación de virus, gusanos, troyanos, etc...

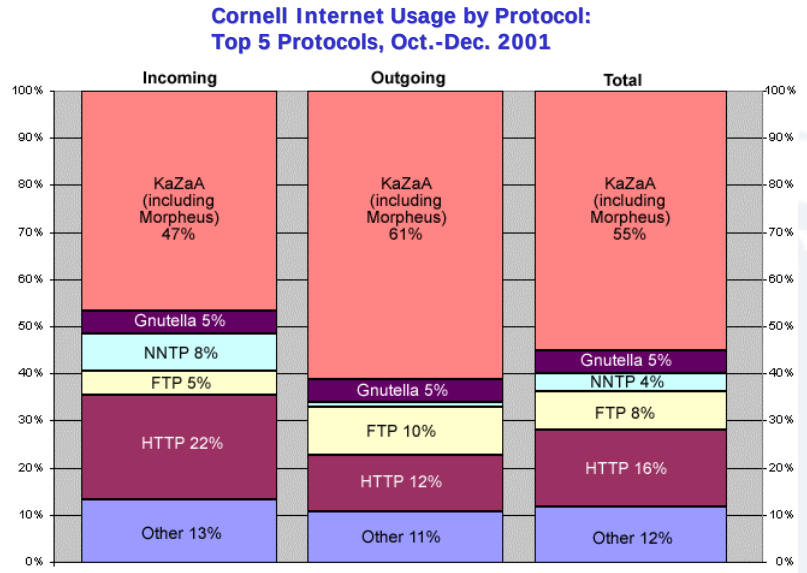
- **Mensajería Instantánea**
- **Aplicaciones P2P**

Otros problemas:

- Aspectos legales (servidor con mp3, mpeg, etc..)
- Consumo de ancho de banda

UNITRONICS

Consumo de ancho de banda



UNITRONICS

Medidas para afrontar estos problemas

- **Establecer filtros en el Firewall perimetral**
  - Filtrar Puertos
  - Filtrar las direcciones IP de los servidores

Solución poco eficaz:

1. **Puertos de las aplicaciones variables**
2. **Complejidad filtrado de los servidores P2P.**

- **Herramienta de análisis y gestión de trafico**

Packeteer Packetshaper

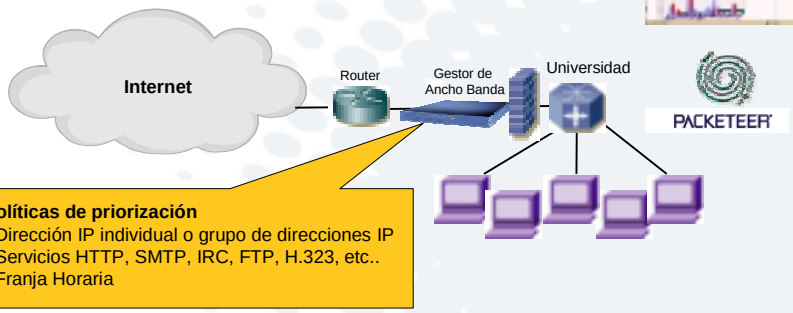
PACKETEER

Análisis y Gestión de Trafico

➢ Permiten establecer un política de gestión de ancho de banda:

- Priorización por IP ó grupos de IP, usuario, servicios (http, smtp, ftp, etc..), franja horaria, etc..

- Características de monitorización y reporting que ofrecen información estadística en tiempo real, permitiendo conocer en detalle el uso de nuestra conexión WAN/Internet



Políticas de priorización
- Dirección IP individual o grupo de direcciones IP
- Servicios HTTP, SMTP, IRC, FTP, H.323, etc..
- Franja Horaria

Análisis y Gestión de Trafico

➢ Actúan como un “sniffer” , analiza el trafico, identificando las aplicaciones, no importa que cambien de puerto:

- Facilita el control de las aplicaciones P2P, mensajería instantánea, etc..

UNITRONICS

Detectores de Intrusión

➢ Consideraciones a tener en cuenta

- ✓ Falsos Positivos / negativos.
- ✓ Actualización de Patrones
- ✓ Gestión y Administración de alarmas y eventos.
- ✓ Actuación frente a los ataques.
- ✓ Diferentes tecnologías (snort, ISS, Cisco, Dragon)
- ✓ Ubicación de los Agentes Detectores.

UNITRONICS

Estrategia de implantación

Detectores de Intrusión

- Núcleo de red de la Universidad
  - Soluciones IDS integradas en el switch (Catalyst 6500)

- Soluciones IDS network sensor
  - -Situación en segmentos de red estratégicos:
    - **Detrás de los Firewall**
    - **DMZ**
    - **etc...**

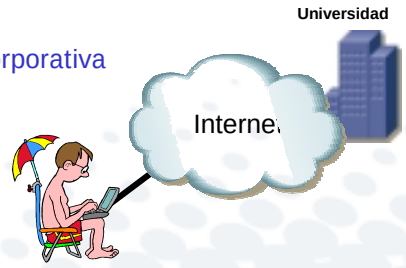
- Servidores críticos
  - IDS basado en host: ISS, Dragon, Cisco
  - Integridad de Archivos: Tripware, ASET

- Switches de nivel 7 (con capacidad IDS)
  - Capacidad de protección servidores

UNITRONICS

Acceso Remoto de Usuarios

Acceso Remoto



- Usuarios Comunidad Interés Corporativa
- Empresas Colaboradoras
- Grupos de Investigación
- Docencia
- Etc…

Aspectos a tener en cuenta:

- ✓ Utilización Internet
- ✓ Autentificación
- ✓ Firewall
- ✓ Antivirus
- ✓ **¿SSL ó IPSEC?**

UNITRONICS

Acceso Remoto usuarios

IPSEC ó SSL

➢ SSL / TLS

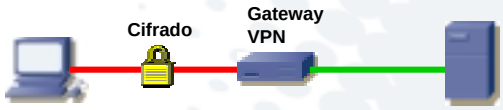
- Integrado en el navegador web (Explorer, Netscape) y aplicaciones de correo (Outlook y Eudora) que incluyen ESMPT o smtp sobre ssl.
- **Solo soporta aplicaciones web o e-mail**
- Fácil de usar, transparente al usuario
- Cifrado entre el cliente y el recurso
- Rendimiento, puede llegar a producir un uso intensivo de CPU

Acceso Remoto usuarios

IPSEC ó SSL

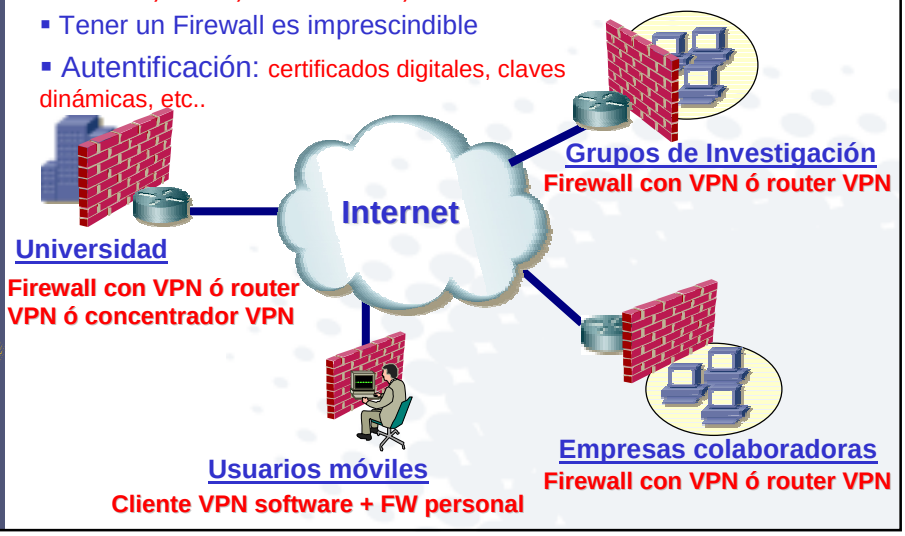
➢ IPSEC

- Necesidad de instalar software o equipamiento, en la red de la universidad (concentradores VPN, Firewall VPN, router VPN, etc..).
- Instalar software cliente (compatibilidad SO, no transparente para los usuarios, etc...)
- **Soporta cualquier servicio IP**
- Cifrado entre el cliente y el gateway VPN



Acceso Remoto usuarios con VPN IPSEC

- Diferentes dispositivos para crear VPN:
  Firewall, router, concentrador, software
- Tener un Firewall es imprescindible
- Autentificación: certificados digitales, claves dinámicas, etc..

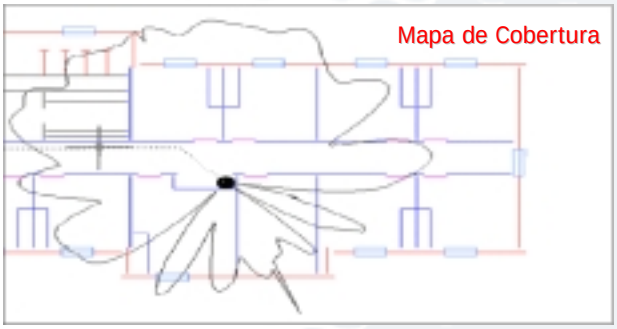


UNITRONICS

Aulas con redes Wireless

Consideraciones: Seguridad Física

- Determinar mapas de cobertura
- Utilizar antenas específicas y adecuadas para la zona a cubrir.
  - Antenas direccional y omnidireccional producen cobertura diferente
- Ajustar la potencia transmitida, en función del medio (obstáculos) y la distancia.



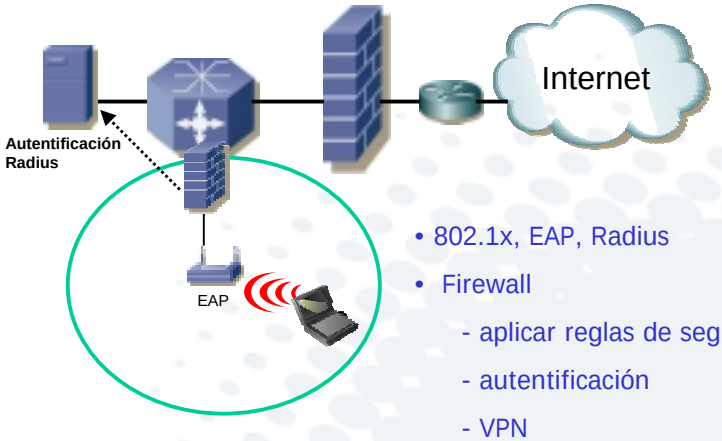
UNITRONICS

Aulas con redes Wireless

Consideraciones: Seguridad Lógica

- **Los elementos de seguridad propuestos en el estándar 802.11b, han demostrado ser insuficientes:**
  - ✓ **WEP.** Claves (airsnort)
  - ✓ **SSID.** Broadcast de los AP, SSID por defecto (tsunami, 101, WaveLan Network). Utilizado como medio para segmentar las redes y no como método de autentificación y control de acceso.
  - ✓ **Filtros MAC.** Las direcciones MAC aparecen en la claro en la cabecera de la trama. La mayoría de las tarjetas WLAN permiten cambiar su dirección MAC.
- **Necesidad de Utilización 802.1x, EAP Radius**
- **Interoperabilidad**

Aulas con redes Wireless



- 802.1x, EAP, Radius
- Firewall
  - aplicar reglas de seguridad
  - autentificación
  - VPN

Seguridad en Telefonía IP y Videoconferencia
Riesgos y Aspectos Clave

- **Disponibilidad:** Ataques DoS contra servidores y terminales

- **Privacidad:** Evitar que personas no autorizadas puedan inspeccionar los mensajes de señalización, audio o video.
- **Integridad de los Mensajes:** Prevenir que usuarios no autorizados puedan manipular los paquetes de información
- **Autenticación:** Controlar la identidad del usuario para evitar suplantaciones y fraudes.

→ **H.323 v.2 incorporó la recomendación H.235 para satisfacer las necesidades de Autenticación, Integridad, Privacidad y no-Repudiación**

→ **El IETF está trabajando para la adopción e integración de ciertos protocolos de seguridad dentro de SIP**

- **Integración con Firewall y NAT:** Facilitar el desarrollo de servicios hacia redes externas a través de Firewalls y NAT

Firewalls y NAT

H.323 y SIP son protocolos que establecen dinámicamente el número de puerto TCP o UDP sobre el que van a intercambiar señalización o datos/voz/vídeo.

- Consecuencia: Algunos Firewall bloquean la comunicación

Los mensajes H.323 y SIP incluyen la dirección IP del remitente y el destinatario.

- Consecuencia: en un entorno con NAT, al destinatario le llegará en la cabecera del mensaje la dirección privada del remitente, cuando intente responder a esa IP fracasará

Integración con Firewalls y NAT

• **Stateful Firewalls/NAT**. Son Firewalls y NATs capacitados para reconocer el tráfico H.323/SIP/SCCP y hacer un seguimiento del estado de cada sesión. A partir de esta información pueden abrir o cerrar el paso sobre los puertos TCP y UDP que sean precisos

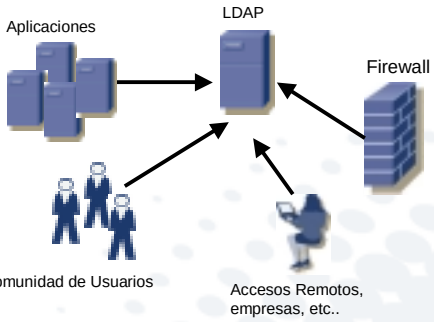
• **MidComm (Middlebox Communications).** Se habilita un mecanismo de comunicación entre el Firewall/NAT y el Gatekeeper H.323/SIP Proxy para que estos últimos puedan informar al Firewall sobre que puertos debe permitir el paso. Esta es una iniciativa del IETF

• **uPnP**. La propuesta Universal Plug&Play está liderada por Microsoft y pretende extender las capacidades PnP hacia la Red.De esta forma un cliente SIP uPnP puede dialogar con un Firewall/NAT uPnP para comunicarle sus necesidades de puertos activos y direcciones IP

UNITRONICS

Autentificación

Soluciones: Repositorio común de usuarios (LDAP) y PKI



Establecer una infraestructura de clave publica (PKI)

- **Confidencialidad**
- **Autentificación**
- **Firma Digital**
- **Etc..**

- Soporte hardware: Tarjeta Inteligente, llave USB

UNITRONICS

Gestión de Logs Centralizada

Una necesidad

- Múltiples sistemas de seguridad heterogéneos: IDS, Firewall, Antivirus, etc...
- Detección de ataques correlacionando diferentes log´s
- Análisis Forense
- Informes de actividad

Conectores universales

- Syslog
- Windows Eventlog
- WMI
- ASCII Logs
- Etc..

UNITRONICS
COMUNICACIONES

Muchas Gracias por su Atención

Israel García Yagüe
igy@unitronics.es