Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

VII Foro de seguridad RedIRIS

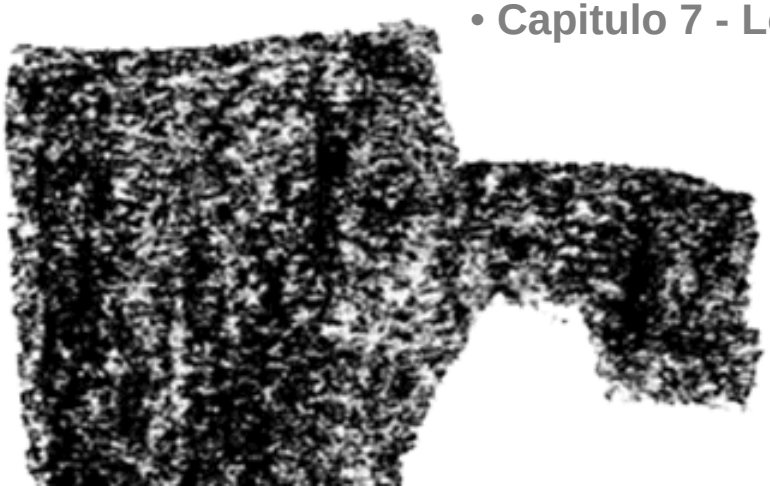
Iñaki Ortega
inaki.ortega@ehu.es

RedIRIS

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

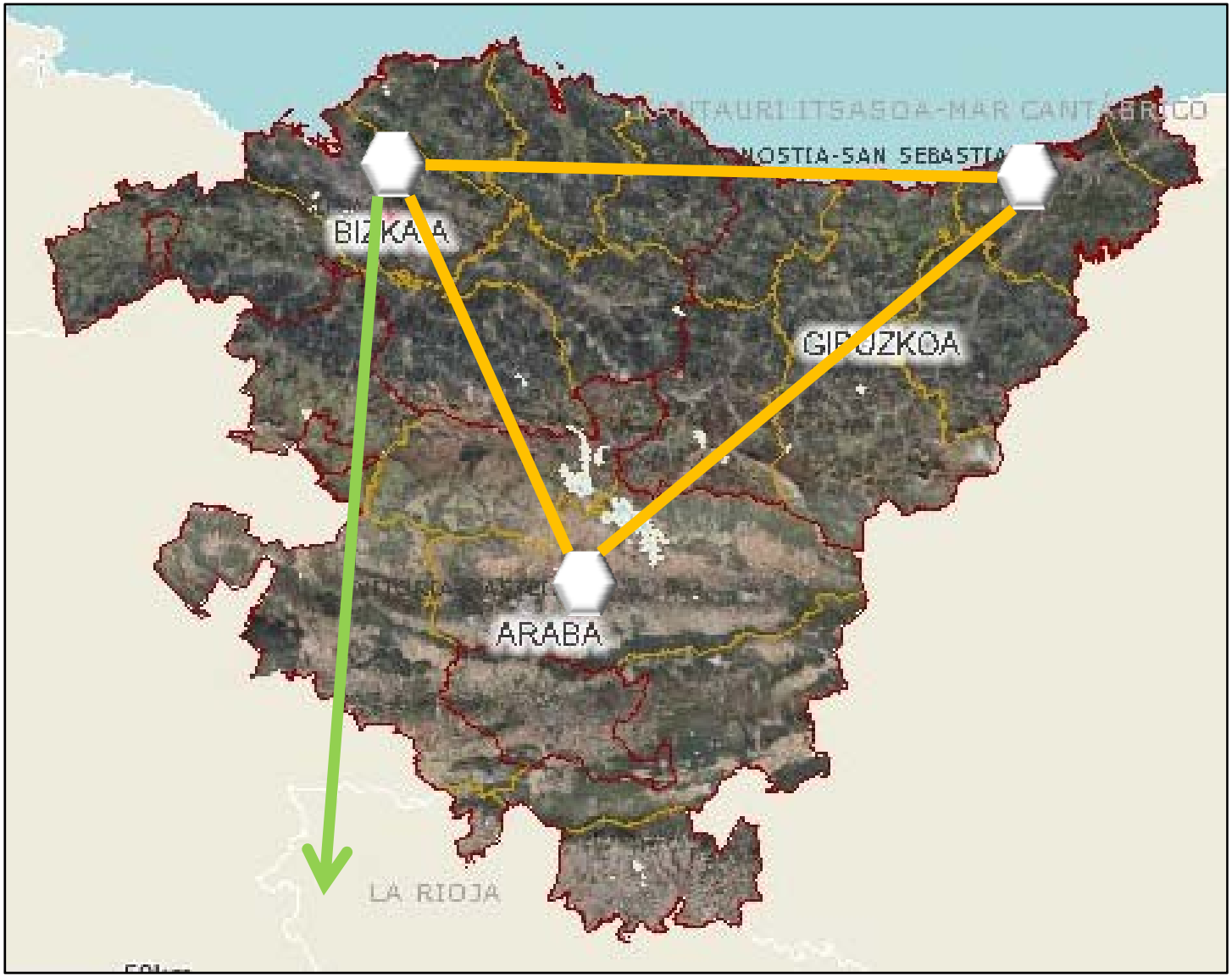
eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

índice



Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

Introducción


BIZKAIA
GIPUZKOA
ARABA
LA RIOJA

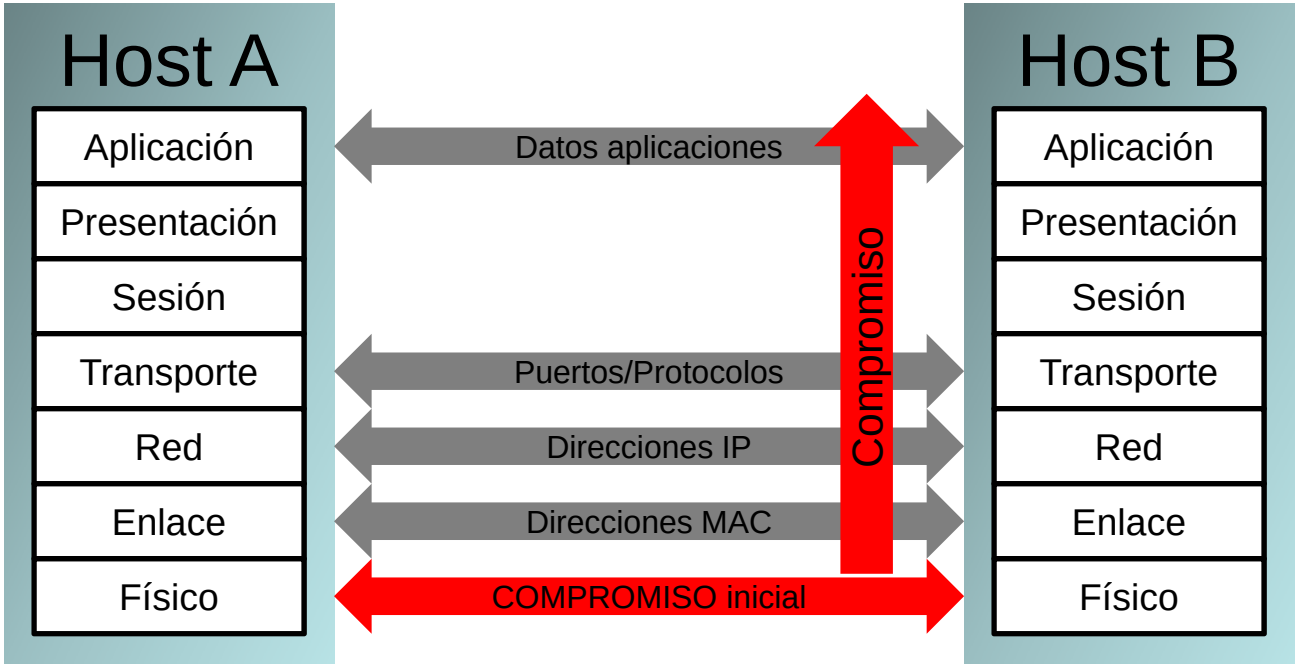
- **Algunos datos de interés**

	Araba	Gipuzkoa	Bizkaia	TOTAL
Centros	18	22	32	**72**
Armarios	39	84	160	**283**
Switches (1)	160 (2)	424	736	**1.320**
APs WiFi (1)	163	228	493	**884**
PCs y perif. (3)	3.385	9.557	13.784	**26.726**

(1) Electrónica CISCO
(2) Switches de 48 puertos
(3) Solo los conectados a la red de cable

- **¿Por qué una presentación por niveles?**

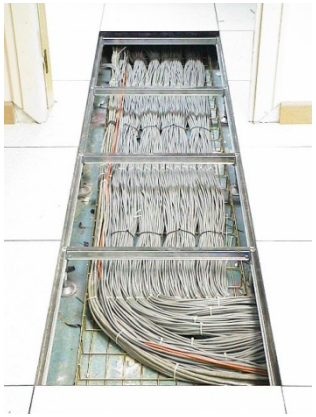
- **¿Por qué una presentación por niveles?**



Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

Problemas y soluciones L1

- Problema: Incidencias en la infraestructura física de red
- Descripción: Cualquier fallo en la instalación física afecta a parte o a toda la red
- Soluciones:
  - Correcta instalación y protección de cableado
  - Control de acceso a Racks y otros elementos de la instalación
  - Protección adecuada de elementos de apoyo (electricidad, AC, etc…)
  - Monitorización de la infraestructura de red



- Problema: Acceso ilícito a la red de cable
- Soluciones si NO se necesita acceso:
  - Rosetas NO parcheadas
  - Rosetas parcheadas a una VLAN no existente y/o deshabilitada
- Soluciones cuando SÍ se necesita acceso:
  - Rosetas parcheadas a VLAN restringida (*usar VPN o similar para acceso a otras VLANes de acceso*)
  - Control de acceso por MAC/Puerto (*gestión compleja*)
  - Utilizar 802.1x
  - Soluciones propietarias (Cisco NAC, Enterasys, etc…)

- Problema: Instalación de elementos extraños en la red lo que lleva a late colision, bucles, errores en tramas, cableados incorrectos…
- Soluciones:
  - Disponer de políticas de conexión y uso de red, de ampliación de puntos de red, uso de equipamiento (p.e. 1 equipo/usuario)
  - Control de acceso por MAC/Puerto (*gestión complicada*)
  - Habilitar PortFast en los puertos de usuario
    - Spanning-tree portfast bpduguard
  - Habilitar port security limitando el número de MAC a utilizar por puerto
    - switchport port-security
    - switchport port-security maximum 1
  - En caso necesario la instalación de equipamiento de red SIEMPRE la autoriza, instala y gestiona el NOC

Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

Problemas y soluciones L2

- Problema: VLAN Hopping
- Descripción: El atacante salta de VLAN haciendo doble encapsulamiento de trama 802.1q (*solo funciona si la VLAN nativa es la VLAN 1*)
- Soluciones:
  - Usar SIEMPRE una VLAN dedicada para los trunks
  - Evitar que la VLAN nativa sea la VLAN 1
  - Deshabilitar auto-trunking en los puertos de usuario (*DTP off*)

- Problema: Ataques MAC
- Descripción: Herramientas comunes como macof o yersinia desbordan las tablas CAM de los switches y los convierten en HUBs
- Solución:

  Habilitar port security mitiga estos ataques deshabilitando el puerto y enviando traps SNMP al receptor de eventos que se haya configurado

NOTA: Si hay teléfonos IP con mini-switch el límite de MACs por puerto deberá ser de 2 o 3

NOTA: Si se ha habilitado port security y hay una ataque, la CPU del switch subirá al 100% pero aun así podremos acceder a él

- Problema: Ataques DHCP (I)
  - DHCP Starvation Attack (DoS)
- Descripción: El atacante (*gobbler*) agota las direcciones de los pooles del servidor DHCP
- Solución:

Una vez más habilitando port security impide que este tipo de ataque se lleve a cabo

- Problema: Ataques DHCP (II)
  - Rogue DHCP Server Attack
- Descripción:
  - El atacante instala un servidor DHCP alternativo al corporativo
  - Normalmente el servidor falso responde antes al cliente que el corporativo
  - El servidor falso le pasa al cliente los datos que quiera (IP, máscara, default-gw, servidor dns…)
- Solución:

Utilizar DHCP snooping lo que permite a la infraestructura de red conocer donde están (switch/puerto) los servidores corporativos y no permitir que se instalen otros servidores falsos. Se crea la siguiente tabla de estado en los switches:

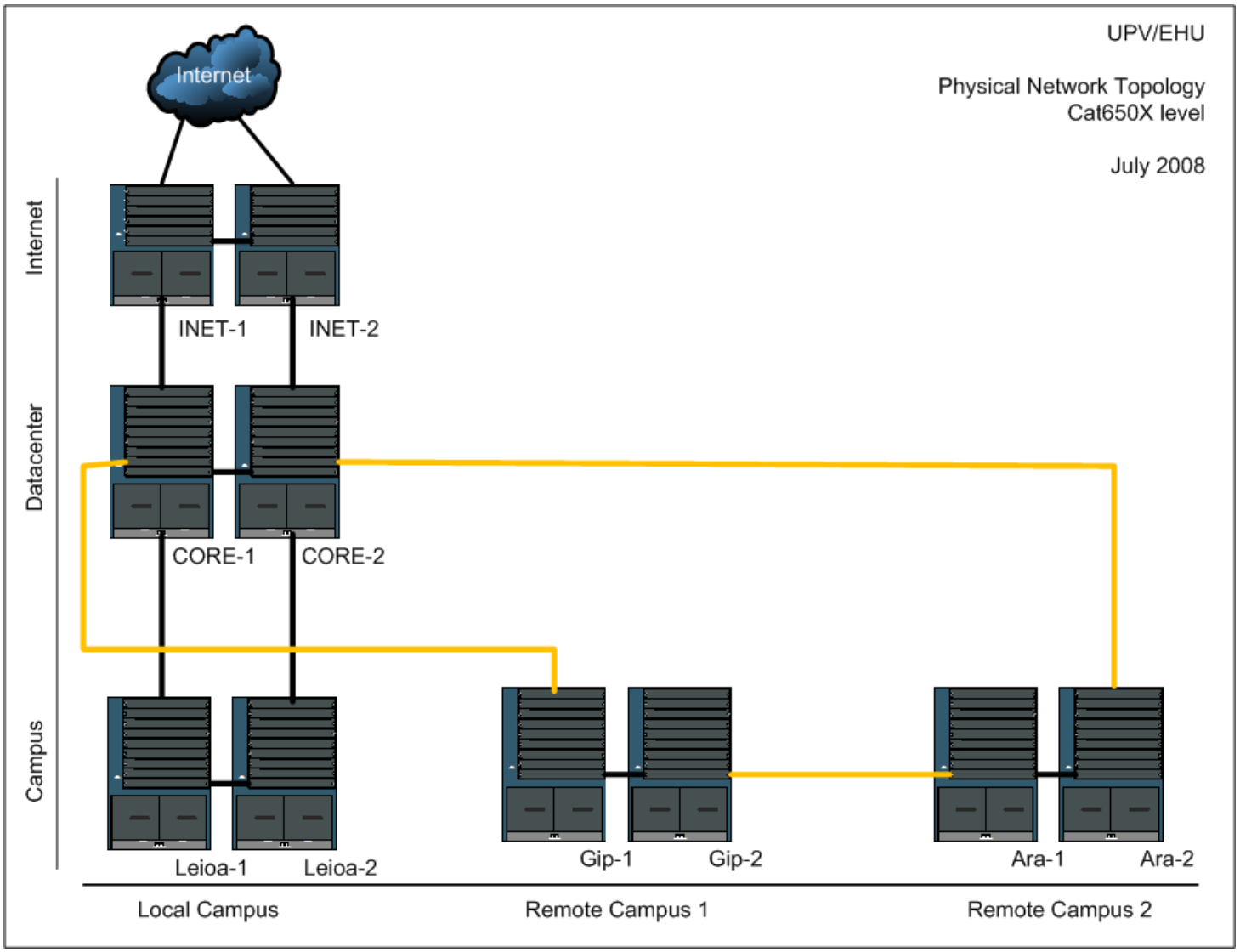
```
sh ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------  --------------- ----------   -------------  ----  --------------------
00:03:47:B5:9F:AD   10.120.4.10     193185       dhcp-snooping  4     FastEthernet3/18
```

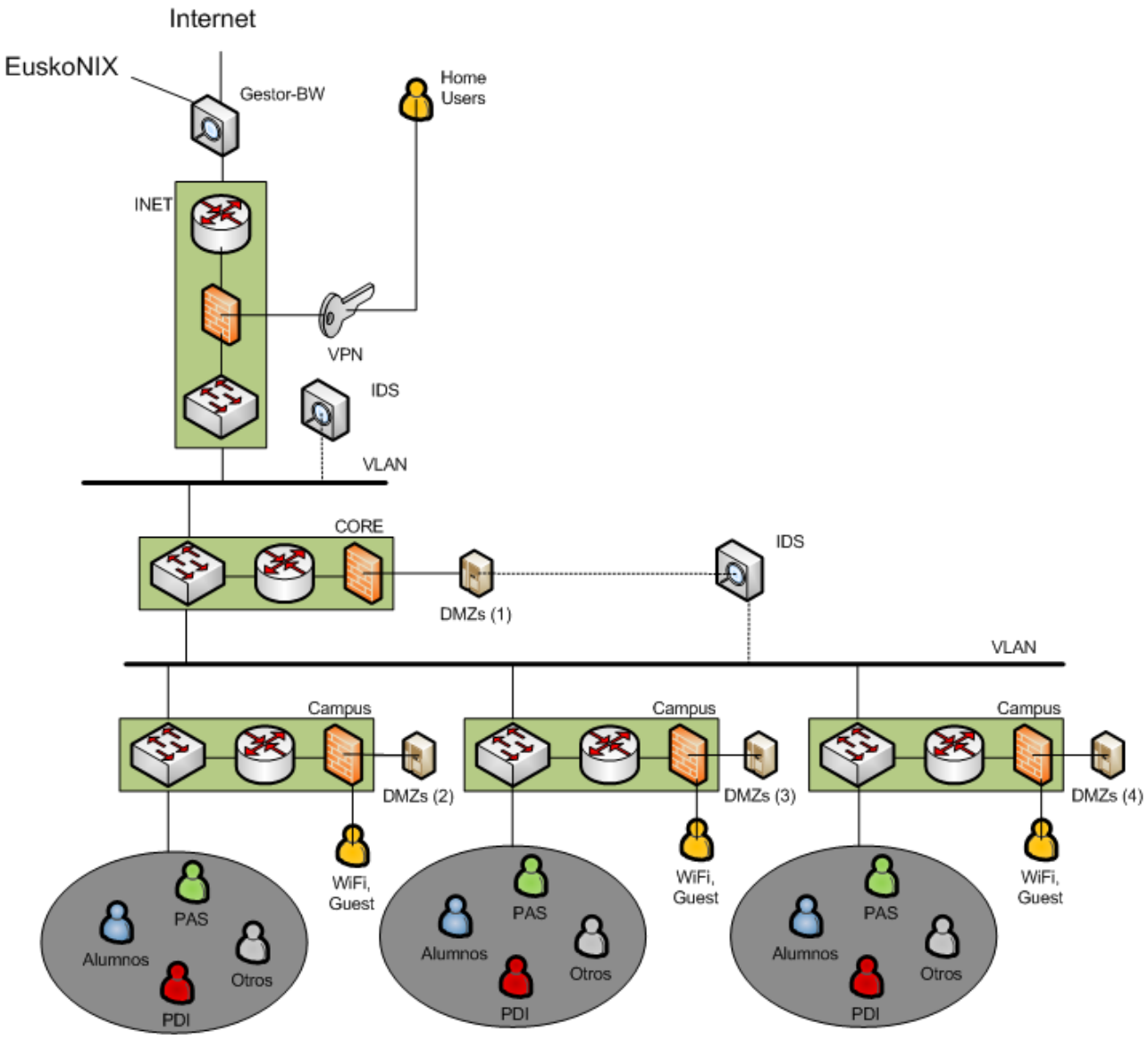
- Problema: Ataques ARP
- Descripción: De acuerdo a los RFC un equipo puede enviar una respuesta ARP aun cuando no ha habido pregunta previa (*gratuitous ARP*) y el resto de equipos en la red guardarán esa información. De esta forma se pueden preparar ataques man-in-the-middle con herramientas como dsniff, Cain & Abel, etthercap, Yersinia, etc…
- Solución:
  1. Activar DHCP snooping
  2. Activar Dynamic ARP Inspection que comprueba los campos MacAddress e IpAddress de la tabla de estado de DHCP snooping y si los datos no son correctos se bloquea el tráfico

- Problema: Ataques IP/MAC Spoofing
- Descripción: Si se falsifica la dirección IP, se pueden realizar ataques del tipo Ping of Death, SYN flood, ICMP unreachable storm, etc…, si por el contrario se usa la MAC para acceder a la red, ésta se falsifica conseguir acceso a la red o la identidad de otro equipo.
- Solución:
  1. Activar DHCP snooping
  2. Activar IP/MAC Source guard que comprueba los campos MacAddress e IpAddress de la tabla de estado de DHCP snooping y si los datos no son correctos se bloquea el tráfico

Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

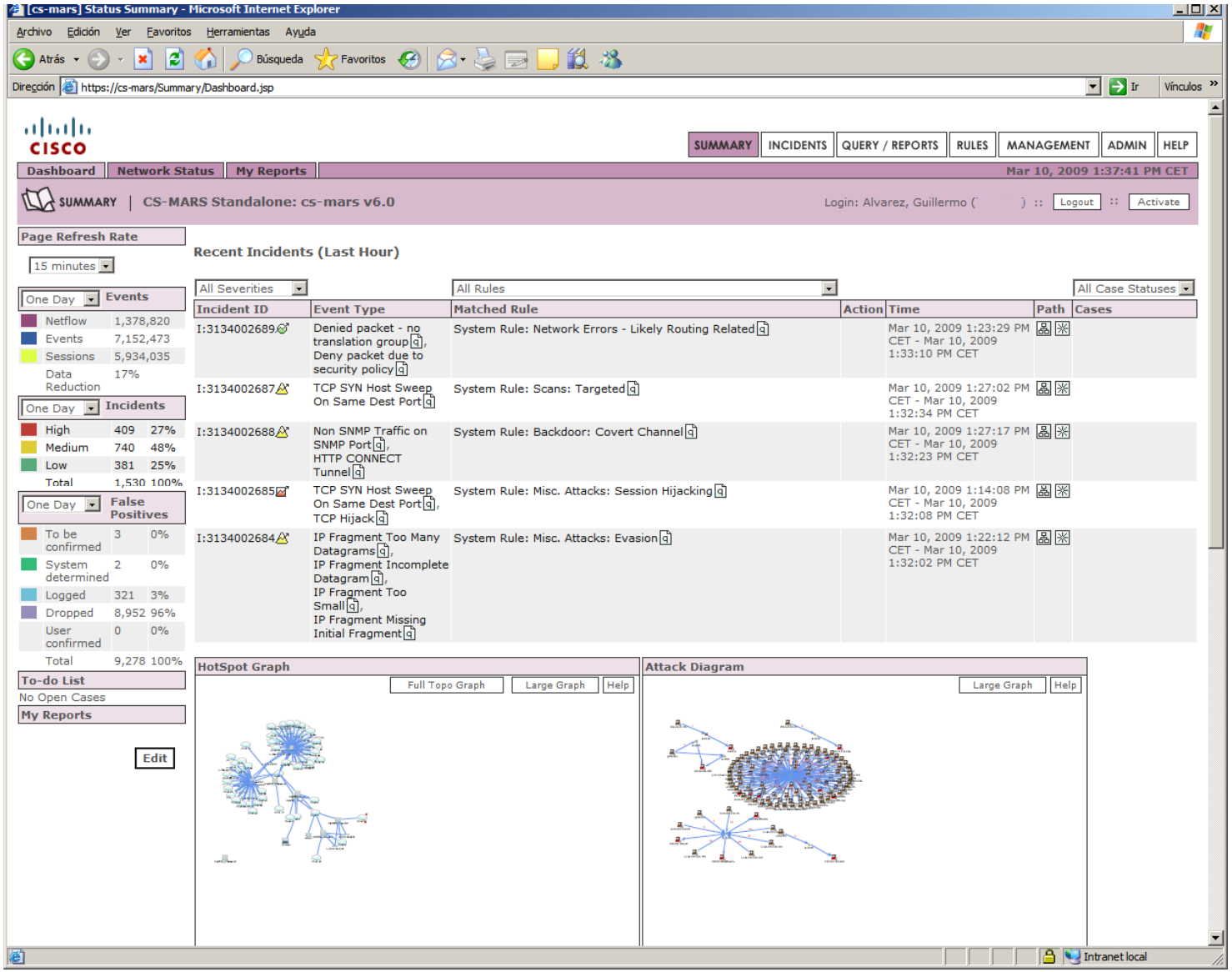
Problemas y soluciones L3


UPV/EHU
Physical Network Topology
Cat650X level
July 2008
Internet
Internet
Datacenter
Campus
INET-1
INET-2
CORE-1
CORE-2
Leioa-1
Leioa-2
Gip-1
Gip-2
Ara-1
Ara-2
Local Campus
Remote Campus 1
Remote Campus 2

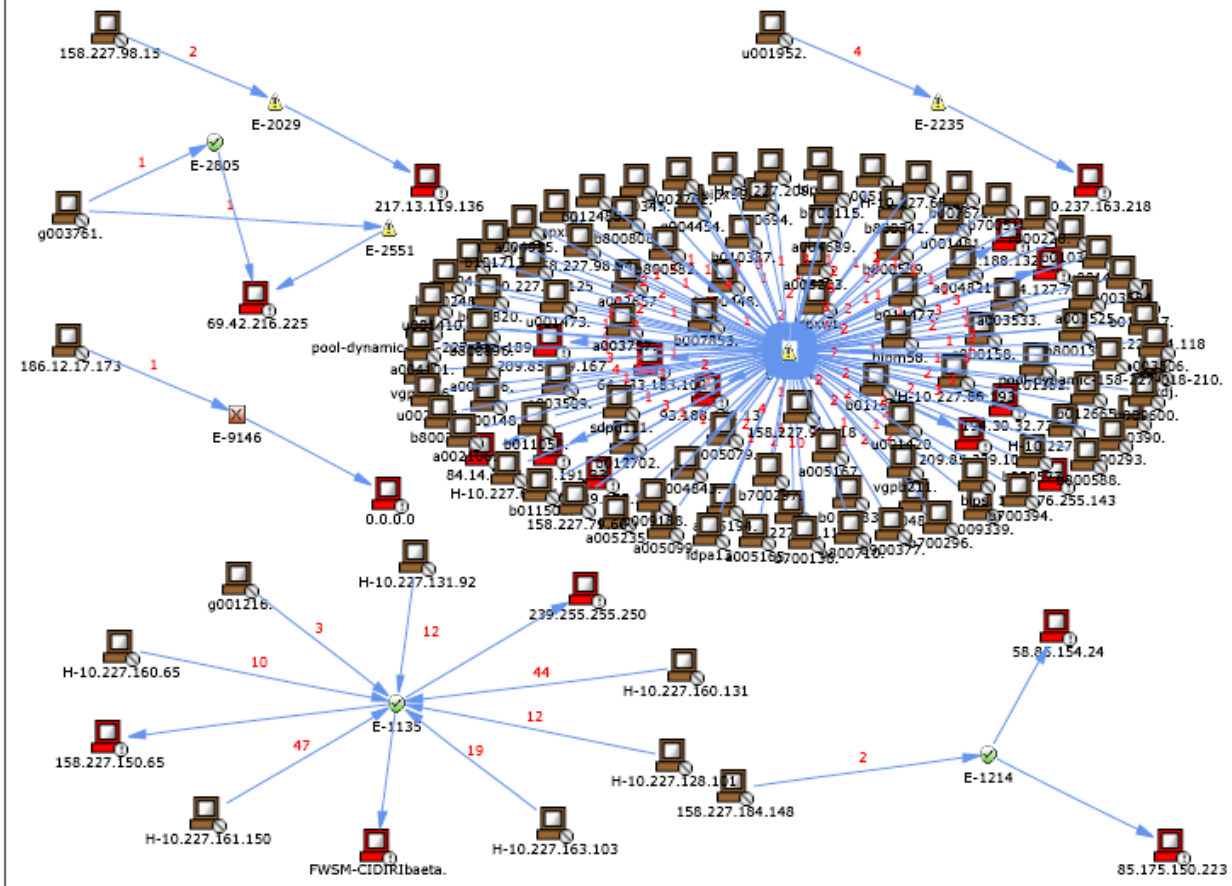

Internet
EuskoNIX
Gestor-BW
Home Users
INET
VPN
IDS
VLAN
CORE
DMZs (1)
IDS
VLAN
Campus
DMZs (2)
Campus
DMZs (3)
Campus
DMZs (4)
WiFi, Guest
WiFi, Guest
WiFi, Guest
PAS
Alumnos
Otros
PDI
PAS
Alumnos
Otros
PDI
PAS
Alumnos
Otros
PDI

- Problema: Muchos cacharros a gestionar y pocas manos
- Solución:
  - Disponer de una herramienta de recogida y correlación de eventos: CS-MARS
    - >4.000 eventos por segundo
    - Gran variedad de eventos a recoger (FW, IPS/IDS, Routers, Switches, Servidores, Servicios…)

  - Disponer de personal preparado y dedicado a gestionar el equipo que eliminando falsos positivos y dotando de mayor efectividad al equipo


[cs-mars] Status Summary - Microsoft Internet Explorer
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección https://cs-mars/Summary/Dashboard.jsp
Ir Vínculos
CISCO
SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP
Dashboard Network Status My Reports
Mar 10, 2009 1:37:41 PM CET
SUMMARY | CS-MARS Standalone: cs-mars v6.0
Login: Alvarez, Guillermo ( ) :: Logout :: Activate
Page Refresh Rate
15 minutes
One Day Events
Netflow 1,378,820
Events 7,152,473
Sessions 5,934,035
Data Reduction 17%
One Day Incidents
High 409 27%
Medium 740 48%
Low 381 25%
Total 1,530 100%
One Day False Positives
To be confirmed 3 0%
System determined 2 0%
Logged 321 3%
Dropped 8,952 96%
User confirmed 0 0%
Total 9,278 100%
To-do List
No Open Cases
My Reports
Edit
Recent Incidents (Last Hour)
All Severities
All Rules
All Case Statuses
Incident ID
Event Type
Matched Rule
Action
Time
Path
Cases
I:3134002689
Denied packet - no translation group, Deny packet due to security policy
System Rule: Network Errors - Likely Routing Related
Mar 10, 2009 1:23:29 PM CET - Mar 10, 2009 1:33:10 PM CET
I:3134002687
TCP SYN Host Sweep On Same Dest Port
System Rule: Scans: Targeted
Mar 10, 2009 1:27:02 PM CET - Mar 10, 2009 1:32:34 PM CET
I:3134002688
Non SNMP Traffic on SNMP Port, HTTP CONNECT Tunnel
System Rule: Backdoor: Covert Channel
Mar 10, 2009 1:27:17 PM CET - Mar 10, 2009 1:32:23 PM CET
I:3134002685
TCP SYN Host Sweep On Same Dest Port, TCP Hijack
System Rule: Misc. Attacks: Session Hijacking
Mar 10, 2009 1:14:08 PM CET - Mar 10, 2009 1:32:08 PM CET
I:3134002684
IP Fragment Too Many Datagrams, IP Fragment Incomplete Datagram, IP Fragment Too Small, IP Fragment Missing Initial Fragment
System Rule: Misc. Attacks: Evasion
Mar 10, 2009 1:22:12 PM CET - Mar 10, 2009 1:32:02 PM CET
HotSpot Graph
Full Topo Graph Large Graph Help
Attack Diagram
Large Graph Help
Intranet local

Attack Diagram



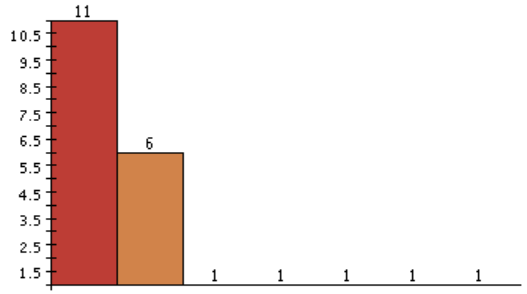
Query Event Data
Click the cells below to change query criteria:

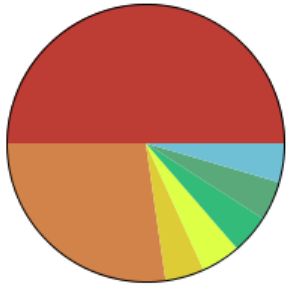
Query type: Source IPs ranked by Sessions, 0d-3h:00m Edit Clear

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	Keyword	Operation	Rule	Action
[158.227.0.0 / 255.255.0.0] n-158.227.0.0/16	ANY	ANY	ANY	ANY	ANY	ANY	ANY	(worm OR troja n)	None	ANY	ANY

Save As Report | Save As Rule | Submit

Query Results





Rank		Count (# of Sessions)	Raw Source IP	Hosts
	1	11	158.227.0.64	<hostname could not be resolved>
	2	6	158.22[redacted]	u.es
	3	1	158.22[redacted]	ehu.es
	3	1	158.22[redacted]	ehu.es
	3	1	158.22[redacted]	ehu.es
	3	1	158.22[redacted]	hu.es
	3	1	158.22[redacted]	ehu.es

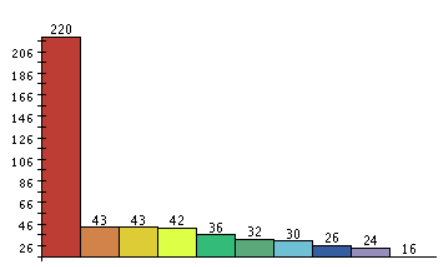
Total Sessions: 22

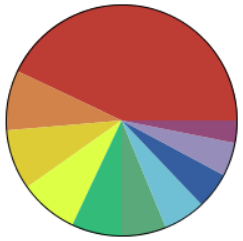
Report Results (Total): Alertas Bizkaia 4h Mar 10, 2009 8:16:09 AM CET - Mar 10, 2009 12:16:09 PM CET

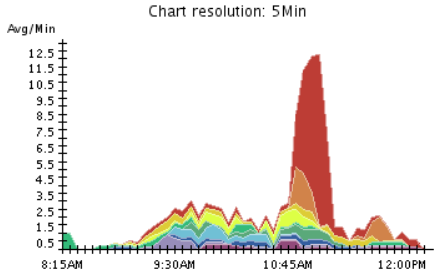
Name	Provider	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Alertas Bizkaia 4h	Local	Weekly: 12:00 Noon, Mon, Tue, Wed, Thu, Fri	Total View	[redacted]	Src: 158.227.0.0-158.227.99.254 Query Type: Source IPs ranked by Sessions Time: 0d-4h:00m	Alertas severas originadas desde IPs de Bizkaia en las ultimas 4 horas Clasificadas por IP origen (8-12 AM)	Finished: Mar 10, 2009 12:16:09 PM CET	Mar 10, 2009 12:16:09 PM CET	Mar 10, 2009 8:15:00 AM CET - Mar 10, 2009 12:15:00 PM CET

Report type: Source IPs ranked by Sessions, 0d-4h:00m

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	Keyword	Operation	Rule	Action
158.227.0.0-158.227.99.254	ANY	ANY	ANY, Only Red Severity	ANY	ANY	ANY	ANY	ANY	None	ANY	ANY





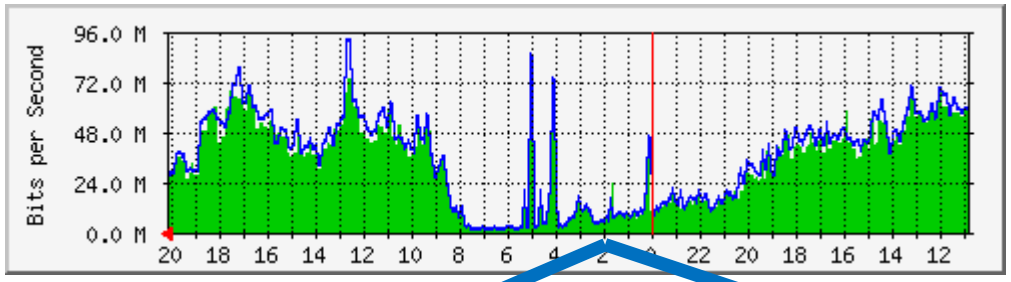


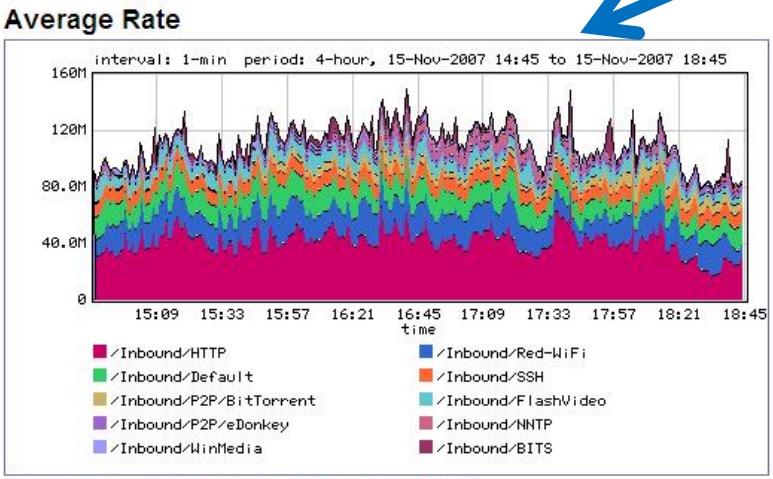
Rank		Total Sessions	Average / Minute	Raw Source IP	Hosts
	1	220	0.92	158.[redacted]	<hostname could not be resolved>
	2	43	0.18	158.[redacted]	[redacted]ll.ehu.es
	2	43	0.18	158.[redacted]	[redacted]u.es
	4	42	0.17	158.[redacted]	[redacted]we.lc.ehu.es
	5	36	0.15	158.[redacted]	[redacted]u.es
	6	32	0.13	158.[redacted]	[redacted]ll.ehu.es
	7	30	0.12	158.[redacted]	[redacted]ll.ehu.es
	8	26	0.11	158.[redacted]	[redacted]u.es
	9	24	0.1	158.[redacted]	[redacted]could not be resolved>
	10	16	0.07	158.[redacted]	[redacted]ll.ehu.es
	11	15	0.06	158.[redacted]	[redacted]could not be resolved>
	11	15	0.06	158.[redacted]	[redacted]ll.ehu.es
	13	14	0.06	158.[redacted]	[redacted]es
	14	13	0.05	158.[redacted]	[redacted]ll.ehu.es

Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

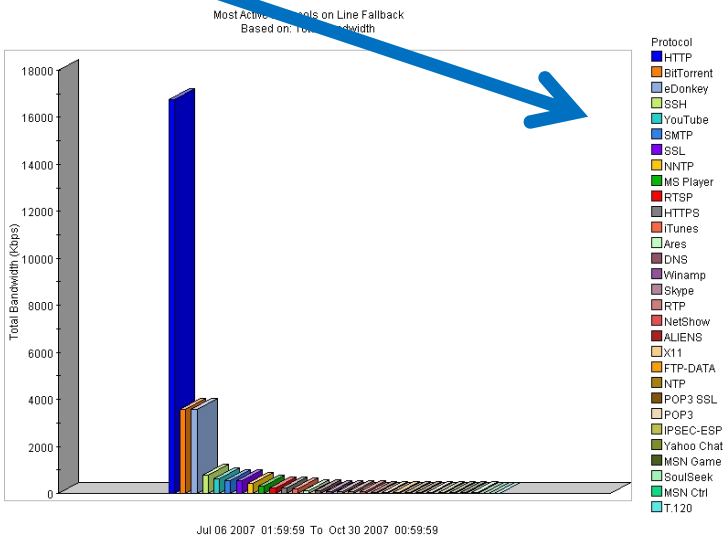
Problemas y soluciones L7

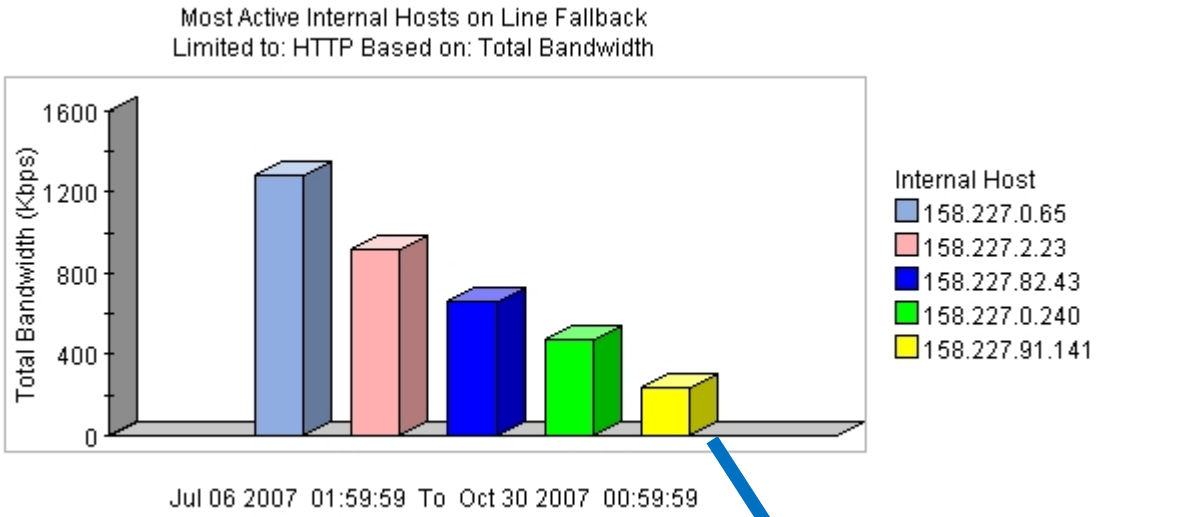
- Gestión del ancho de banda

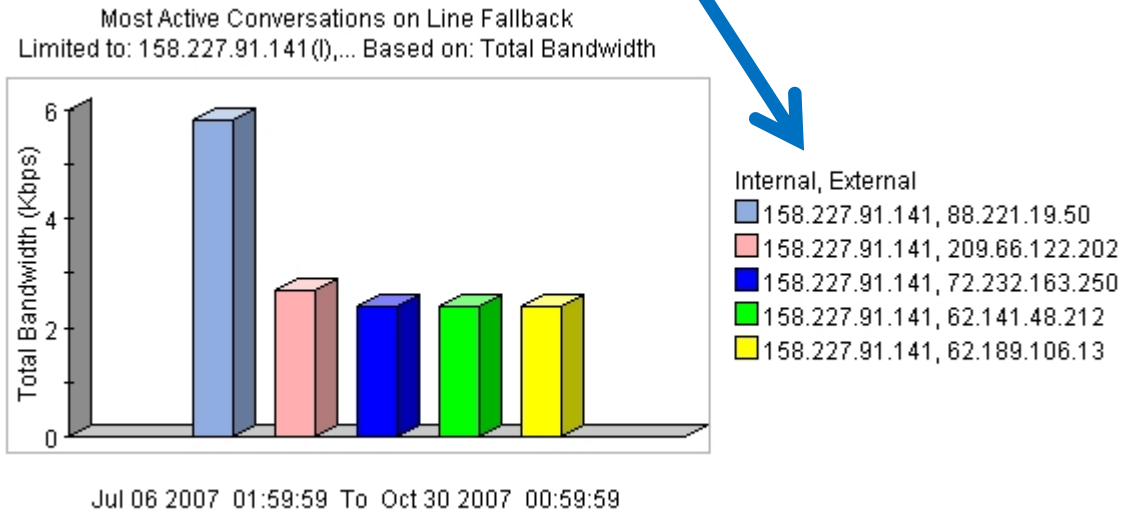




Classes other than the Top Ten are not shown.




Most Active Internal Hosts on Line Fallback
Limited to: HTTP Based on: Total Bandwidth
Total Bandwidth (Kbps)
1600
1200
800
400
0
Internal Host
158.227.0.65
158.227.2.23
158.227.82.43
158.227.0.240
158.227.91.141
Jul 06 2007 01:59:59 To Oct 30 2007 00:59:59


Most Active Conversations on Line Fallback
Limited to: 158.227.91.141(I),... Based on: Total Bandwidth
Total Bandwidth (Kbps)
6
4
2
0
Internal, External
158.227.91.141, 88.221.19.50
158.227.91.141, 209.66.122.202
158.227.91.141, 72.232.163.250
158.227.91.141, 62.141.48.212
158.227.91.141, 62.189.106.13
Jul 06 2007 01:59:59 To Oct 30 2007 00:59:59

Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

Gestión proactiva y reactiva

Ante este panorama solo tenemos dos opciones

- **Realizar una gestión de la seguridad proactiva**

  Necesitaremos un buen diseño de base, herramientas de control, monitorización y gestión pero a cambio trabajaremos de una forma más planificada y con menos incidentes de seguridad

- **Realizar una gestión de la seguridad reactiva**

  Trabajaremos ‘bajo demanda’ según vayan surgiendo los incidentes de seguridad con mucho más estrés y con menor control de la situación

Puntos fuertes en la gestión de la seguridad

1. Red de datos de acceso homogénea y bien estructurada
2. Gestión hasta el puesto de usuario
3. Red propia de gestión (OAM)
4. Políticas de acceso y uso de la red, de adquisición de equipamiento, de tratamiento de incidentes, etc…
5. Aplicación de gestión de inventario+DNS+DHCP (XIXARE)
6. Aplicación de políticas de prevención en L1, L2, L3 y L7
7. Monitorización continua de lo que ocurre en la red (Scripts, NetDisco, otros…)
8. Aplicación de políticas de contención de plagas (filtrado automático en los FW ante ciertos patrones)
9. Personal preparado y dedicado para la gestión de la red y la seguridad

Experiencias en arquitecturas de seguridad en la comunidad RedIRIS

Lo que queda pendiente…

…pero falta mucho por hacer

1. Disponer de una POLITICA DE SEGURIDAD o SGSI
   1. Corporativa
   2. De servidores departamentales
   3. De acceso a Internet
2. Mejorar la prevención
3. Mayor visibilidad de aplicaciones (FW-L7)
4. Mejorar la gestión de los incidentes de seguridad
5. Mejor coordinación con otros grupos de seguridad (RedIRIS, otras Universidades, etc…)

6. Y otros retos que van surgiendo cada día

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

www.ehu.es