Redes Auto-protegidas

Fernando Rodriguez Martinez
fernarod@cisco.com

1

Agenda

Cisco.com

- ¿Por qué se necesita una red auto protegida?
- Evolución de las redes auto protegidas.
- Seis propiedades de las redes auto protegidas
- Conclusión

2

Seguridad: Tendencia número 1 en las empresas

Cisco.com

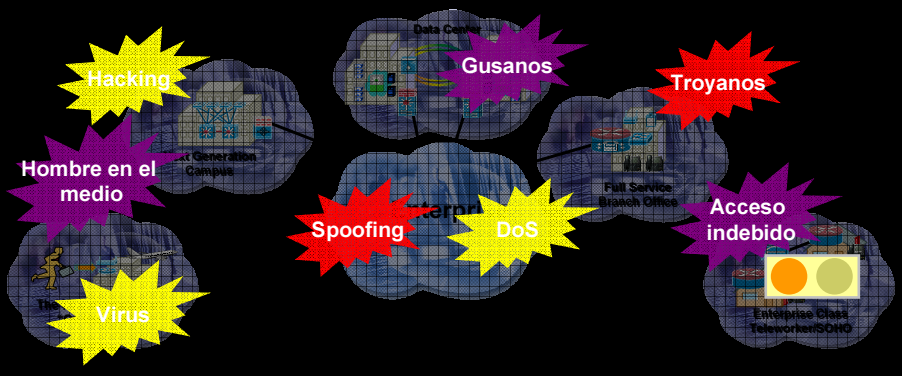
10 principales tendencias durante 2004

Rankings:	2002	2003	2004
Seguridad / Interrupción del negocio	—	12	1
Costos operacionales	1	1	2
Protección de la información - Privacidad	4	2	3
Incrementar ganancias	—	—	4
* Uso de la información en productos-servicios	—	—	5
* Recuperación económica	—	—	6
Vista única por clientes	3	5	7
Innovación rápida	6	3	8
Mayor transparencia en reportes	—	7	9
Manejo de riesgo empresarial	—	4	10

Source: Gartner Top Ten Business Trends, 2004

Retos cada vez más complejos

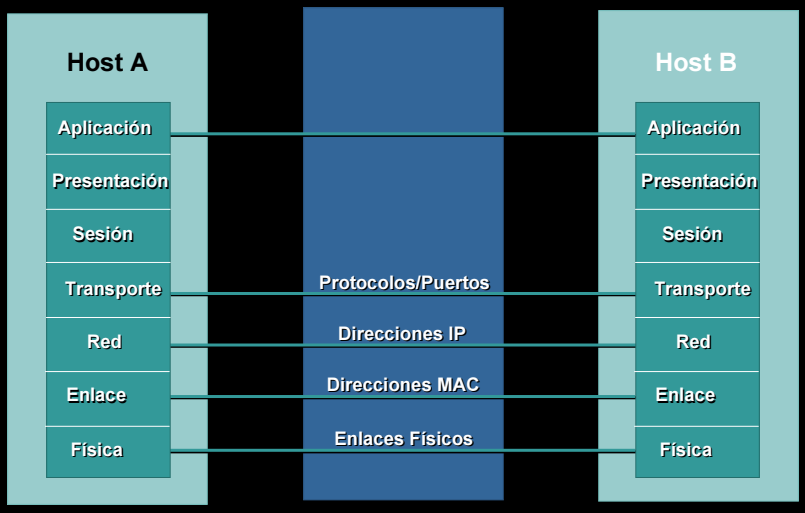
Cisco.com



Modelo OSI: Confianza implícita

Cisco.com

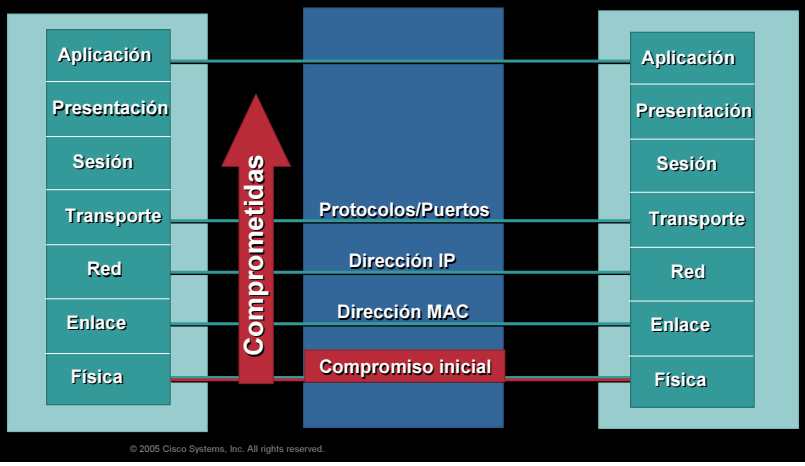
OSI fue construido para permitir que diferentes niveles trabajen sin conocerse entre si



El Efecto dominó

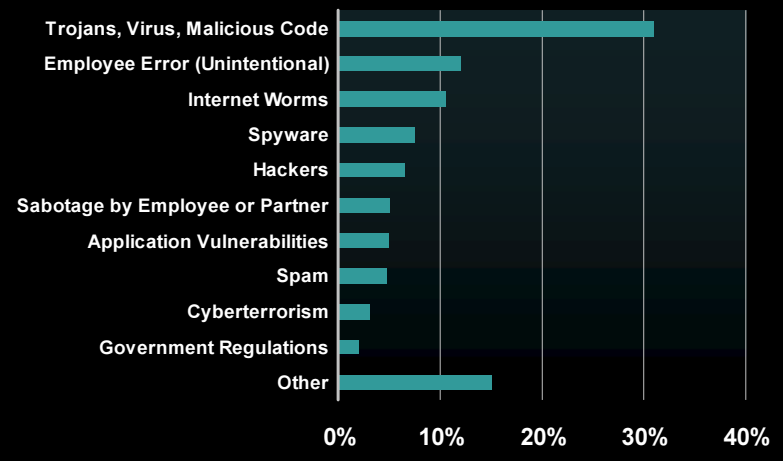
Cisco.com

- La seguridad sólo es tan fuerte como el mas débil de sus enlaces



Amenazas para la seguridad empresarial

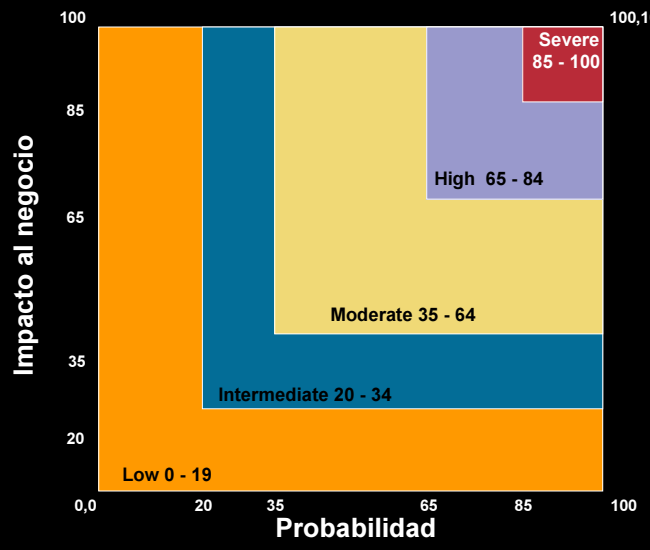
Cisco.com



Source: IDC's *Enterprise Security Survey*, 2004

Seguridad: Manejo de riesgos

Cisco.com



Algunas causas de los problemas de seguridad actuales

Cisco.com

- Educación. Falta de políticas corporativas de seguridad.
- Penetración de defensas por parte de Malware
  Los virus son la causa #1 de pérdidas financieras. *(2004 CSI/FBI)*
- Soluciones reactivas contra ataques de día cero.
- Tecnologías puntuales son evadidas fácilmente.
- Es dificil llevar las políticas de seguridad (si las hay) a la práctica. Como identificar estaciones o servidores que no cumplan con lo dicho por la política.

Velocidad de los ataques

¿Hay tiempo de reaccionar?

Cisco.com

1980s-1990s
Semanas o meses

2000-2002
Horas

2003-Presente-Futuro
Segundos

SQL Slammer
Cada 8.5 seg se duplica
Después de 3 min : 55M scans/sec
1Gbps se satura despues de un minuto

Estrategia de redes auto protegidas
Identificar, prevenir y adptarse a las amenazas

Cisco.com

Fase 3 *"Defensa adaptable a las amenzas"*

- Reconocimiento e inspección segura de aplicaciones.
- Anti-X
- Respuesta proactiva contra amenazas.

Fase 2 *"Colaboración entre sistemas de seguridad"*

- Seguridad de sistema: *Endpoints* + Red + Políticas
- Verificación de aplicaciones, antivirus, red.
- Autenticación y autorización de usuarios.

Fase 1 *"Seguridad Integrada"*

- Hacer de cada elemento de red un punto de defensa.
  - Routers, Switches, Appliances. Endpoints
- Conectividad segura a nivel WAN, LAN. IEEE 802.1x
- Protección de la infraestructra.

Seguridad puntual

- Multiples cajas de seguridad *(appliances)*
- Administración separada

Propiedades de una red auto-protegida

Cisco.com



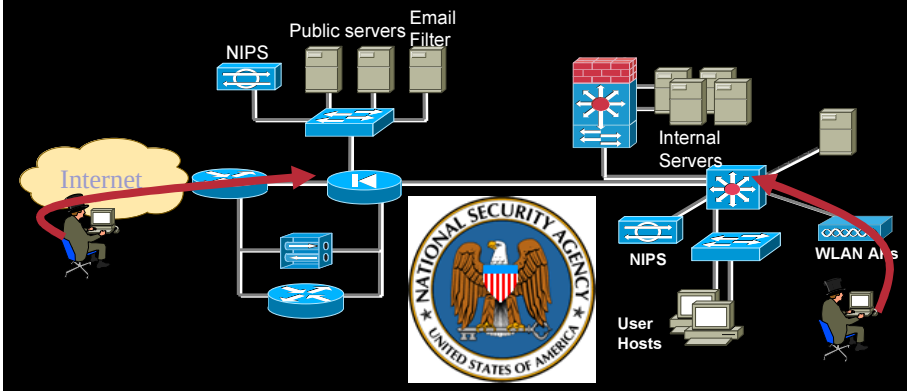


1. ***Disponibilidad de red***: Permanezca activa, aun bajo un ataque.
2. ***Control de acceso***: Autenticar, autorizar usuarios y posturas
3. ***Énfasis en movilidad***: Acceso seguro desde cualquier sitio.
4. ***Inspección de aplicaciones***: Extender la visibilidad de las aplicaciones a la red.
5. ***Contención de ataques***: Identificar y contener rápidamente ataques.
6. ***Protección en el día cero***: Asegurar que las estaciones finales de usuario sean inmunes a nuevas amenazas.

1. Disponibilidad de red

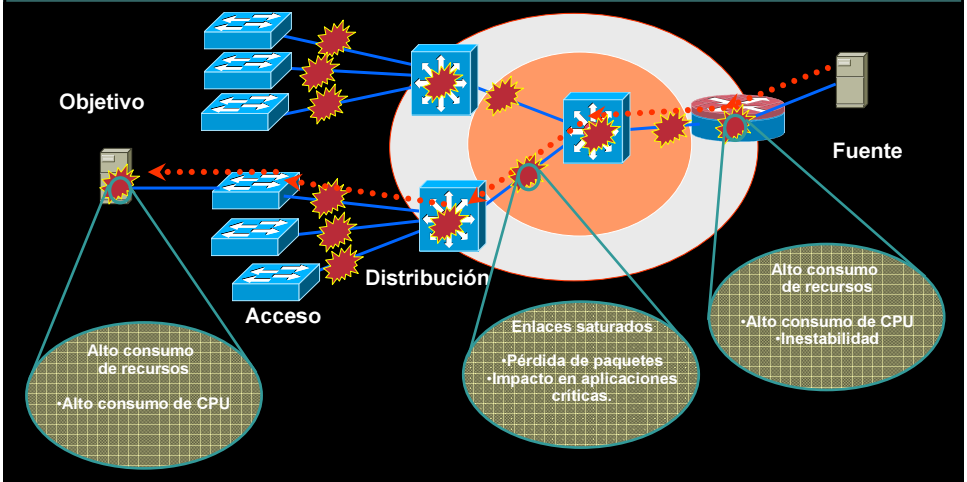
Cisco.com

- **Problema tradicional:** Ataques consumen el ancho de banda de red, al igual que los recursos de las estaciones de usuario y/o equipos de red. Hoy, TODO puede ser un objetivo.



1. Disponibilidad de red (cont)

Cisco.com

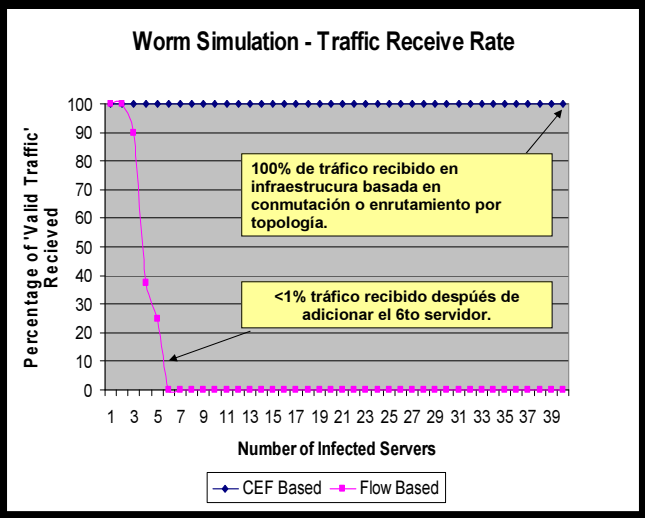


Ataques dirigidos a equipos finales AFECTAN la infraestrucura

1. Disponibilidad de red (cont)

Conmutación basada en flujos o en topología

Cisco.com

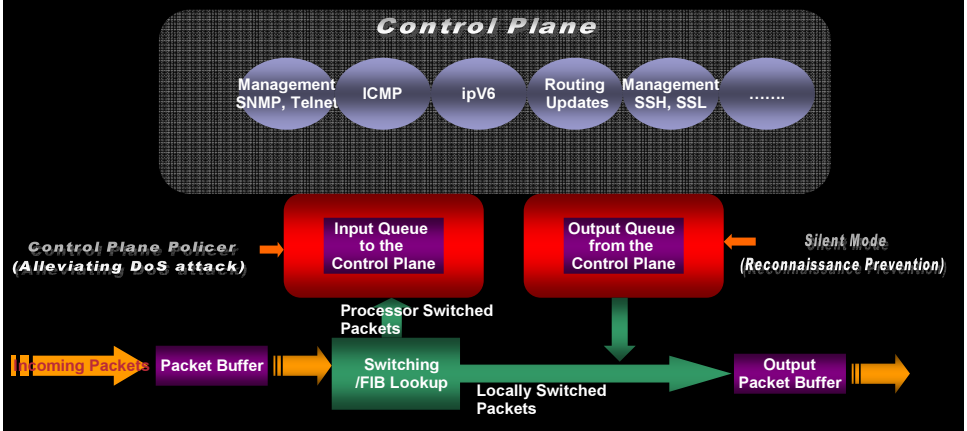


- Alta CPU resulta en una red inestable!

1. Disponibilidad de red (cont)

Control plane policing

Cisco.com



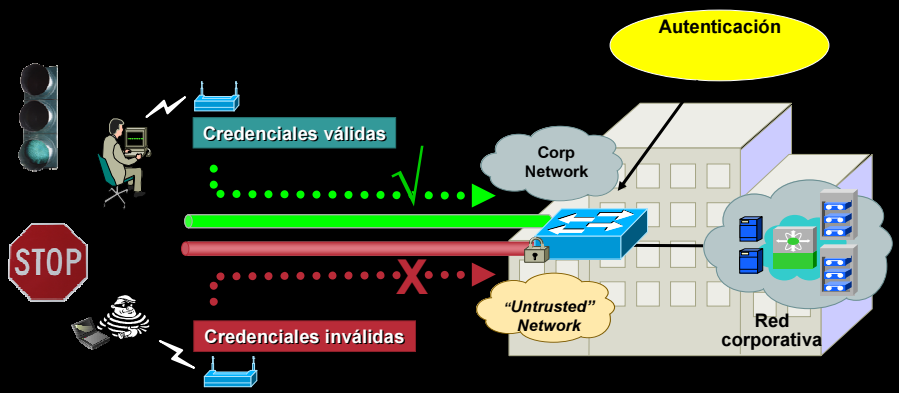
2. Control de acceso

Cisco.com

- **Problema tradicional:** Identificación, autenticación, autorización y control de usuarios no es consistente y la verificación de la postura de seguridad de los equipos es complicada.

2. Control de acceso (cont)

Cisco.com

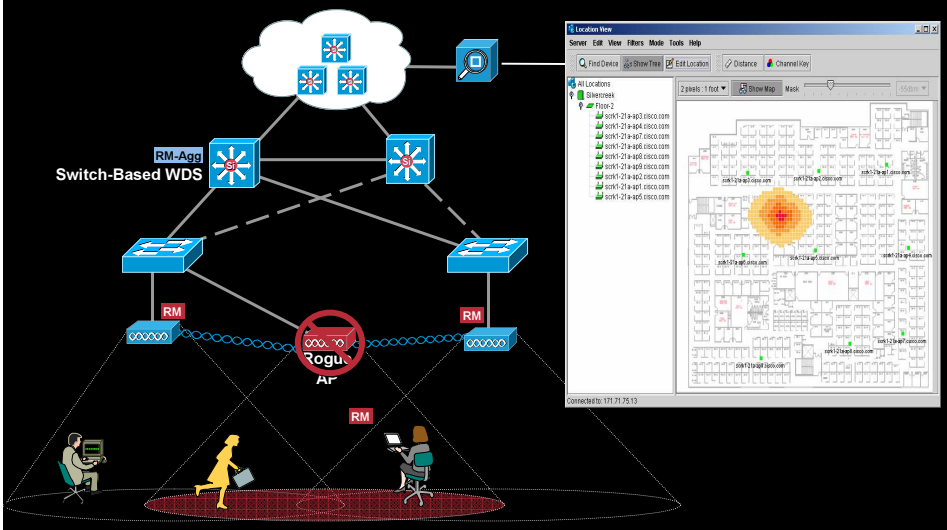


Autenticación 802.1x básica

EAP-MD5, PEAP, EAP-TLS, LEAP…

2. Control de acceso (cont)
Structured Wireless Aware Networks (SWAN)

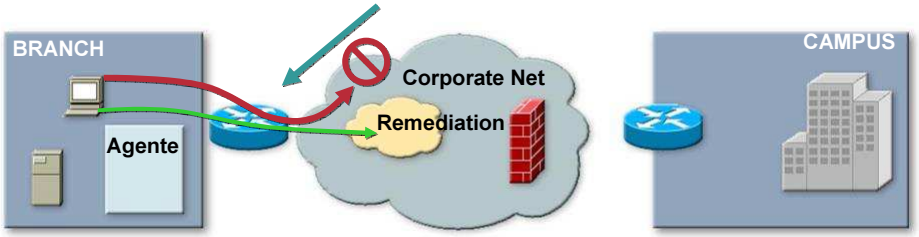
Cisco.com



2. Control de acceso (cont)
Seguridad basada en posturas y configuración

Cisco.com

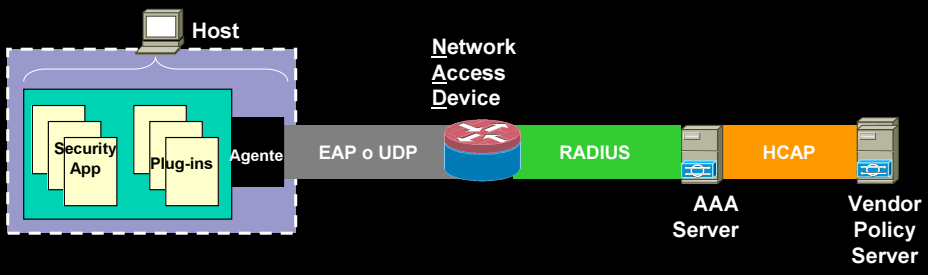
1. Un equipo que no cumple la política de seguridad, intenta conectarse a la red
2. Cuarentena o remedio
3. La infección se contiene-previene.



2. Control de acceso (cont)

Seguridad basada en posturas y configuración

Cisco.com

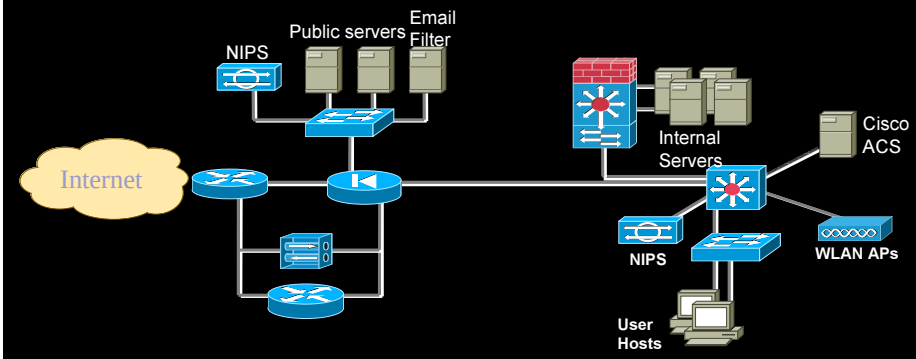


- HCAP: Host Credential Authorization Protocol

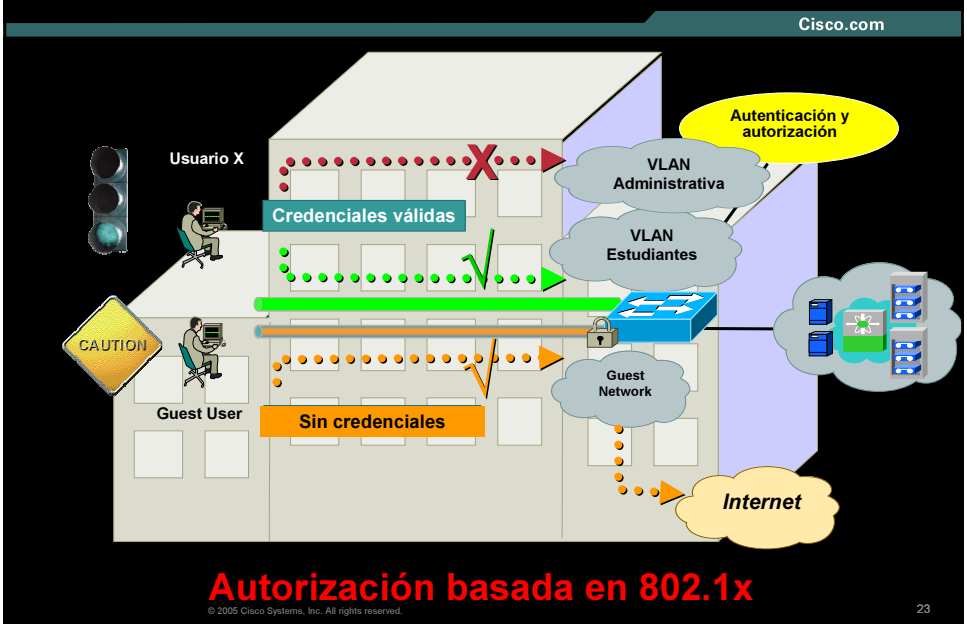
3. Enfasis en movilidad

Cisco.com

- **Problema tradicional:** El acceso es, o demadiado abierto o demasiado restringido.



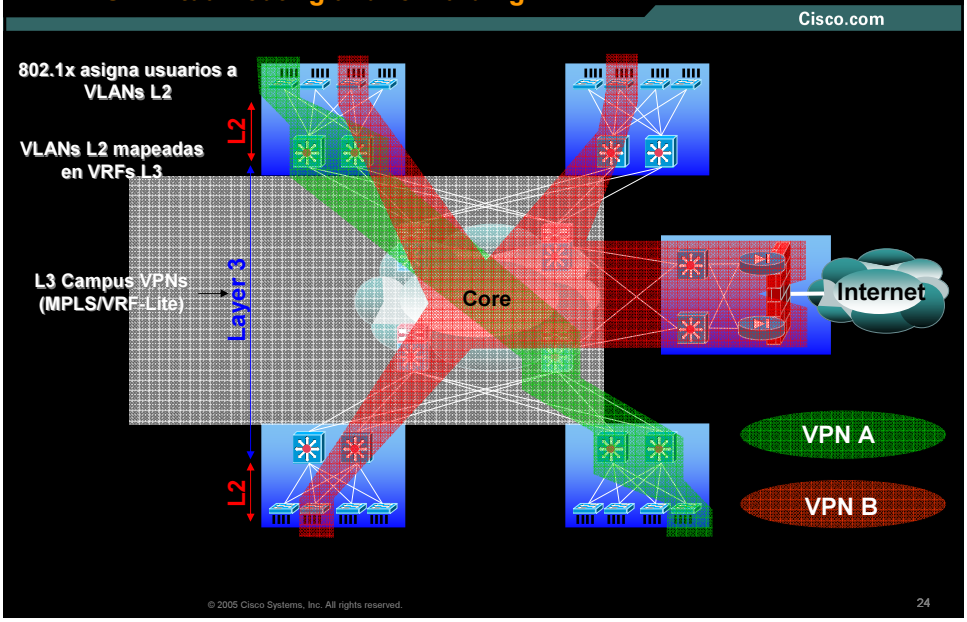
3. Enfasis en movilidad (cont)



Autorización basada en 802.1x

3. Enfasis en movilidad (cont)

MPLS / Virtual routing and forwarding



3. Enfasis en movilidad: SSL VPN

Cisco.com

Análisis completo antes de la conexión:

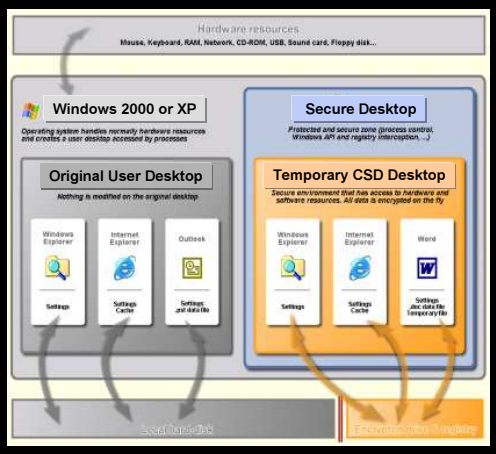
- Análisis de la ubicación – ¿Equipo de la empresa, o no?
- Análisis de la postura de seguridad – AV actualizado? Firewall personal activado? algún indicio de malware?

Protección de la conexión:

- Cajas de arena y encripción protegen todo el tiempo la sesión

Limpieza después de la conexión:

- Sobre-escritura de la memoria usada (no solo borrar) usando algoritmo del DoD
- Sobre-escritura de cache, historia y cookies
- Sobre-escritura de archivos bajados y de attachments de emails.
- Sobre-escritura de *Auto-complete* passwords.

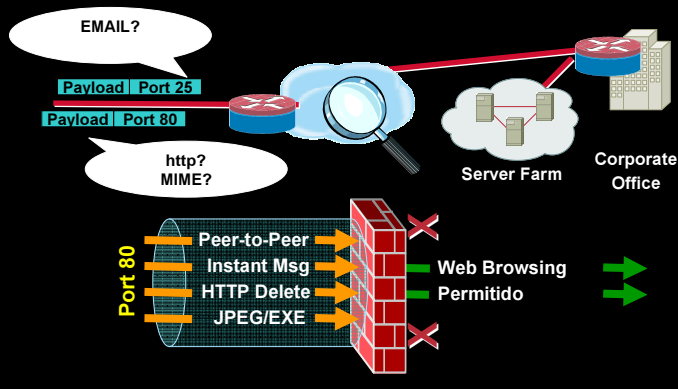


25

4. Inspección de aplicaciones

Cisco.com

- **Problema tradicional:** **Es dificil conocer y controlar los flujos de datos y las sesiones de las aplicaciones dentro de una red (no solo el perímetro).**



26

4. Inspección de aplicaciones

Cisco.com

What About the Future?

- It is clear that there will always be administrative boundaries between networks
- It is clear that there will always be something to enforce those boundaries
- There will always be firewalls
  - They're going to evolve

26

cido
all

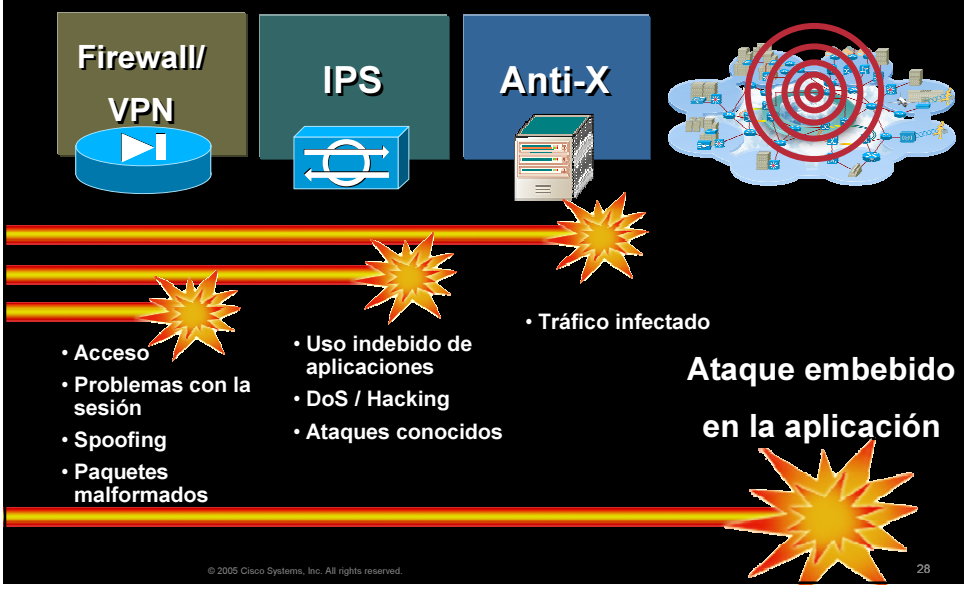
wall

Marcus J. Ranum

27

4. Inspección de aplicaciones (cont)

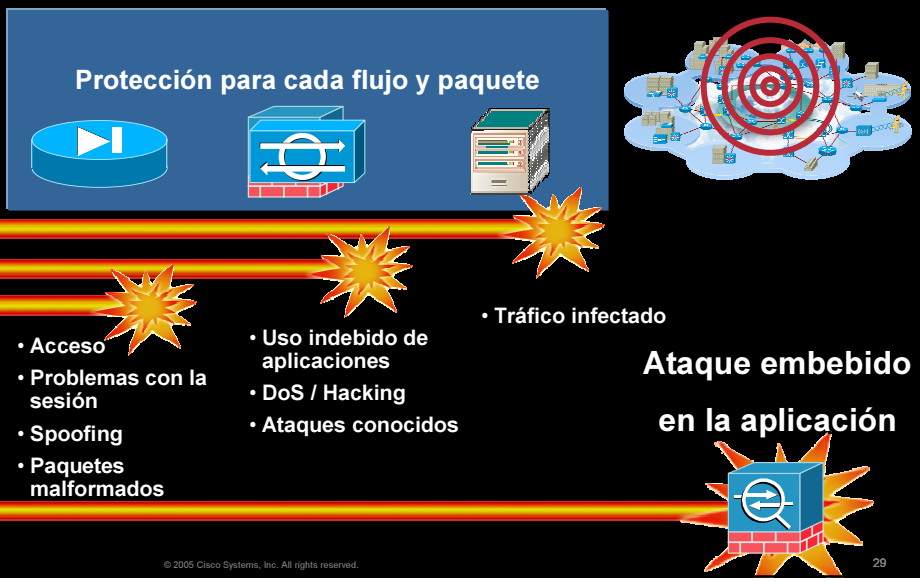
Cisco.com



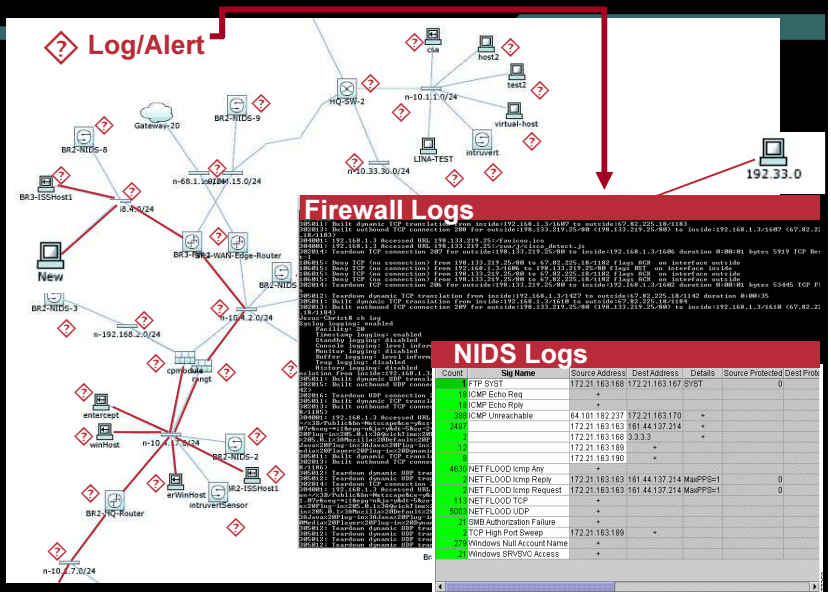
28

4. Inspección de aplicaciones (cont)

Cisco.com



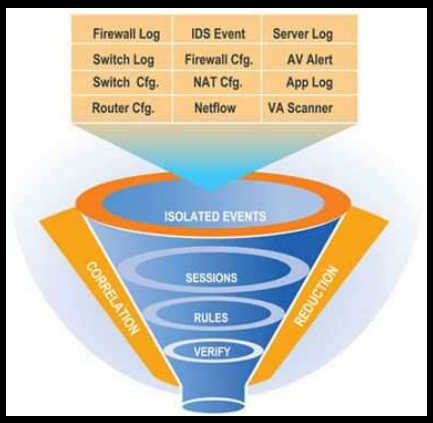
4. Inspección de aplicaciones (cont)

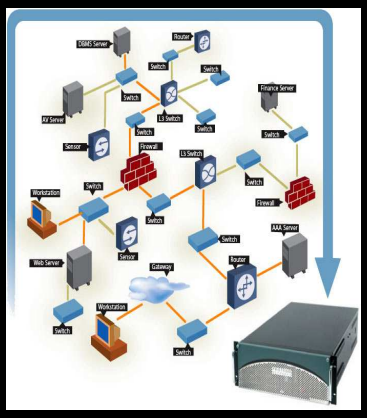


5. Contención de ataques

Cisco.com

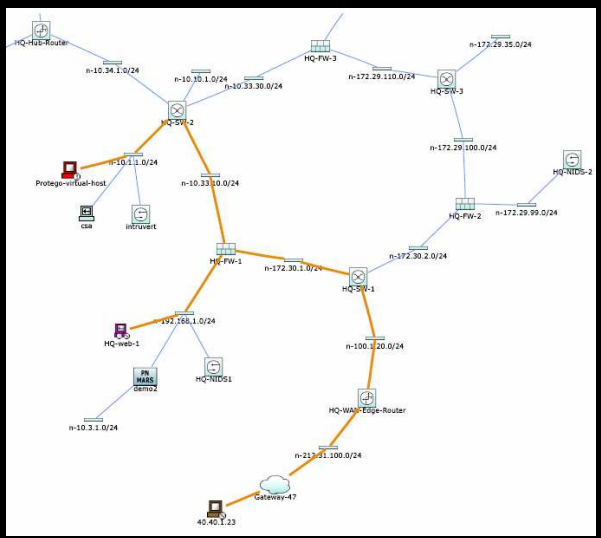
- **Problema tradicional:** No hay rápida visibilidad de ataques y aislar sistemas o mitigar efectos es difícil, consume mucho tiempo y es un proceso manual.





5. Contención de ataques (cont)

Cisco.com

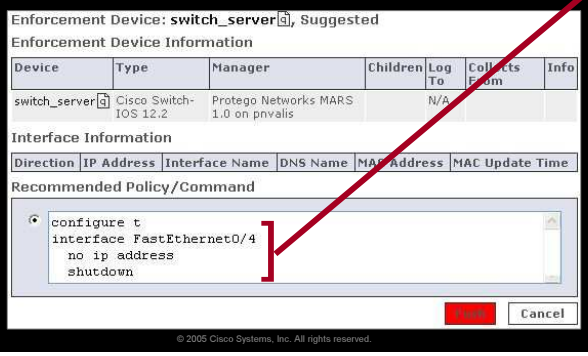


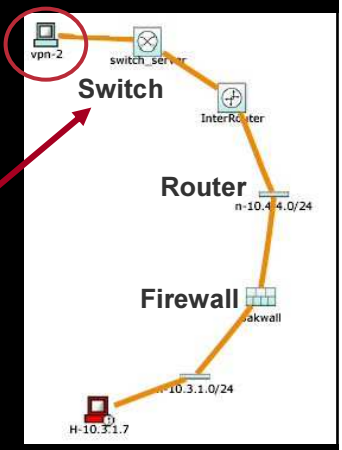
- Visualización del vector de ataque!!
- Es necesario información topológica.
- Equipos que hacen NAT deben ser tenidos en cuenta.
- SNMP, SSH a los equipos de red para tener información.

5. Contención de ataques (cont)

Cisco.com

- Gracias a la información topológica y de cada equipo de red, es posible ubicar incluso el puerto al que está conectado la máquina que está enviando el ataque. Automáticamente el sistema podría mitigar. Hay que manejarlo con cuidado.



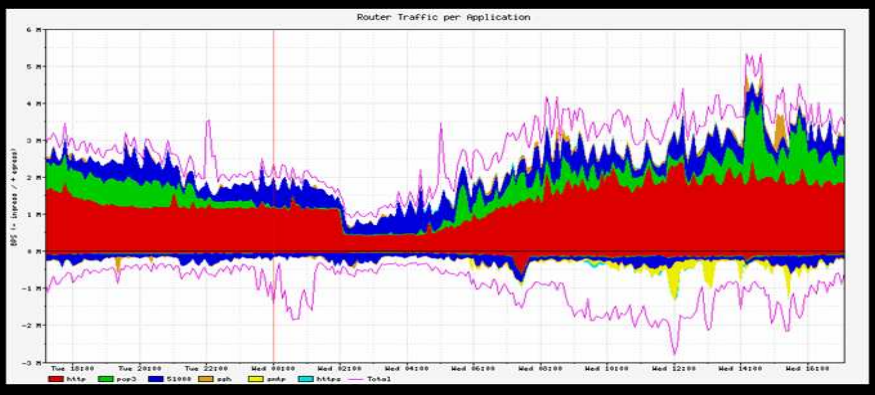


5. Contención de ataques (cont)

Flujo de aplicaciones (Netflow)

Cisco.com

Es posible identificar anomalías de tipo de tráfico que se salga del promedio de día-hora. Posibles falsos positivos pero muy útil.



5. Contención de ataques (cont)

Cisco.com

Al salir una nueva amenaza, los sistemas de AV pueden tardar en promedio dos horas en tener una vacuna. Sin embargo, en un tiempo promedio de 15 minutos pueden crear una política que ayude a mitigar el riesgo de su propagación. La red juega un papel clave. El proceso podría ser automático.

```
! --- block ICMP. Blaster example
access-list 115 deny icmp any any echo
access-list 115 deny icmp any any echo-reply
! --- block vulnerable protocols
access-list 115 deny tcp any any eq 135
access-list 115 deny udp any any eq 135
access-list 115 deny udp any any eq 69
access-list 115 deny udp any any eq 137
access-list 115 deny udp any any eq 138
access-list 115 deny tcp any any eq 139
```

```
access-list 115 deny udp any any eq 139
access-list 115 deny tcp any any eq 445
access-list 115 deny tcp any any eq 593

Allow all other traffic -- insert
! --- other existing access-list entries here
access-list 115 permit ip any any
!
interface <interface>
ip access-group 115 in
ip access-group 115 out
```


6. Protección en el día cero

Cisco.com

- **Problema tradicional:** Sistemas vulnerables a ataques de día cero. (desconocidos). Un sistema reactivo que necesite actualización de firmas no alcanza a proteger.

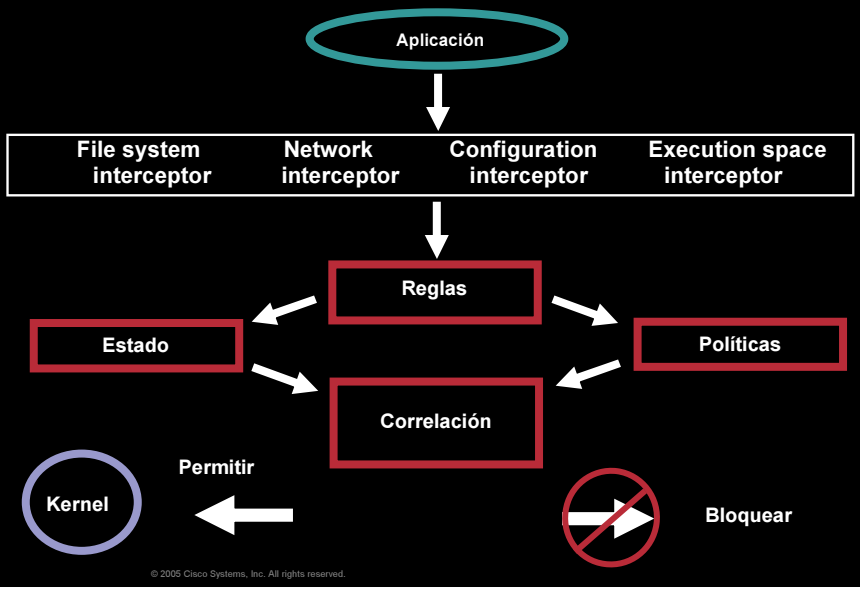
6. Protección en el día cero (cont)

Cisco.com

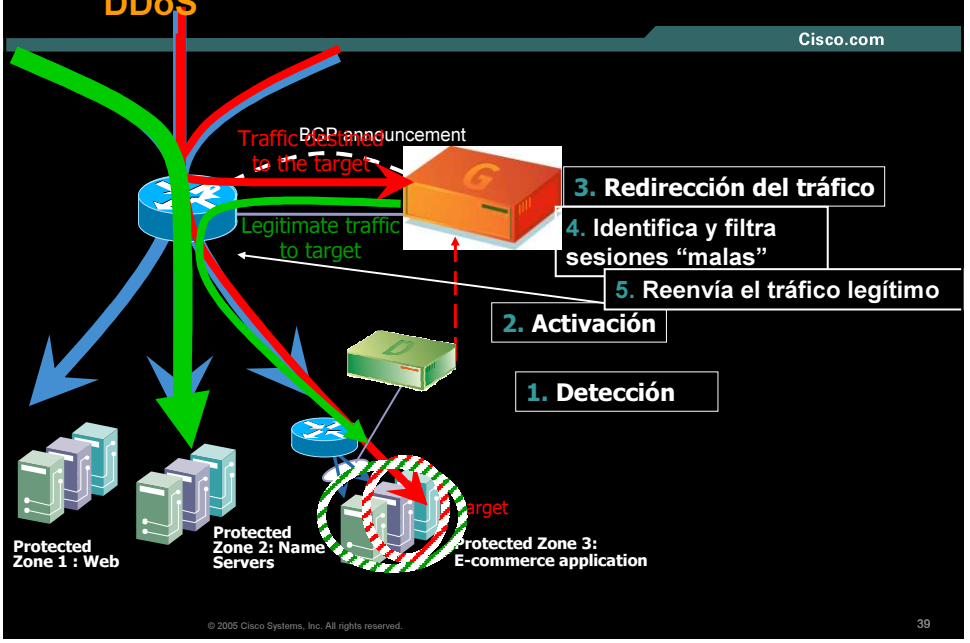
- Fases de un ataque (5 Ps)
  - Probar
  - Penetrar
  - Persistir
  - Propagar
  - Paralizar

6. Protección en el día cero (cont)

Cisco.com



6. Protección en el día cero (cont)
DDoS

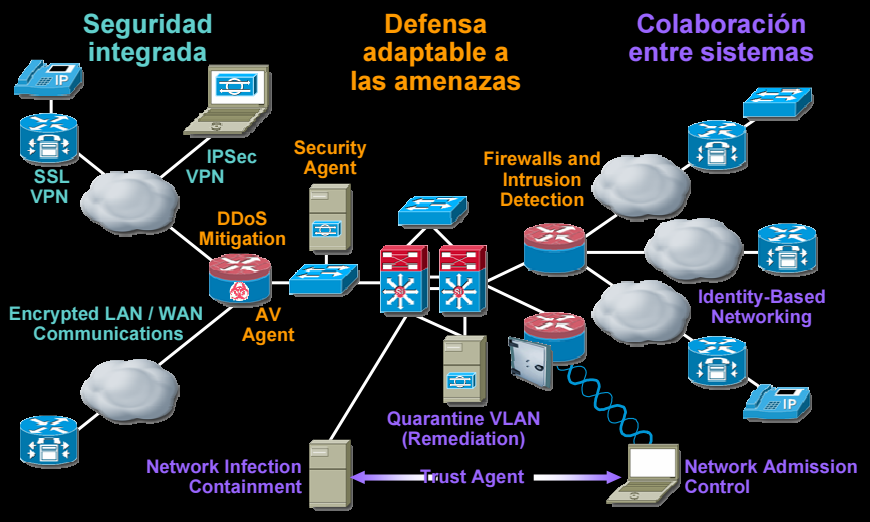


CISCO SYSTEMS

CONCLUSIONES

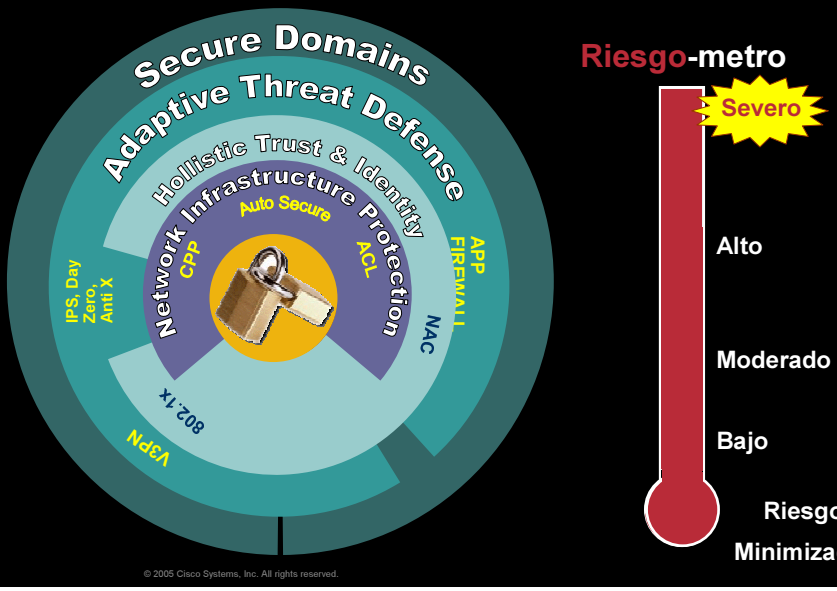
Redes auto-protegidas: Arquitectura integral

Cisco.com



Redes auto protegidas reducen el *Riesgo*

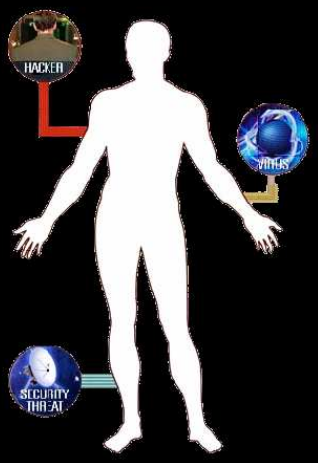
Cisco.com



Analogía:
Sistema inmunológico del cuerpo humano

Cisco.com

- La infraestructura de TI y las redes necesitan operar como un ser viviente
- La presencia de virus es un hecho de vida, y continuara presentando desafios
- El cuerpo humano sigue funcionando aun cuando acarreamos virus o tenemos alguna enfermedad



Valor de un Sistema Integrado de Seguridad
Hoy en día, seguridad no es opcional… *Es una necesidad*

Cisco.com

Seguridad como opcional

Seguridad es un agregado
Costos no eficientes
No enfoca en prioridad principal

Seguridad integrada de un sistema

Seguridad incorporada
Colaboración Inteligente
Seguridad apropiada
Enfoque directo en prioridad principal

CISCO SYSTEMS

GRACIAS!!