Cisco Self-Defending Networks

Tercer encuentro Tecnológico

Gobierno de Chile / Ministerio del Interior

Donald Bennett
Cisco Systems Chile
dobennet@cisco.com

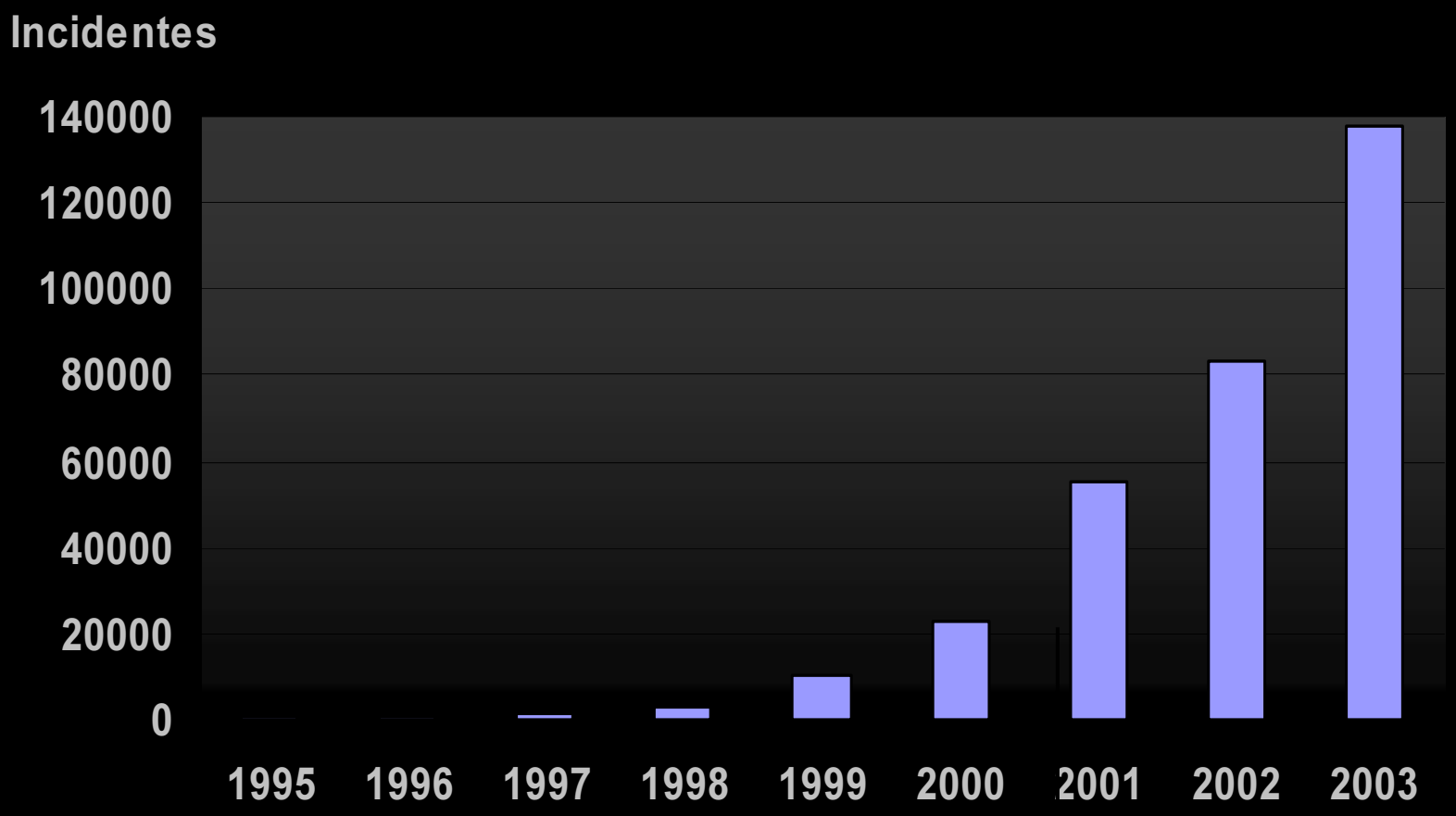
Abril 2005

Necesidades de las Empresas

- Responder más rápido y proactivamente a los cambios en las condiciones de los negocios
- Invertir en Tecnología Informática para estar “en ofensiva”
- Reducir la complejidad de sistemas y procesos

> Afrontar el diseño de la red en forma innovativa puede ayudar a resolver todos estos desafíos

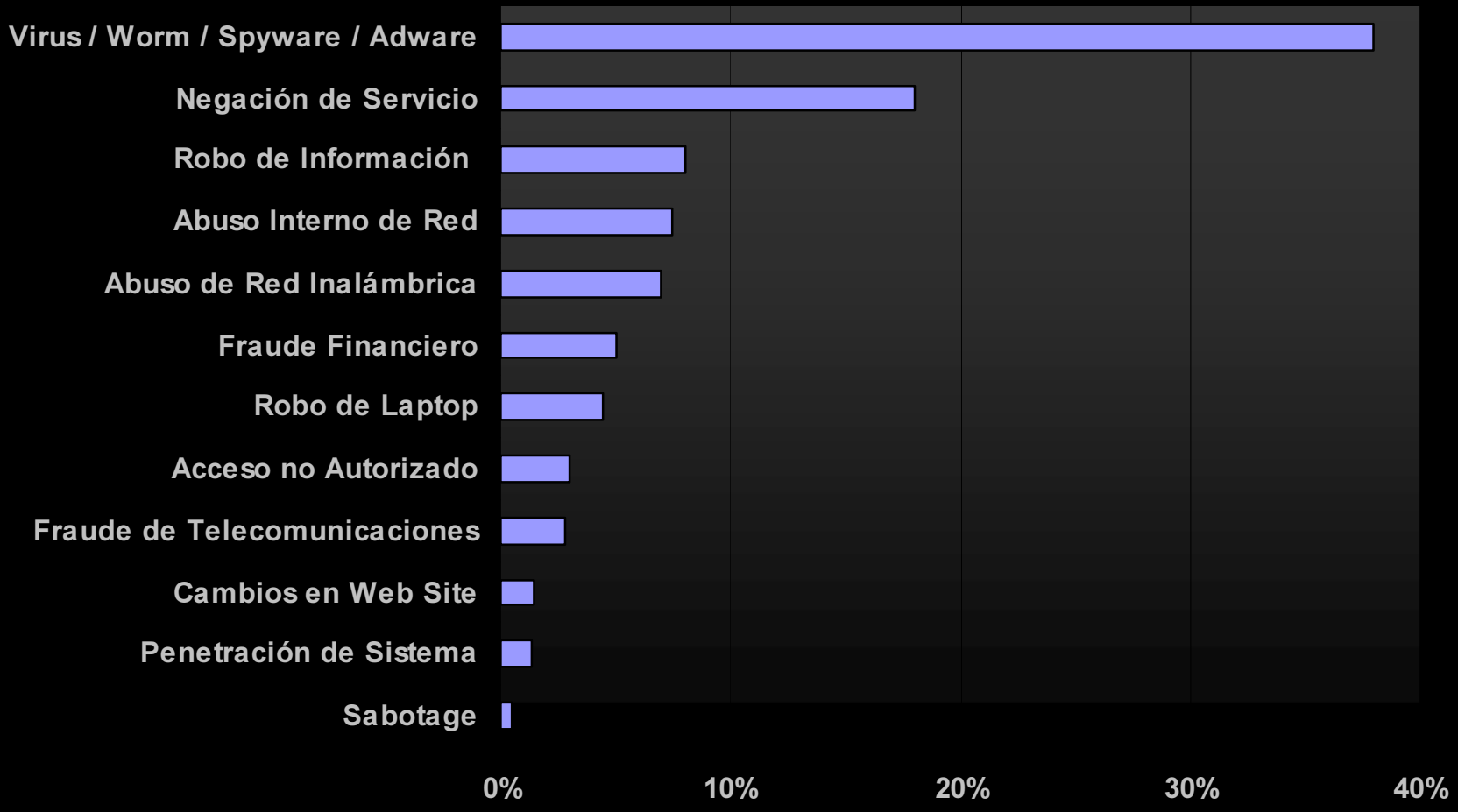
Incidentes de Seguridad en Alza



Fuente: CERT: Carnegie Mellon Software Engineering Institute. IDC

Incidentes de Seguridad Costosos

Perdidas por Incidentes de Seguridad



Fuente: CSI/FBI Computer Crime and Security Survey 2004

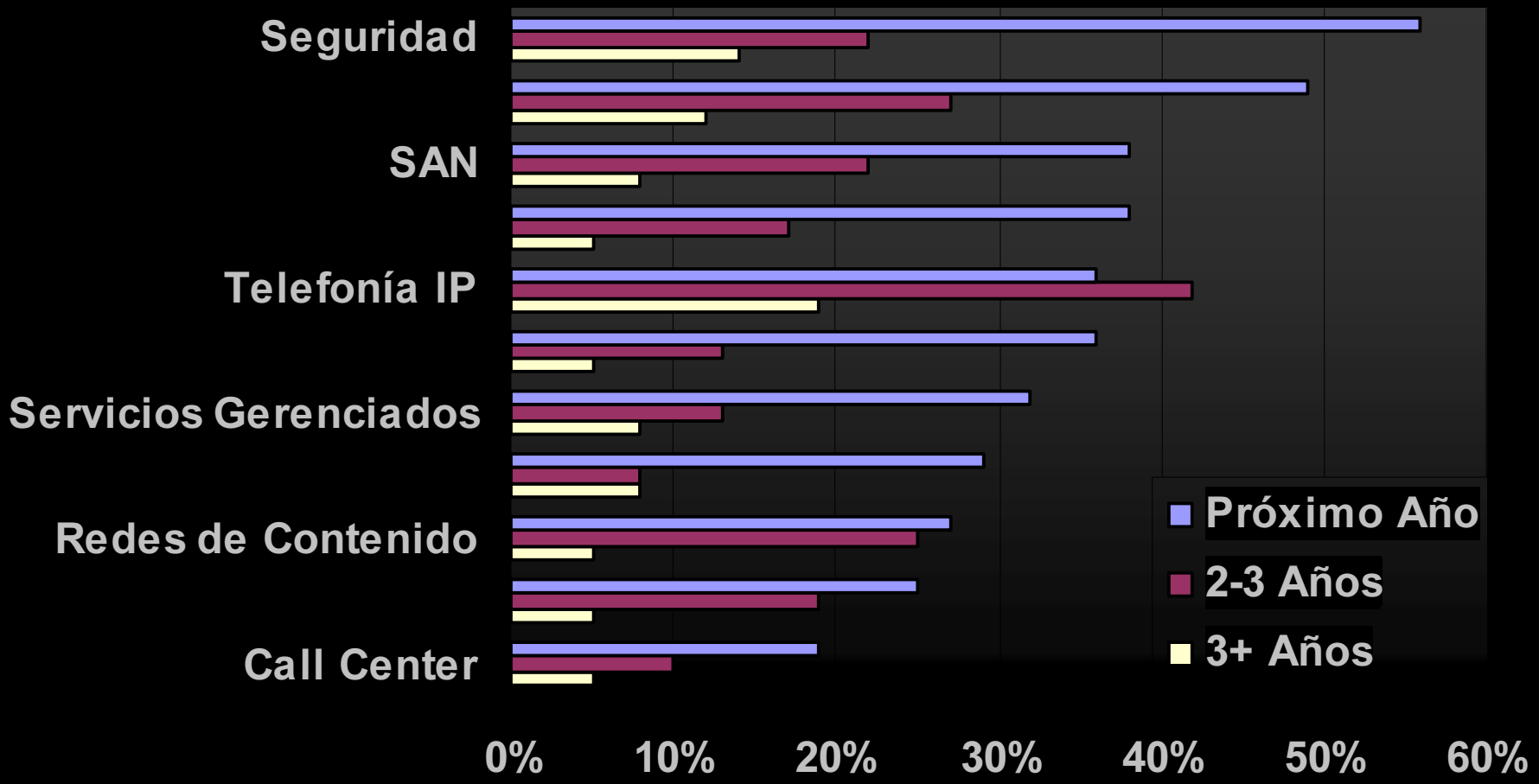
Seguridad… Prioridad en las Empresas

Tendencias de Negocios en el 2004

	2002	2003	2004
Seguridad / Disrupción de negocio	-	12	1
Costos operativos	1	1	2
Protección de datos y privacidad	4	2	3
Crecimiento de ventas	-	-	4
Uso de informacion en productos / servicios	-	-	5
Recuperación económica	-	-	6
Datos consolidados de clientes	3	5	7
Innovación más rapida	6	3	8
Transparencia en los reportes	-	7	9
Mitigación de riesgo	-	4	10

Fuente: Gartner Top Ten Business Trends. 2004

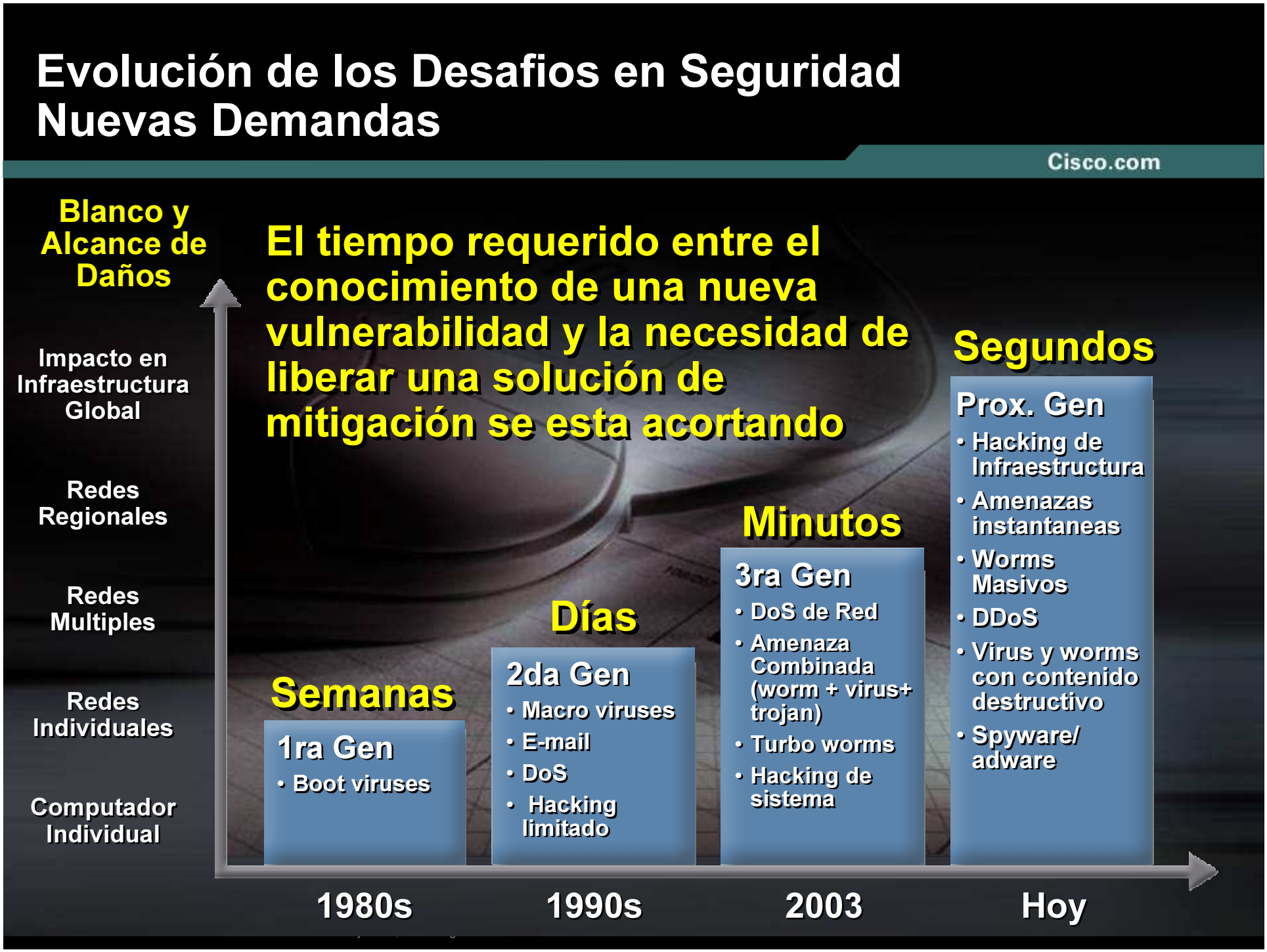
Encuesta CIO… Inversión en Seguridad
Inversión Futura en Tecnologias de Red



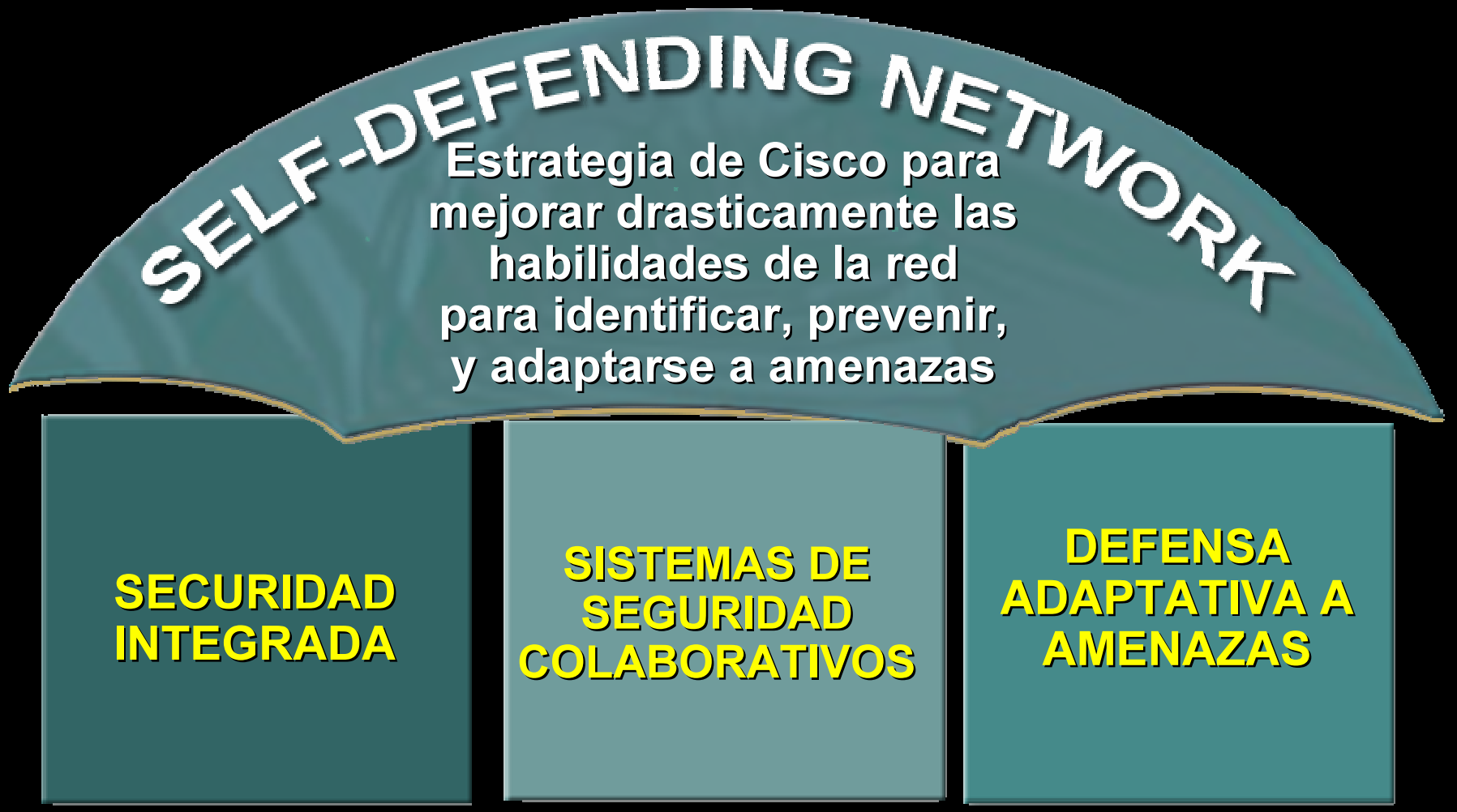
Fuente: Cisco CIO Survey. FY2004

Evolución de los Desafios en Seguridad Nuevas Demandas

Cisco.com



Estrategia de Cisco: Red Auto-Defensiva



Evolución de la Estrategia de Seguridad de Cisco

Productos Puntuales

- Multiples Dispositivos de Securidad
- Software de gerenciamiento separado

SDN Fase III *"Defensa Adaptativa a Amenazas"*

- Alerta mutua entre servicios de seguridad e inteligencia de la red
- Incrementa la efectividad de seguridad y posibilita respuesta proactiva
- Consolida servicios, mejora eficiencia operativa
- Reconocimiento de aplicación y entrega / optimización segura de datos de aplicación

SDN Fase II *"Sistemas de Seguridad Colaborativos"*

- Seguridad se convierte en un sistema de red: Puntos extremos + Red + Políticas
- Servicios multiples y dispositivos trabajando en coordinación para mitigar ataques con gerenciamiento activo
- NAC, IBNS, SWAN

SDN Fase I *"Seguridad Integrada"*

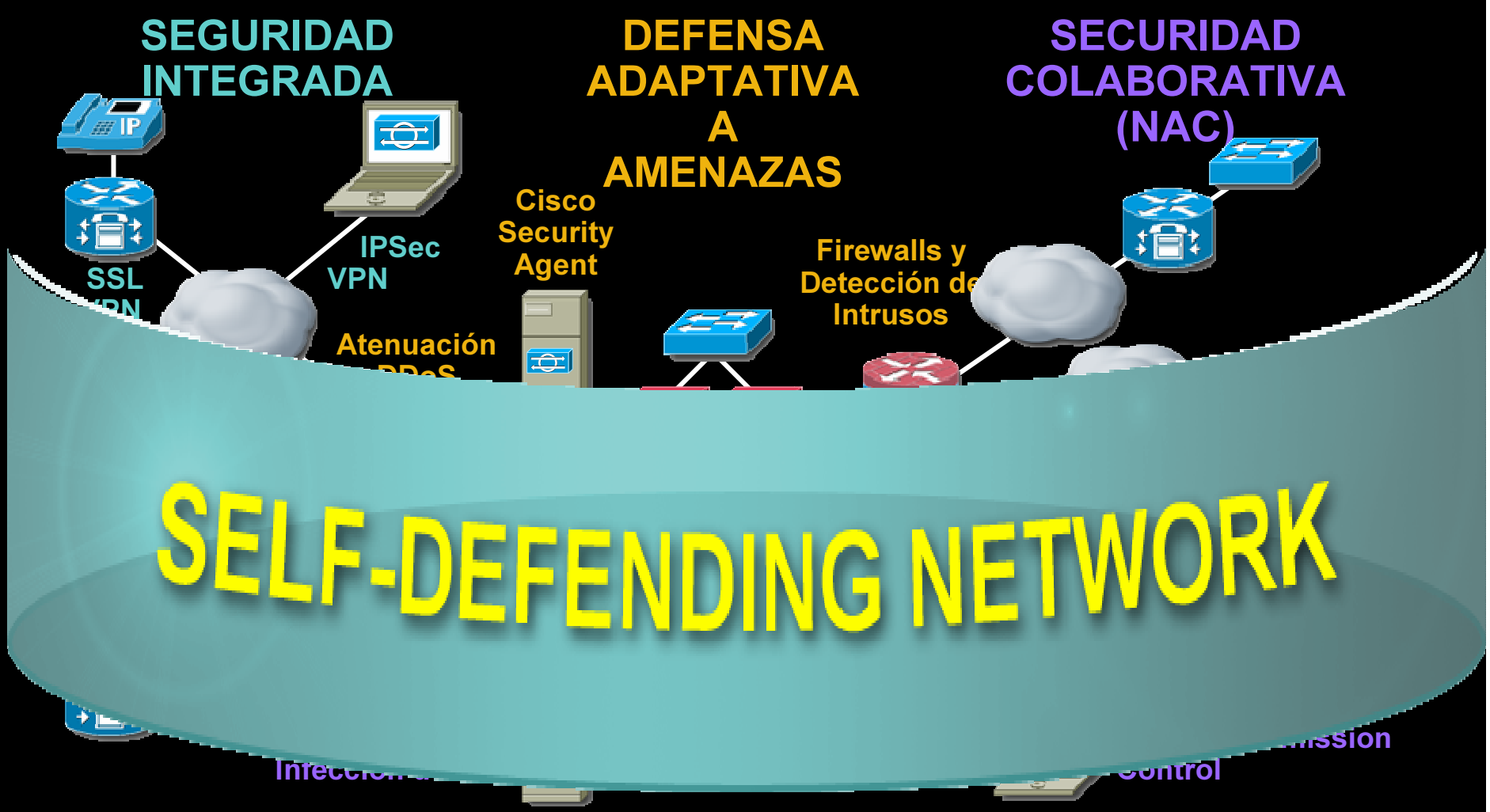
- Cada elemento de red como punto de defensa
  Routers, Switches, Appliances. Endpoints
- Conectividad Segura (V3PN, DMVPN), Defenza de Amenazas, Identidad y Confianza
- Protección de Red

Modelo de red basado en el cuerpo humano

- La infraestructura de TI y las redes necesitan operar como un ser viviente
- La presencia de virus es un hecho de vida, y continuará presentando desafios
- El cuerpo humano sigue funcionando aún cuando acarreamos virus o tenemos alguna enfermedad
- La visión de seguridad de Cisco y su estrategia esta basada en el sistema inmunológico humano

Visión de Seguridad: Diseño de Arquitectura de Sistema

Cisco.com



"5–7 Años para Diseñar la Arquitectura"

Defensa Adaptativa a Amenazas (ATD)

La Convergencia de Tecnologias Incrementa Efectividad y Eficiencia

Defensa Adaptativa a Amenazas en Acción

Productos, Servicios y Ejemplo de Arquitectura

Cisco.com

Control de Acceso, Inspección de Paquetes
Servicios de Firewall

Inteligencia de Aplicación, Inspección de contenido, Atenuación de Virus

Identidad, Virtualización, Segmentación QoS, Visibilidad de Tráfico

Inspección Ap., Control de uso, Control de Web
Seguridad de Aplicación

Defensa de Contenido/Malware, Detección de Anomalias
Anti-X Defenses

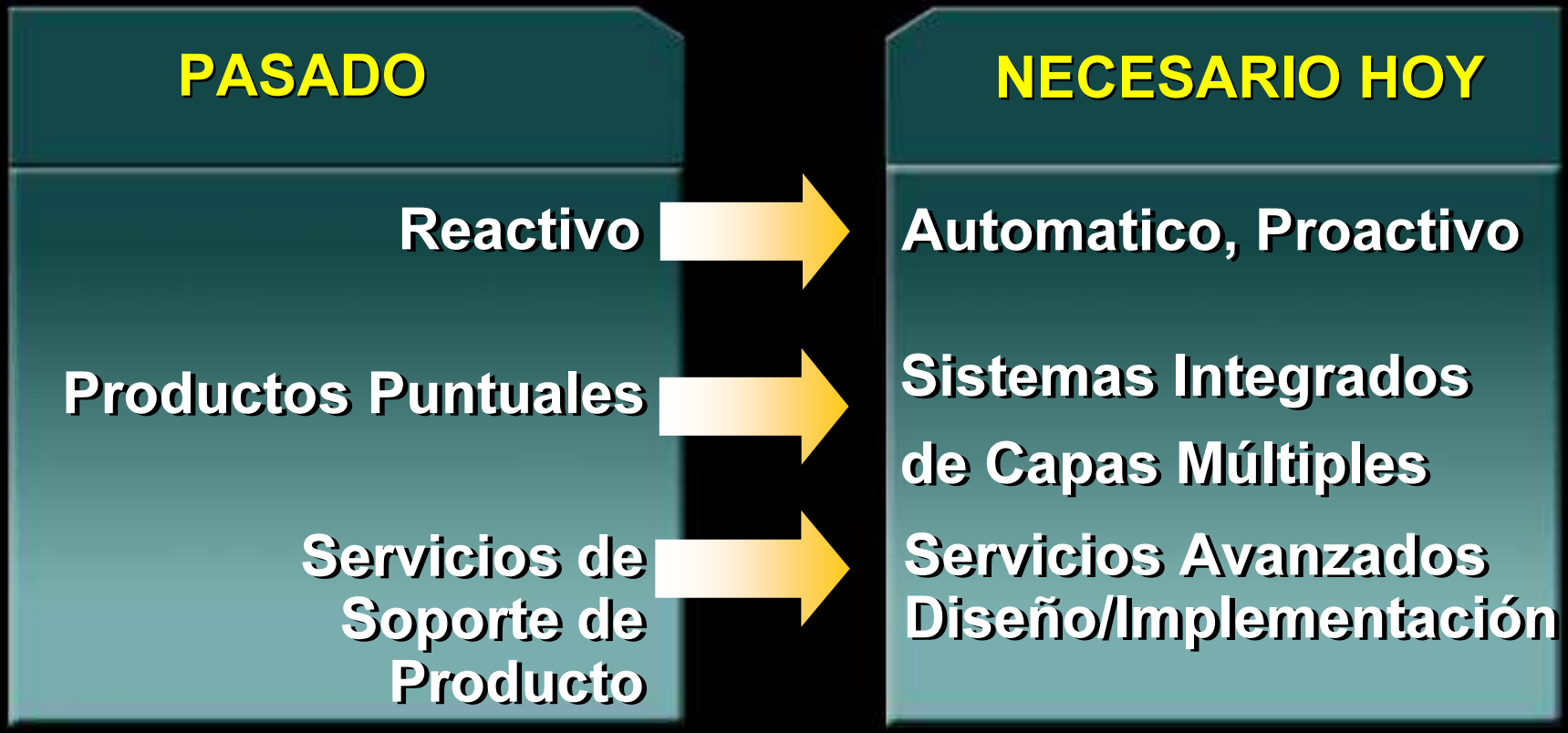
Control de Admisión/Tráfico, Respuesta Proactiva
Contención y Control

Defensa de Adaptativo a Amenazas

Anuncios de Productos

Productos	Application Security	Anti-X	Containment & Control
IPS 5.0	• Multi-Vector Threat Identification	• Malware, virus, worm mitigation	• Accurate Prevention Technologies for In-Line IPS
VPN 3000 Concentrator 4.7	• SSL VPN Tunnel Client • Fully Clientless Citrix	• Cisco Secure Desktop	• Cisco NAC
IOS 12.3(14)T	• Application Inspection/ Control for IOS Firewall	• Enhanced In-Line IPS	• Network Foundation Protection, Virtual Firewall, IPSec Virtual Interface
PIX 7.0	• Application Inspection/ Control for Firewall • Enhanced VoIP Security		• Virtual firewall, QoS, transparent firewall, IPv6
Cisco Security Agent 4.5		• Spyware mitigation • System inventory/auditing	• Context-based policies
Catalyst DDoS Modules		• Anomaly Guard Module • Traffic Anomaly Detector	
Cisco MARS			• Event correlation for proactive response
Cisco Security Auditor			• Network-wide security policy auditing

Las Defensas del Pasado no son obstáculo contra las Amenazas de Hoy



Necesidad de Sistemas Colaborativos y Adaptativos

Valor de un Sistema Integrado de Seguridad

Seguridad no es más opcional… *Es una necesidad*

Seguridad como opcional

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

Seguridad integrada de un sistema

- Seguridad incorporada
- Colaboración Inteligente
- Seguridad apropiada
- Enfoque directo en prioridad principal

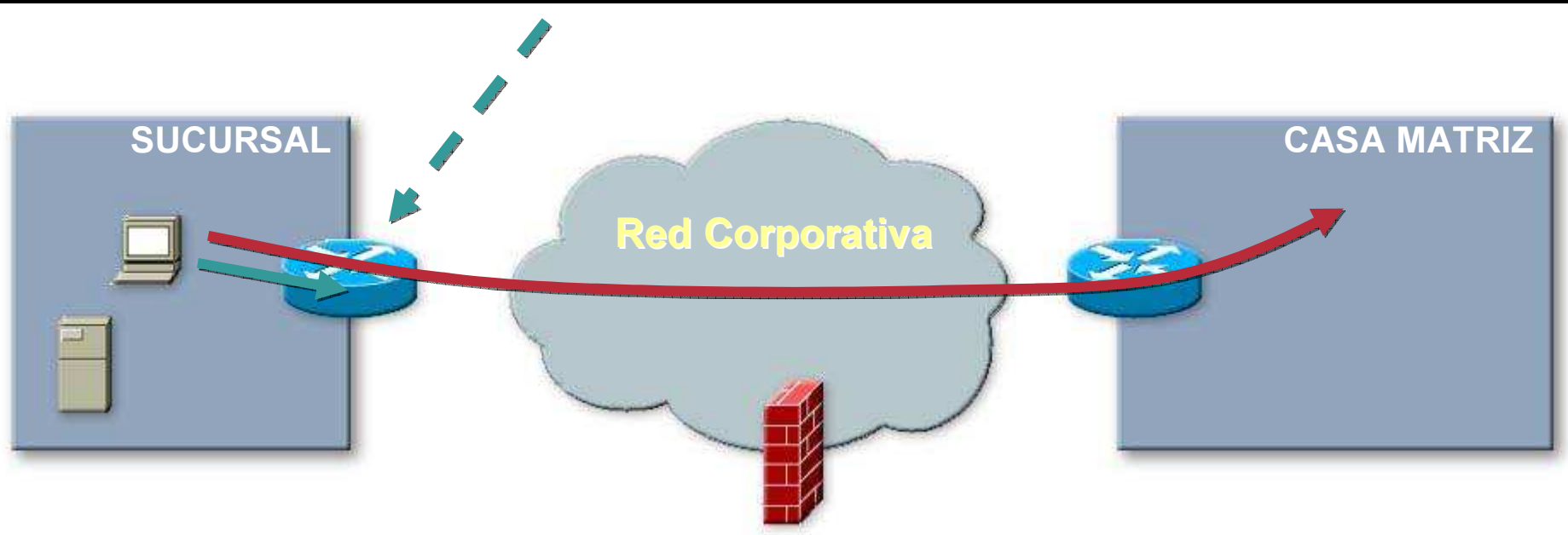
“Network Admission Control (NAC)”

como ejemplo de

“Sistemas de Seguridad Colaborativos”

¿ Qué sucede realmente en nuestras redes ?

1. Una Estación de Trabajo “Non-compliant” intenta una conexión
2. Router permite la conexión
3. La “infección” se propaga; todos los Servidores y Estaciones de Casa Matriz quedan expuestos

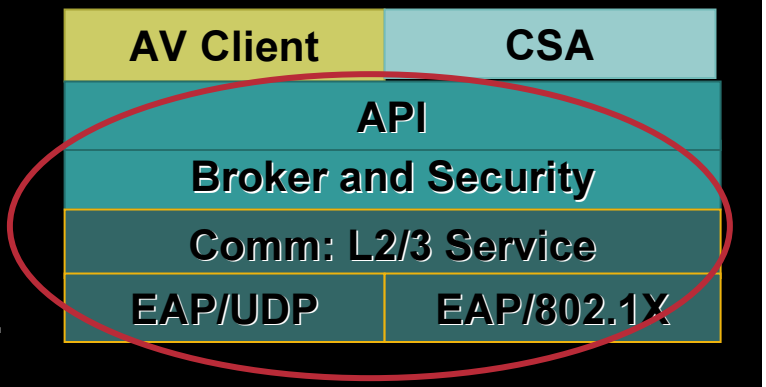


Cuáles son nuestros problemas asociados a la seguridad a nivel de hosts ?

- Virus y gusanos continúan irrumpiendo / interrumpiendo los negocios
- Ataques del tipo “día-cero” (Day-zero) hacen que las soluciones reactivas sean poco eficientes
- Tecnologías puntuales (ejemplo: AV, HIPS) tienden a preservar la disponibilidad de los hosts en lugar de la disponibilidad de la Red y la resistencia de la empresa
- Servidores y Estaciones de Trabajo no-complaint (con AV y parches de Sistema Operativo desactualizados) son difíciles de detectar y de contener su ingreso a la Red
- La localización de sistemas infectados es muy intensiva en recursos humanos y tiempo

Programa NAC – Anuncio público el 18-Nov-2003

- Cisco está liderando la arquitectura, especificaciones, y pautas de NAC.
- Los patrocinadores iniciales del programa NAC incluye a los principales fabricantes de aplicaciones Anti-Virus: McAfee, Symantec, y Trend Micro
- La aplicación "Cisco Security Agent (HIPS)" y los patrocinadores de soluciones AV utilizarán el agente "Cisco Trust Agent" para el control inteligente de admisión en las Estaciones de Trabajo, Servidores, PDAs, ...
- La primera fase del programa NAC, traducida en productos, partirá a fines del segundo trimestre calendario 2004, cubriendo los routers Cisco, y Sistemas Operativos Microsoft Win NT, 2000, y XP.
- Futuras extensiones de NAC:
  - Más elementos de red Cisco (Switches, APs, Concentradores VPN, NAS, Firewalls).
  - Mayor soporte de OSs y aplicaciones en Estaciones de Trabajo, Servidores, PDAs, ...
  - Más patrocinadores.

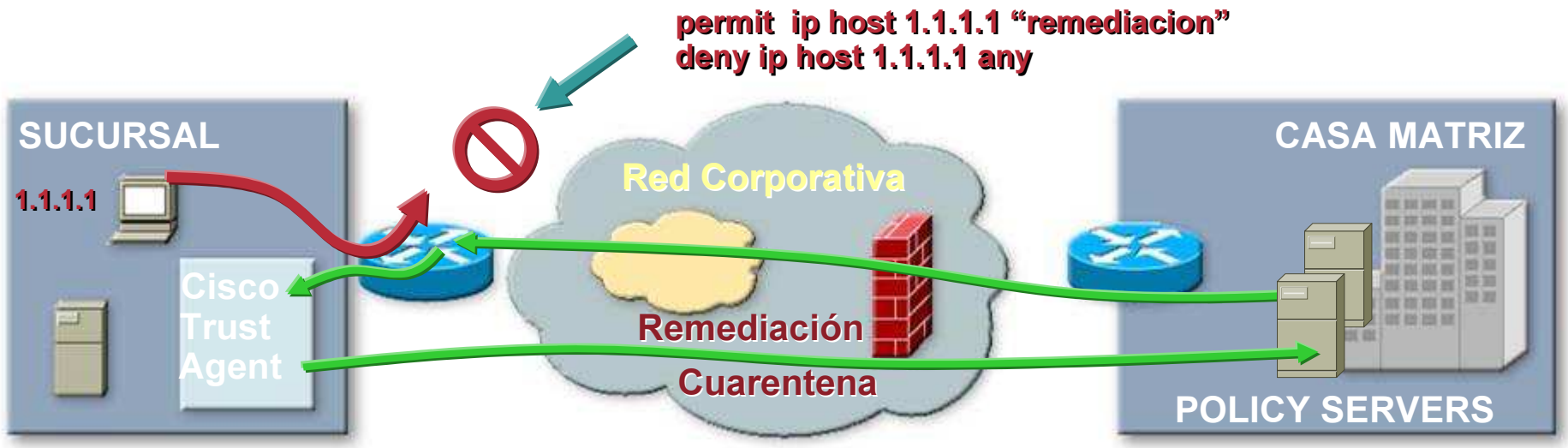


Cisco Trust Agent

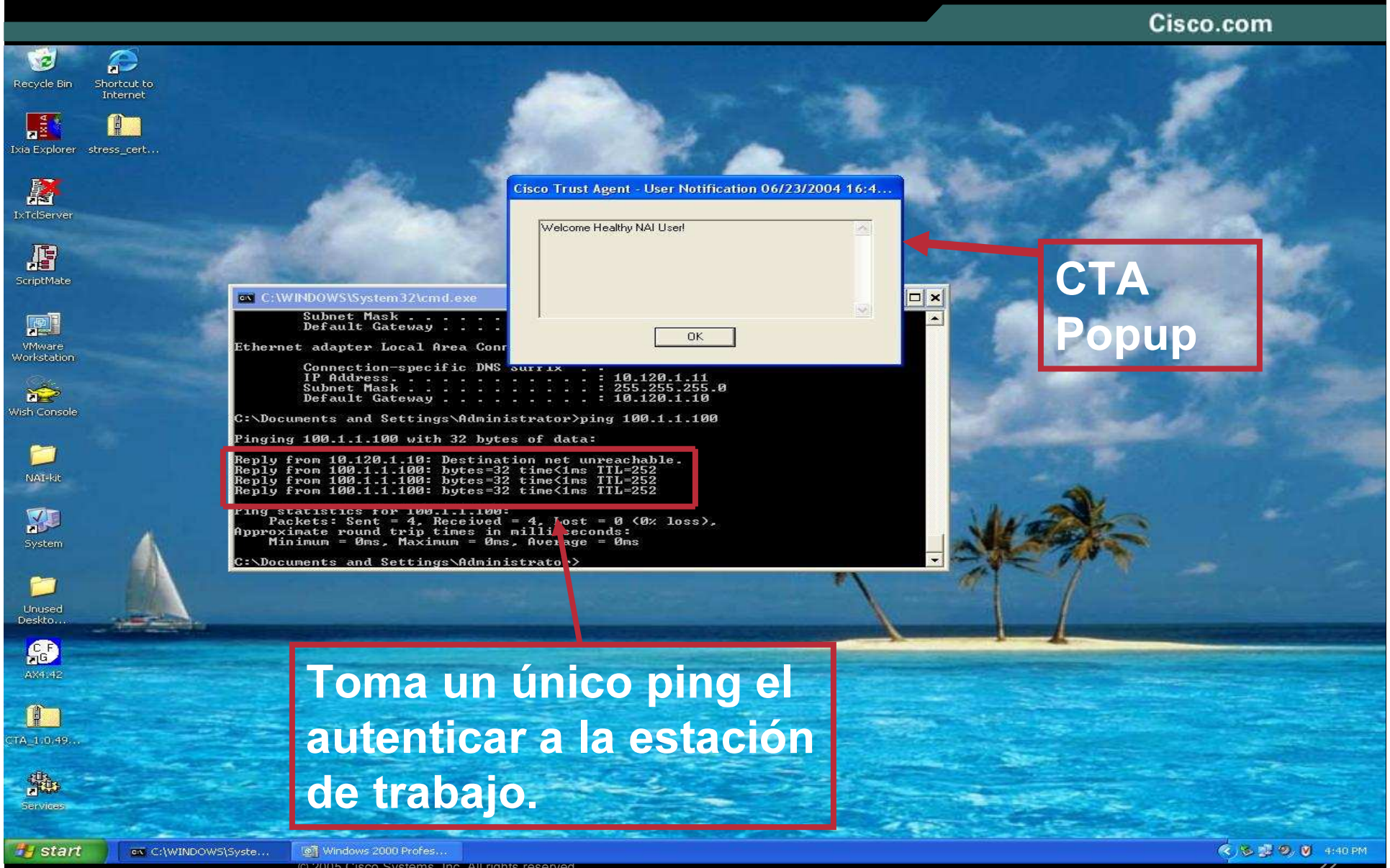
Cisco Network Admission Control:

Qué hace ?

1. Una Estación de Trabajo “Non-compliant” intenta una conexión
2. Cuarentena/ remediación
3. La “infección” es contenida; todos los Servidores y Estaciones de Casa Matriz están protegidos



Cliente NAC – Experiencia del Usuario Final

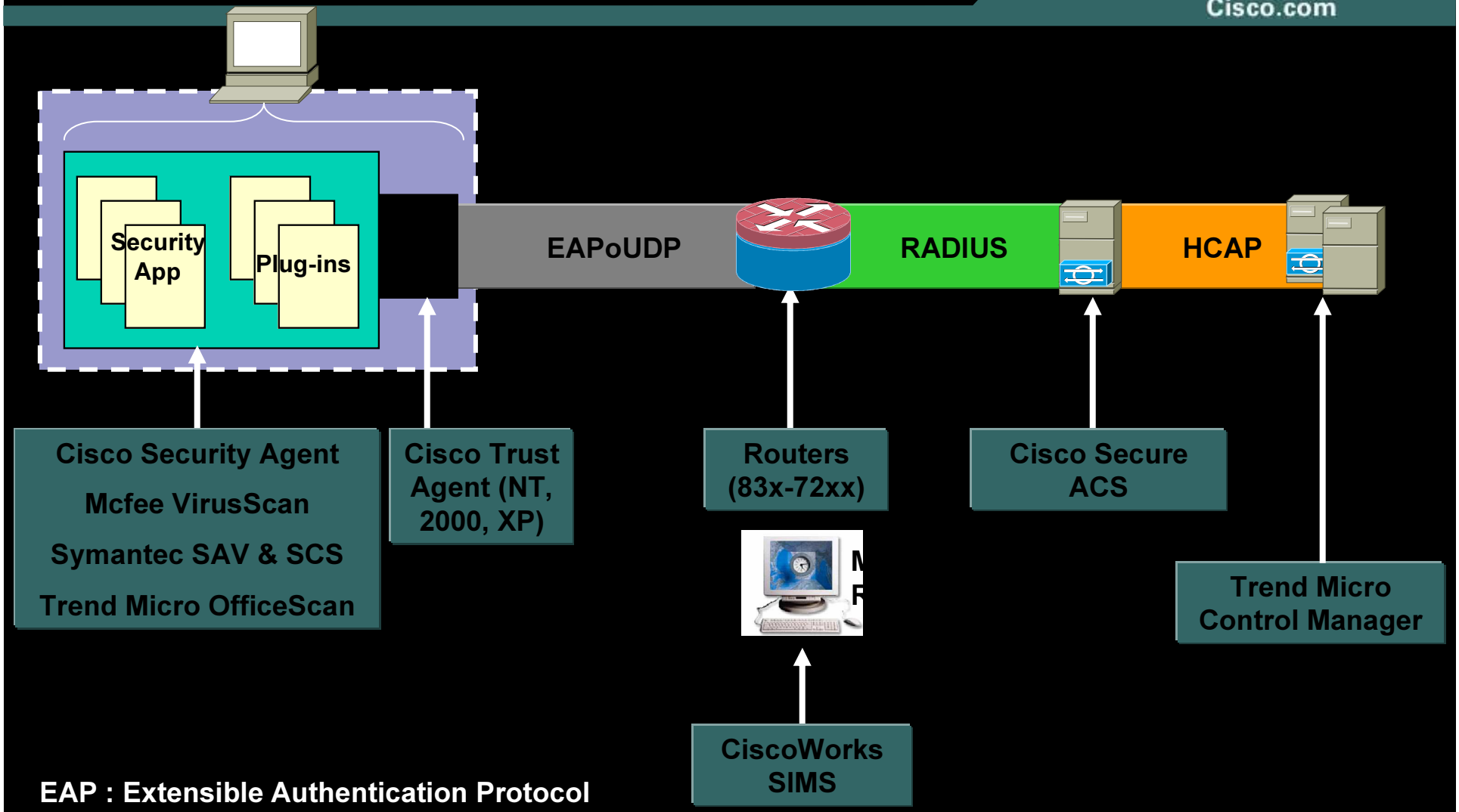


Funciones de Cisco Secure ACS 3.3

- Punto de Decisión de Políticas para NAC en versión 3.3
- Obtención de credenciales desde los endpoint
  - Establecer canal de comunicación seguro con el CTA
  - Solicitar y Recibir las credenciales de las aplicaciones (AV, ...) & Sistemas Operativos
- Ejecutar funciones AAA sobre las credenciales
  - Autenticar cada conjunto de credenciales
  - Cada una evaluada por CS ACS o Servidor del fabricante de la aplicación (ej: CSA en ACS, OfficeScan de TMCM)
  - ACS determina los derechos de autorización
  - Los menores derechos de todos los resultados de autenticación (Healthy + Checkup = Checkup)
  - Lista de Excepción, basada en direcciones MAC & IP
  - Audit log (recolectado por CiscoWorks SIMS)
- Enviar reglas de autorización al router, y realimentación al endpoint
  - ACL dinámicas y opcionalmente redirección URL
  - Posibilidad de enviar notificaciones por aplicación al endpoint, y también realimentación al usuario
  - Basado en la aplicación del fabricante, la retroalimentación puede gatillar remediación

Phase 1 : Componentes Lógicos

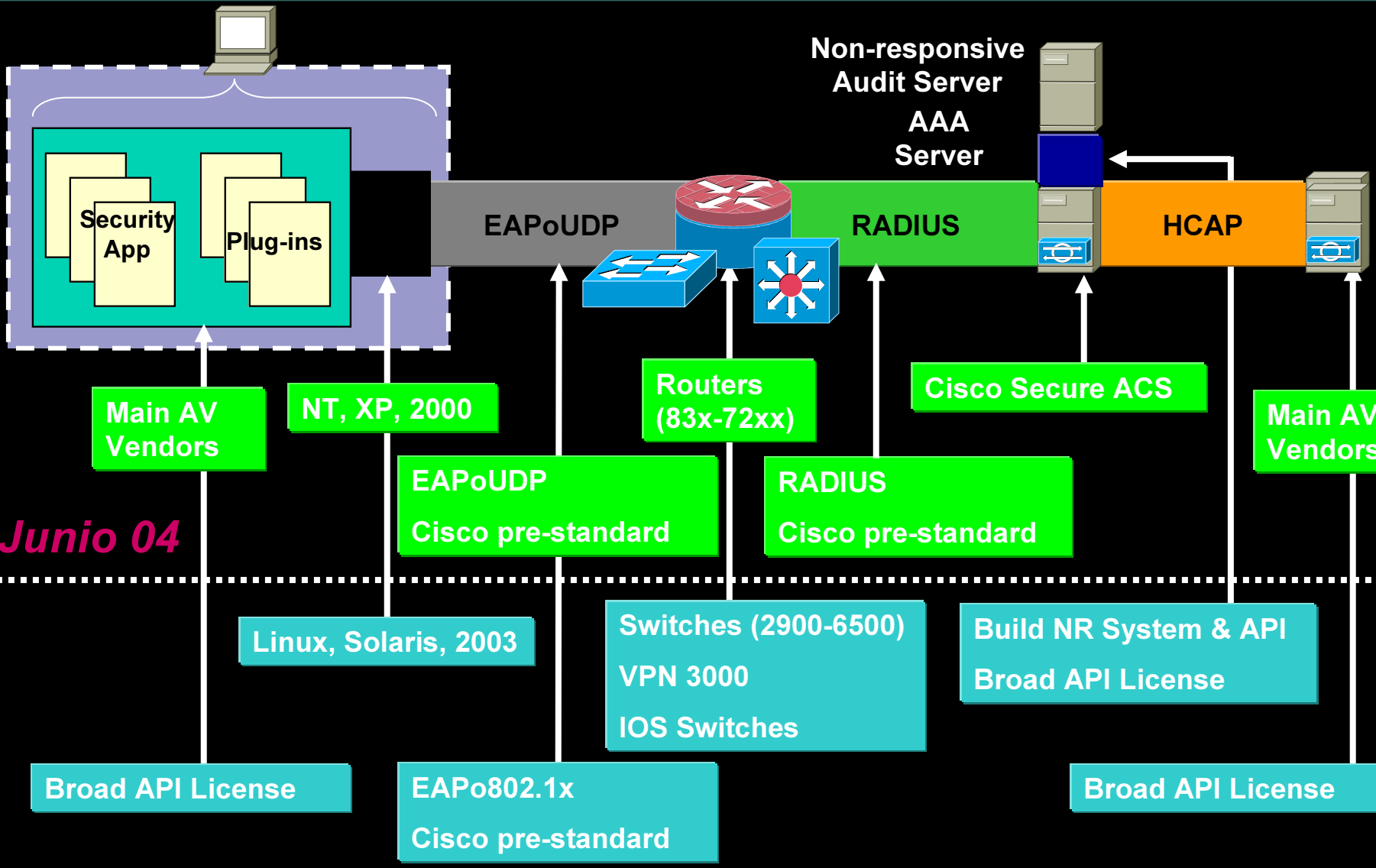
Junio 2004



EAP : Extensible Authentication Protocol

HCAP : Host Credential Authorization Protocol

Phase 2 : Componentes Lógicos



Current Program Participants

http://www.cisco.com/en/US/partners/pr46/nac/partners.html

Cisco.com

“Cisco Secure Desktop (CSD)”

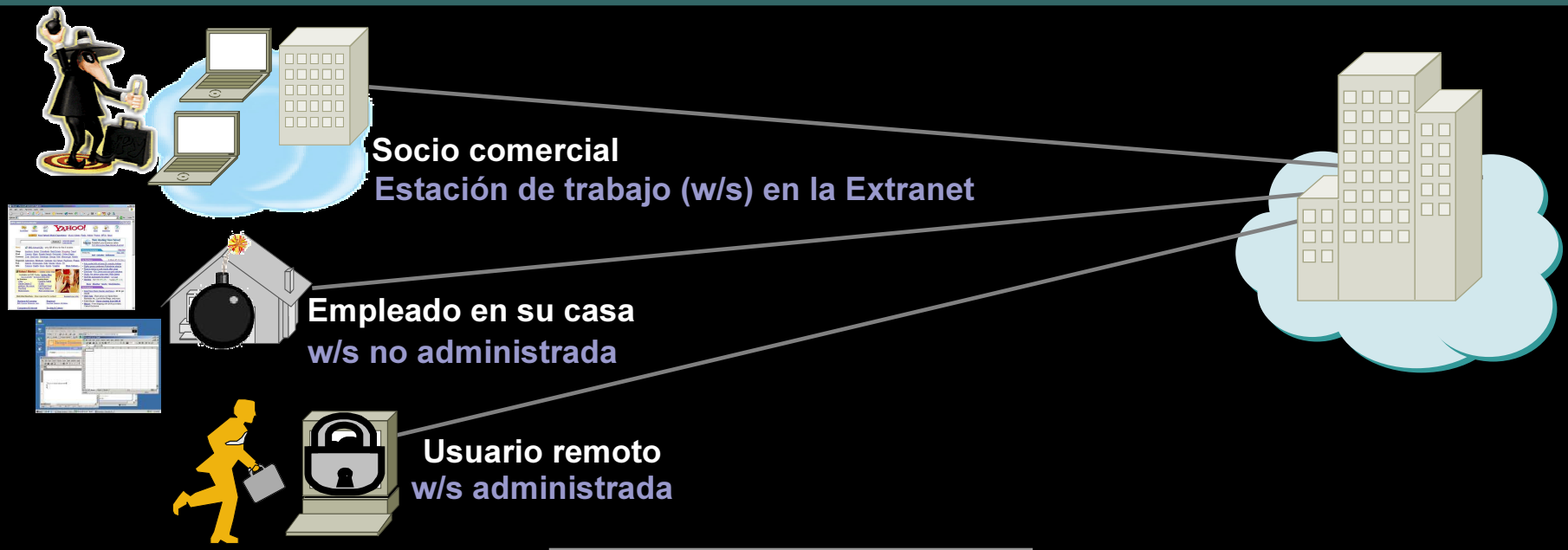
como ejemplo de

“Anti-X Defense”

Desafios a la Seguridad

SSL VPN trae consigo muevos puntos de ataque

Cisco.com



Antes sesión SSL VPN

- Quién es el propietario de la w/s?
- Cuál es el nivel de protección de la w/s: AV, firewall personal?
- Malware en ejecución?

Durante la sesión SSL

- Están los datos de la sesión protegidos?
- Las passwords ingresadas están protegidas?
- Alguna aplicación del tipo Malware?

Terminada la sesión SSL

- El browser almacenó páginas visitadas?
- El browser almacenó passwords?
- Se dejaron archivos descargados en la w/s?

Cisco Secure Desktop

Completa protección para la sesión SSL VPN

Evaluación completa pre-conexión:

- Estación de trabajo administrada o no ?
- Evaluación del nivel de protección de la w/s – firewall personal operacional, malware presente?

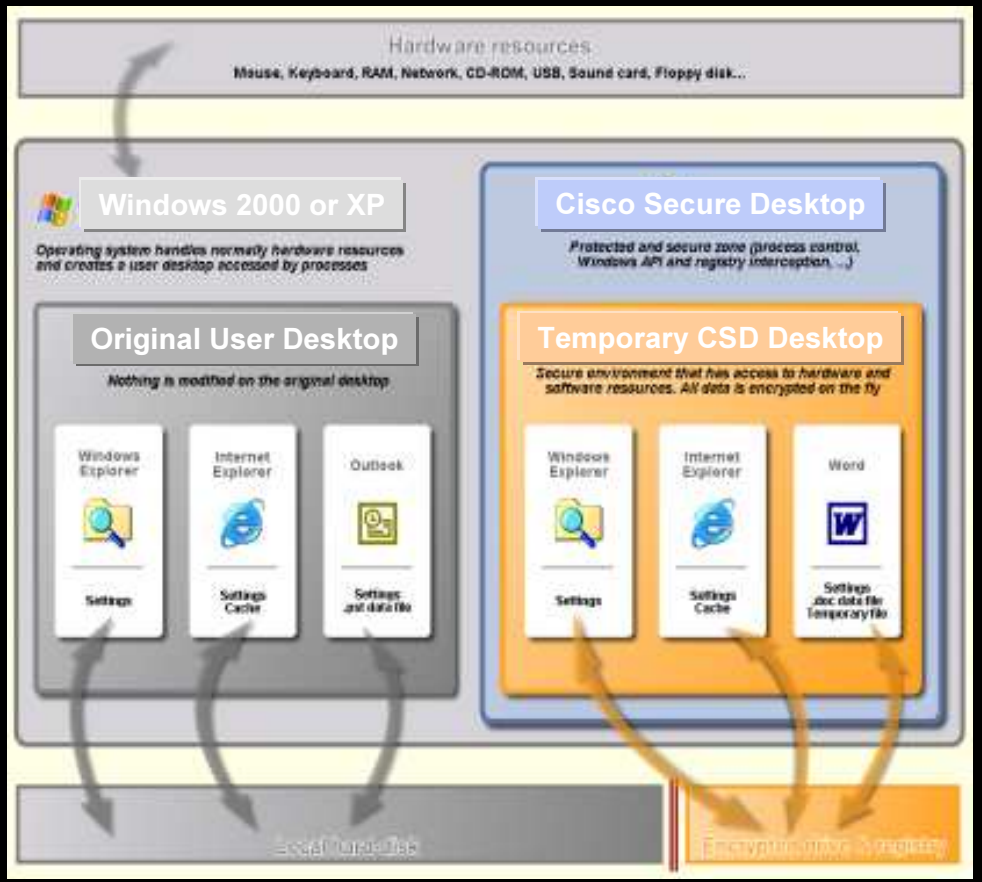
Completa protección de la Sesión:

- "Data sandbox" y encriptación protegen cada aspecto de la sesión
- Detección de Malware (trabaja con software de protección anti-spyware de Microsoft (free))

Limpieza completa terminada la sesión:

- Partición encriptada es "destruída" utilizando algoritmo DoD
- Cache, historia y cookies eliminadas
- Descarga de archivos y attachments de email son destruídos
- Auto-complete password overwrite

Trabaja con los permisos "Guest"
No se requieren privilegios "Admin"



Cisco Secure Desktop

Cómo trabaja ?

Paso 1: Un empleado se conecta desde cualquier punto de Internet

Paso 2: El Concentrador VPN "empuja / descarga" Cisco Secure Desktop a la estación de trabajo del empleado

Paso 3: CSD crea una partición en el disco duro ("encrypted sandbox") para que el empleado trabaje en ella.

Paso 4: Una vez realizado el logout el "Virtual Desktop" es erradicado y el usuario es notificado

Nota : CSD download and eradication is seamless to the user. If the user forgets to terminate the session auto-timeout will close the session and erase all session information