



Comunidad de Soporte de Cisco en  
Español Webcast en vivo:

# Identity Services Engine (ISE): Habilitando su red para BYOD (Bring Your Own Device)

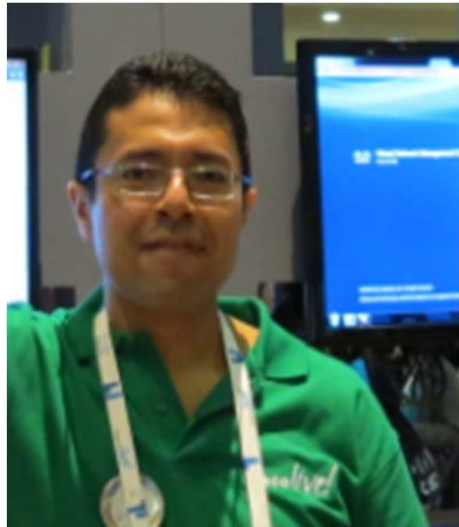
Israel Gonzalez  
Solutions Architect

Julio 2013

# Comunidad de Soporte de Cisco – Webcast en vivo

- El experto del día de hoy es: **Israel González**

Ahora puede hacerle sus preguntas sobre Tema



**Israel Gonzalez Quezada**

Solutions Architect

CCIE en R&S, SP & Security

# Identity Services Engine (ISE): Habilitando su red para BYOD (Bring Your Own Device)

## Panel de Expertos



**Mauricio Ramírez**

Solutions Architect

CCIE en Security

# Gracias por su asistencia el día de hoy

La presentación incluirá algunas preguntas a la audiencia.

Le invitamos cordialmente a participar activamente en las preguntas que le haremos durante la sesión





## Copia de la presentación

Si desea bajar una copia de la presentación de hoy, vaya a la liga indicada en el chat o use ésta dirección

<https://supportforums.cisco.com/docs/DOC-35002>



# Webcast pasados:

Usted puede encontrar todos los Webcast de la Comunidad de Soporte de Cisco en español en:

<https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/webcasts>



# Primera Pregunta

**¿Cuál es su experiencia trabajando con BYOD?**

- a) Sé lo básico**
- b) Tengo conocimiento teórico, no práctico**
- c) He tenido experiencia en laboratorio**
- d) Tengo experiencia en implementaciones en producción**

# ¡ Ahora puede realizar sus preguntas al panel de expertos!

Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora. Ellos empezarán a responder.





# Cisco Support Community Expert Series Webcast:

## ***Identity Services Engine (ISE): Habilitando su red para BYOD (Bring Your Own Device)***

Israel Gonzalez  
Solutions Architect

Julio 23, 2013




# Agenda

- ¿Porqué BYOD?
- Estrategia a seguir para la implementación de BYOD
- Cisco Identity Services Engine: BYOD y mejores prácticas
- Walkthru sobre los equipos

# ¿Porqué BYOD?



# ¿Qué es BYOD?



Es una política que permite a los empleados llevar sus dispositivos personales a su lugar de trabajo y utilizar estos dispositivos para acceder información restringida en su empresa de forma segura y controlada.

Como trabajabas  
dependía de....



Ahora depende de....





BYOD y Movilidad se han convertido en las principales prioridades para la mayor parte de las compañías.

# Enfoque a seguir para la implementación de BYOD

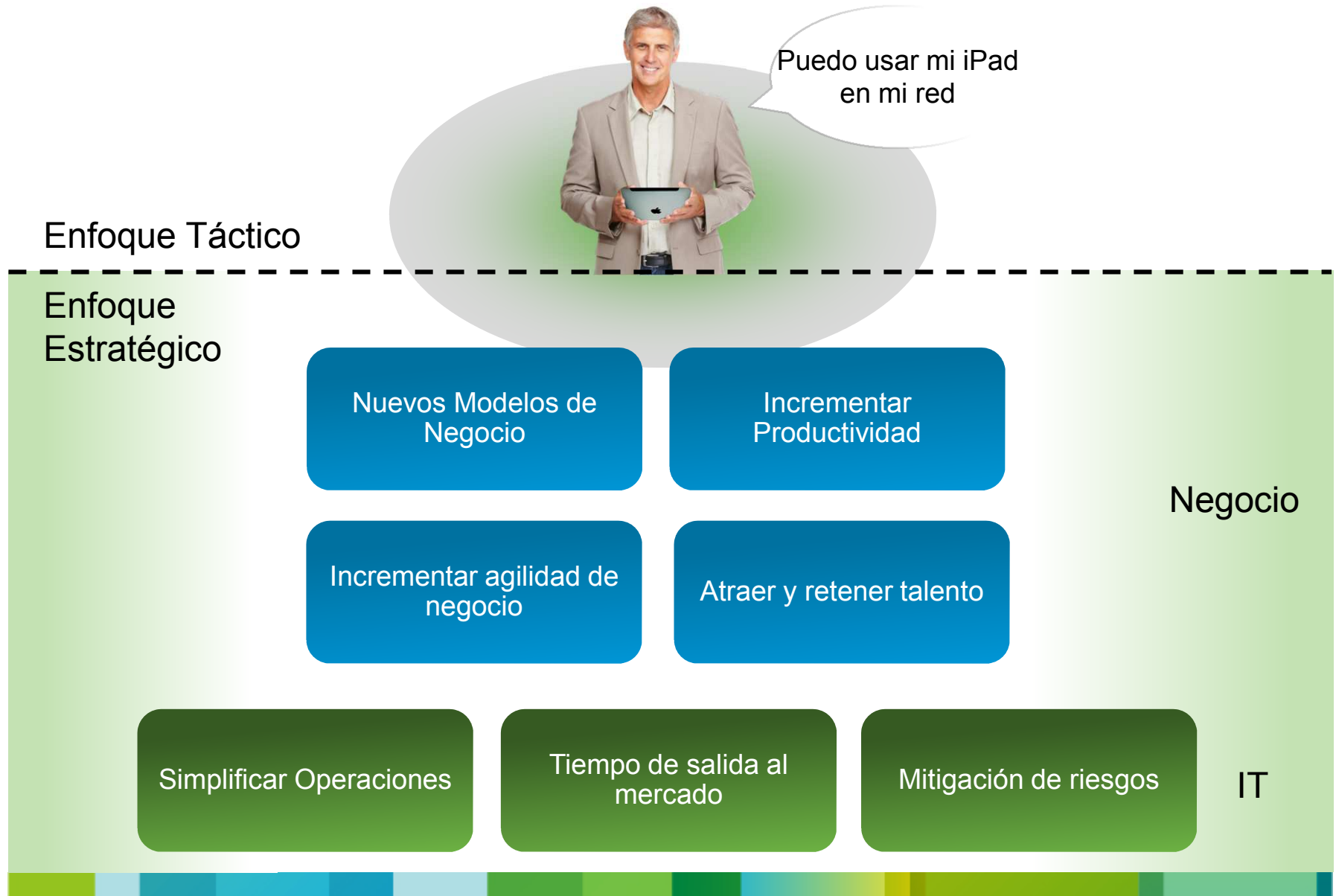


## Segunda Pregunta

**¿En su empresa existe alguna iniciativa de BYOD?**

- a) No formalmente.**
- b) Si, con un enfoque táctico.**
- c) Si, con un enfoque estratégico.**

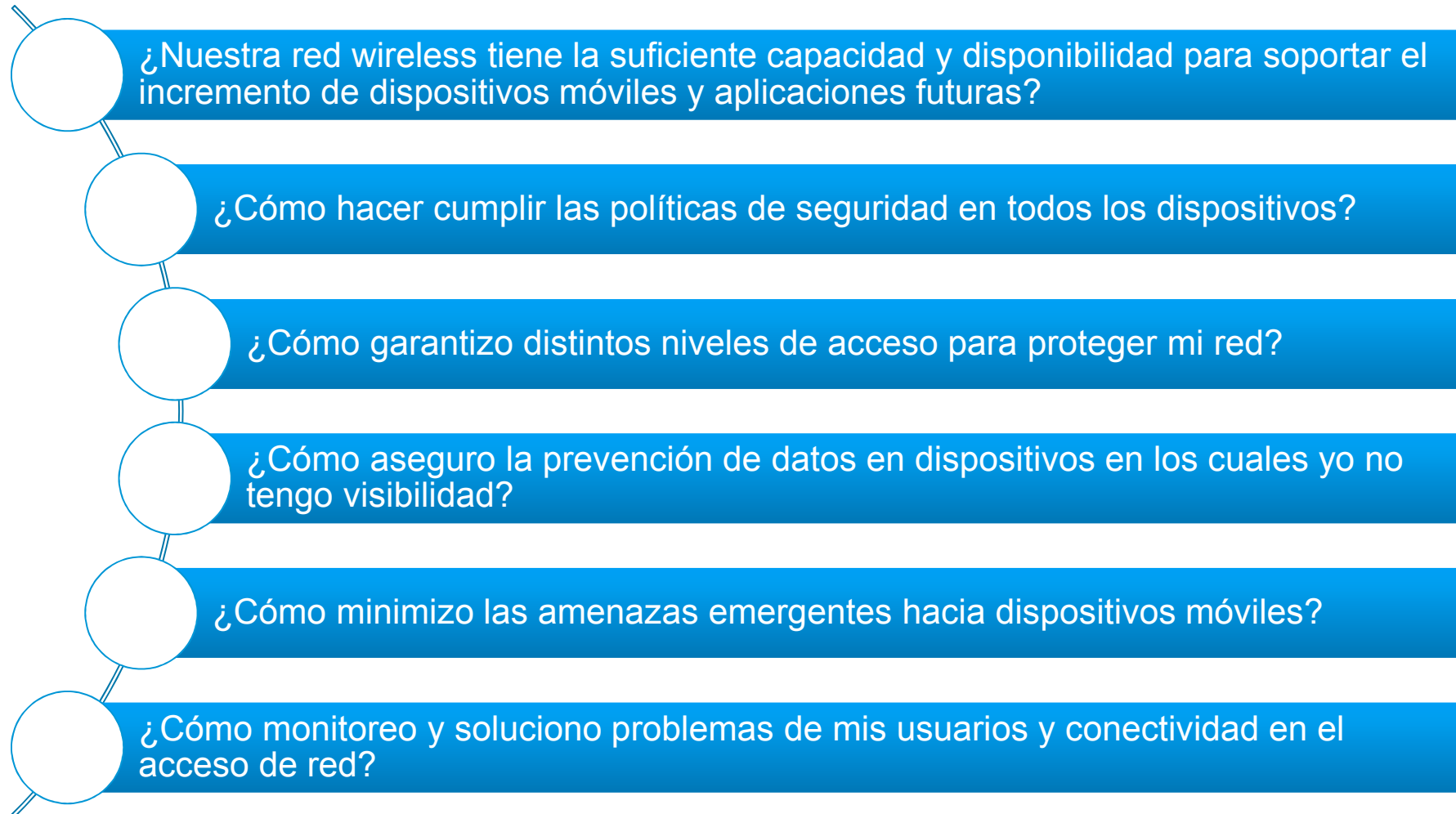
# BYOD Driving Organizational Change



# BYOD – Proyecto con alcance corporativo



# Habilitar movilidad mientras garantizamos la seguridad



# Bring Your Own...X

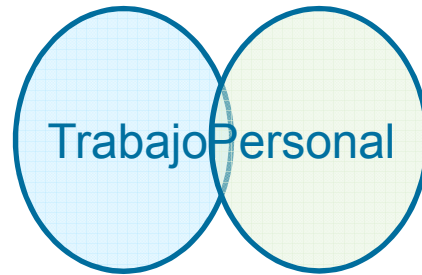
Políticas



# Qué esta impulsando BYOD?



Productividad



Nuevos dispositivos móviles



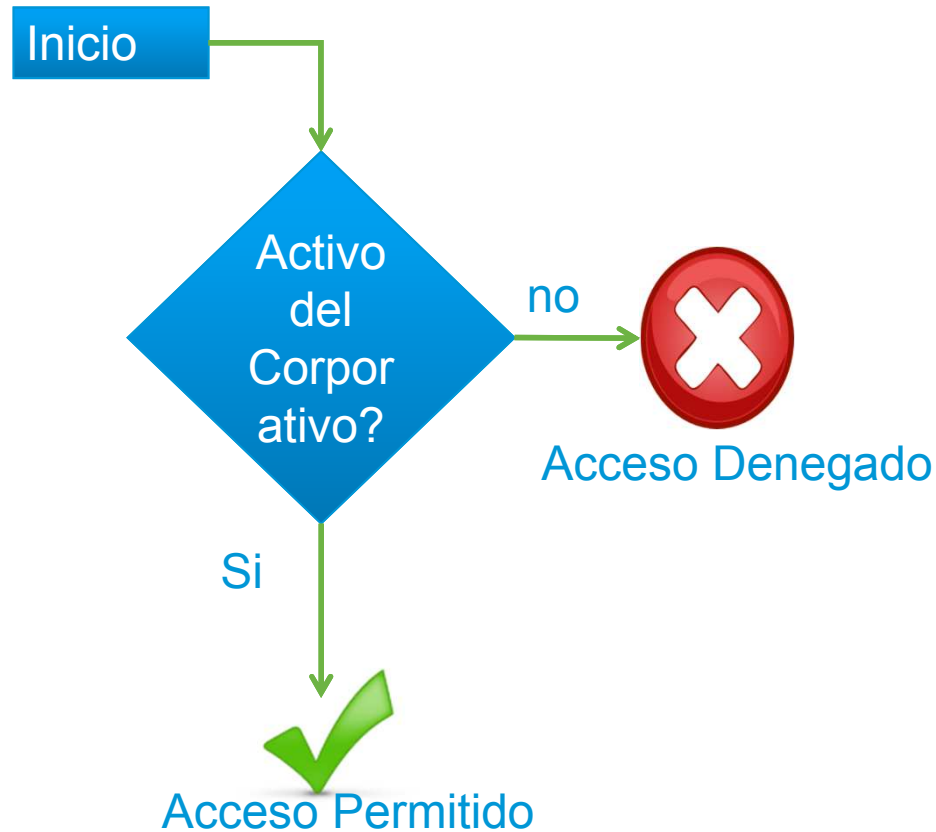
Libertad y movilidad



Nueva imagen corporativa

# En qué consiste una política de BYOD?

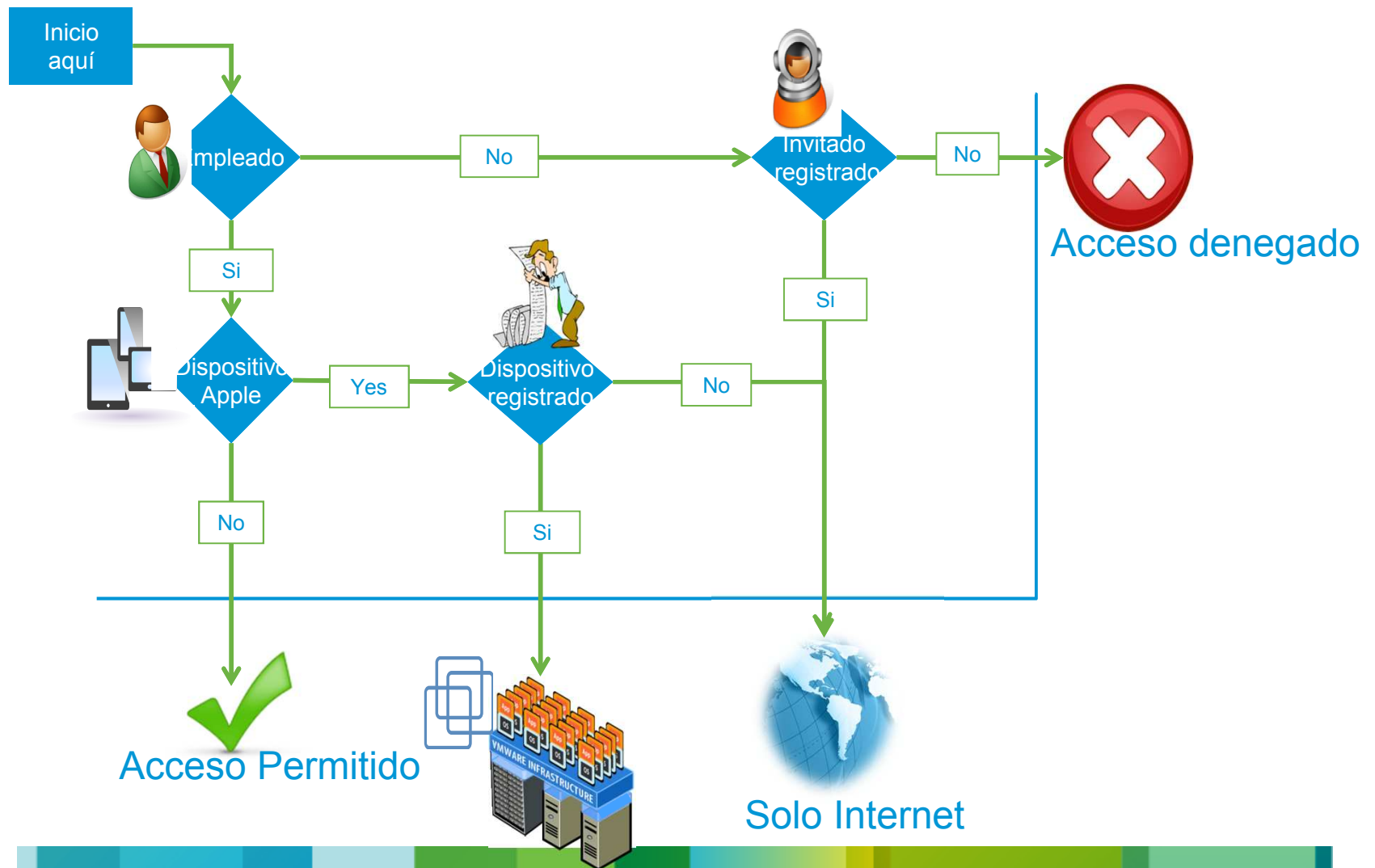
## Autenticación de máquina



- Solo dispositivos corporativos pueden acceder mi red.
  - Esta es tu política de BYOD.

# En qué consiste una política de BYOD?

Aun mas complicado



# Tercera Pregunta

**¿Su empresa esta preparada para la adopción de BYOD (procesos, políticas, infraestructura de red)?**

- a)** Cuenta con la infraestructura de red necesaria pero los procesos de negocio no están listos.
- b)** No cuenta con las políticas de seguridad requeridas para asegurar la integridad y confidencialidad de la información.
- c)** No, la infraestructura de red no esta lista.



# Auto Aprovisionamiento



# Retos

¿Mayor carga operativa?

¿Difícil administración?

¿Cómo gestiono los accesos?

¿Cómo garantizo la seguridad?

# Autoprovisionamiento

Delegar el aprovisionamiento de los dispositivos al usuario

Configuración automática de los equipos

Limitando el número de dispositivos permitidos por usuario

Garantizando la seguridad

# BYOD AuthZ Policy

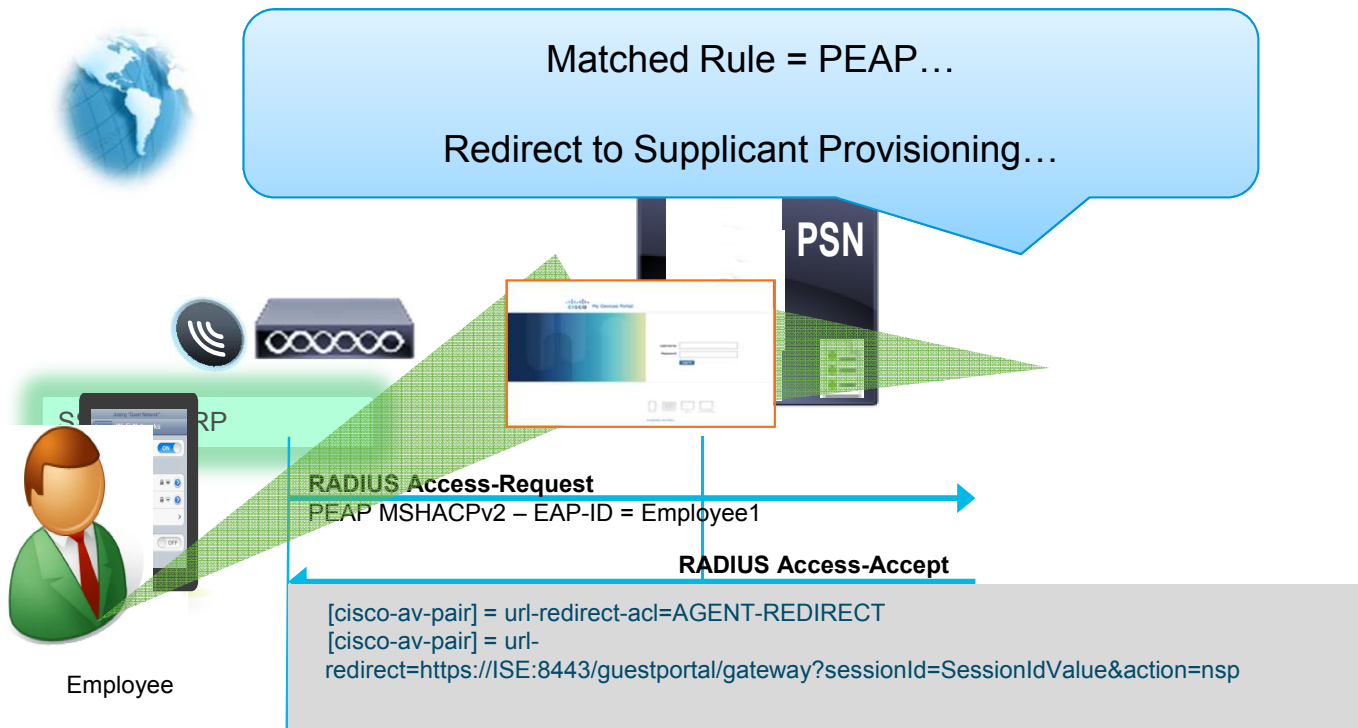
## Un SSID – Empleado usando PEAP

### 1. Cualquier autenticación PEAP :

Aprovisionamiento del cliente nativo

### 2. CWA hacia un SSID abierto

Rule Name	Conditions		Permissions
Guest	if	Guest	then Guest
Open Rule	if	Wireless_MAB	then WEBAUTH
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then Employee
Default	If no matches, then		Deny Access

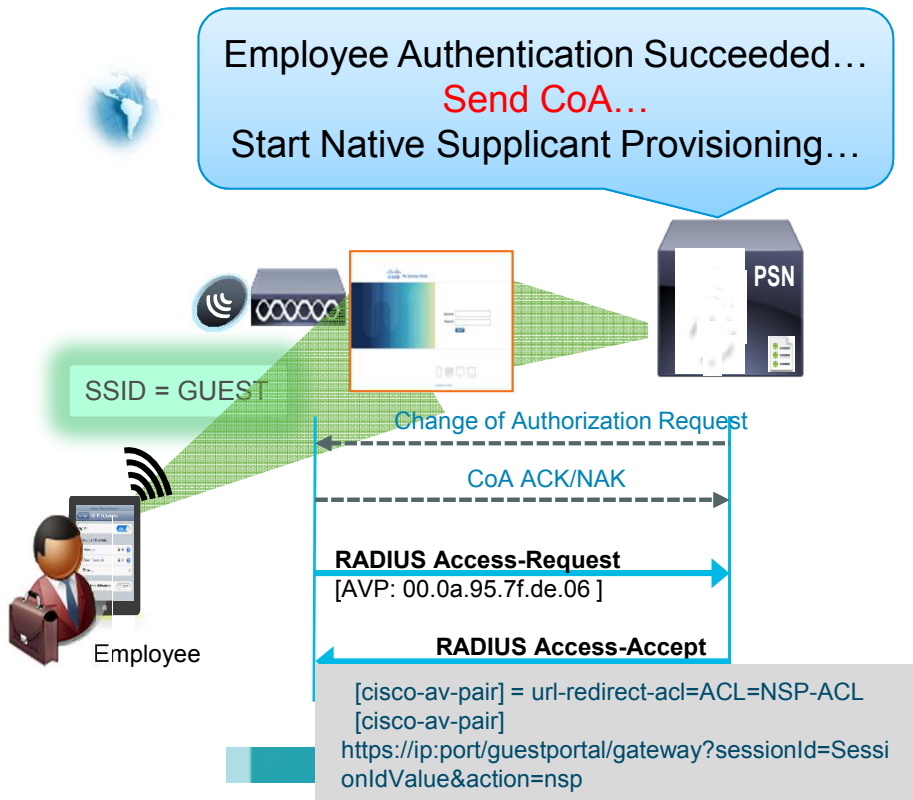


# BYOD Política de authz

## Dos SSID – Empleado + CWA

1. SSID Abierto para aprovisionamiento o cualquier otro método de PEAD, aprovisionamiento
2. EAP TLS SSID para empleados

Rule Name	Conditions			Permissions
Guest	if	Guest	then	Guest
EmpWebAuth	if	Employee & Guest-Flow	then	Supp-Provision
Open Rule	if	Wireless_MAB	then	WebAuth
PEAP	if	Network Access:EapTunnel EQUALS PEAP	then	Supp-Provision
Employee	if	Employee & EAP-TLS & Certificate SAN = MAC_Addr	then	Employee
Default	If no matches, then		Deny Access	



**Multi-Portal**

General Operations Customization Authentication

**Guest Portal Policy Configuration**  
Guest users should agree to an acceptable use policy

☐ Not Used  
☒ First Login  
☐ Every Login

☐ Enable Self-Provisioning Flow

☒ Allow guest users to change password  
☐ Require guest users to change password at expiration and first login  
☐ Guest users should download the posture client  
☒ Guest users should be allowed to do self service

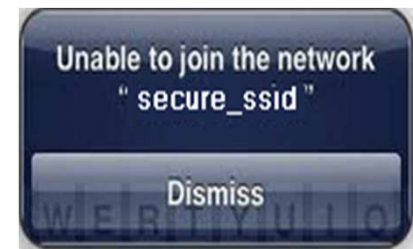
The diagram illustrates the relationship between an Employee, a RegisteredDevice, and an IdentityGroup. An Employee (represented by a person icon) is linked to a RegisteredDevice (represented by a smartphone icon). The RegisteredDevice is linked to an IdentityGroup (represented by a server rack icon). The IdentityGroup is also linked to a PSN (PlayStation Network) icon. The IdentityGroup is also linked to a PSN icon.

# Fast SSID Change

## Configuración del WLC

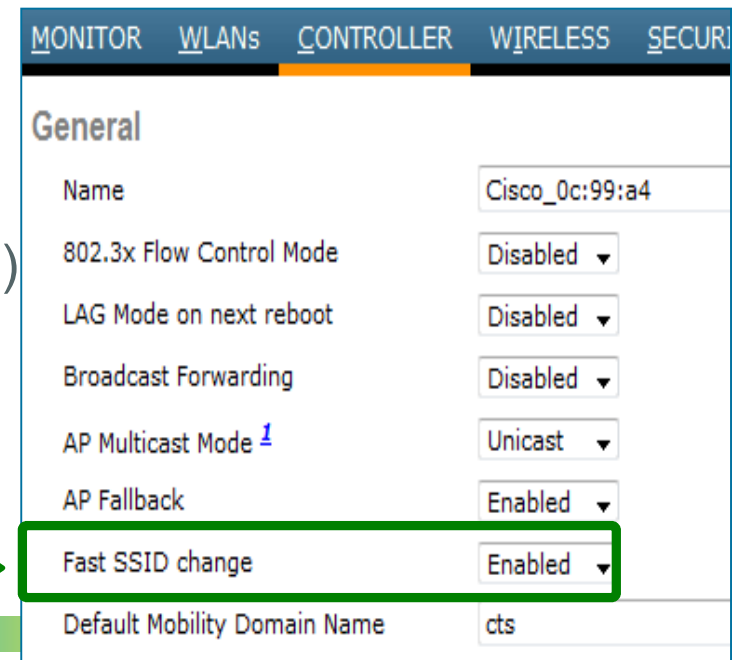
### Descripción del problema:

- No es posible unirse a una red mientras se está conectado actualmente a una.
- Ocurre cuando se cambia rápidamente entre SSIDs como cuando se tiene dual SSID.



### Solución:

- Habilitar "Fast SSID Change" en el WLC (Controller > General > Fast SSID Change)



# Políticas de usuario + máquina

Identificando dispositivos corporativos en la red



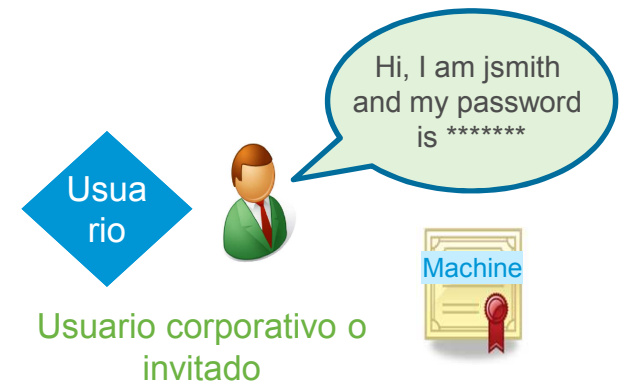
# Políticas de usuario y máquinas

Se quien eres pero, te estas conectando desde un dispositivo corporativo?

- Identidad de usuario...

Username/password (802.1X o WebAuth)

Certificado de usuario(802.1X)



- Identidad de máquina ...

MAC Address?

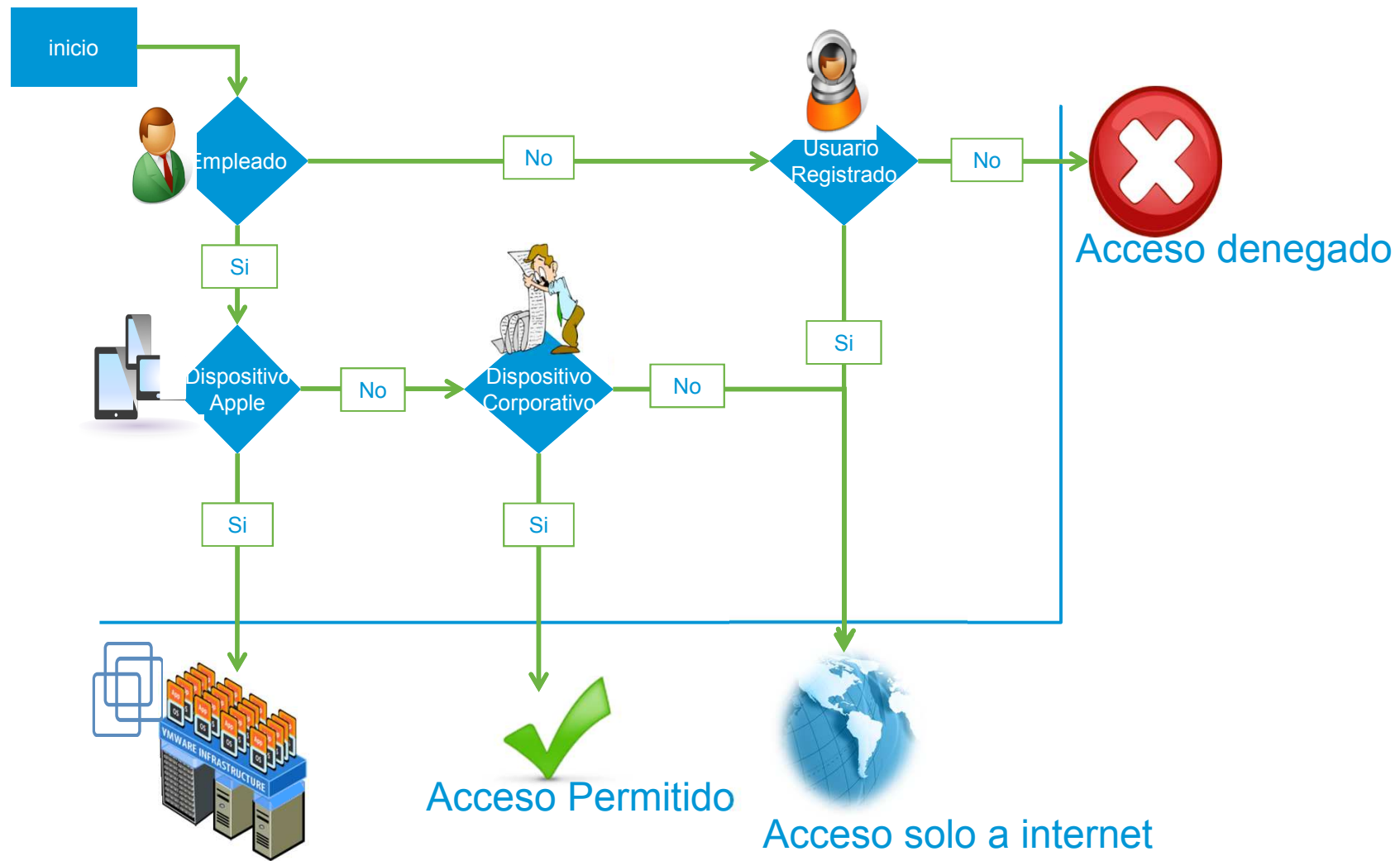
Certificado de máquina(802.1X)



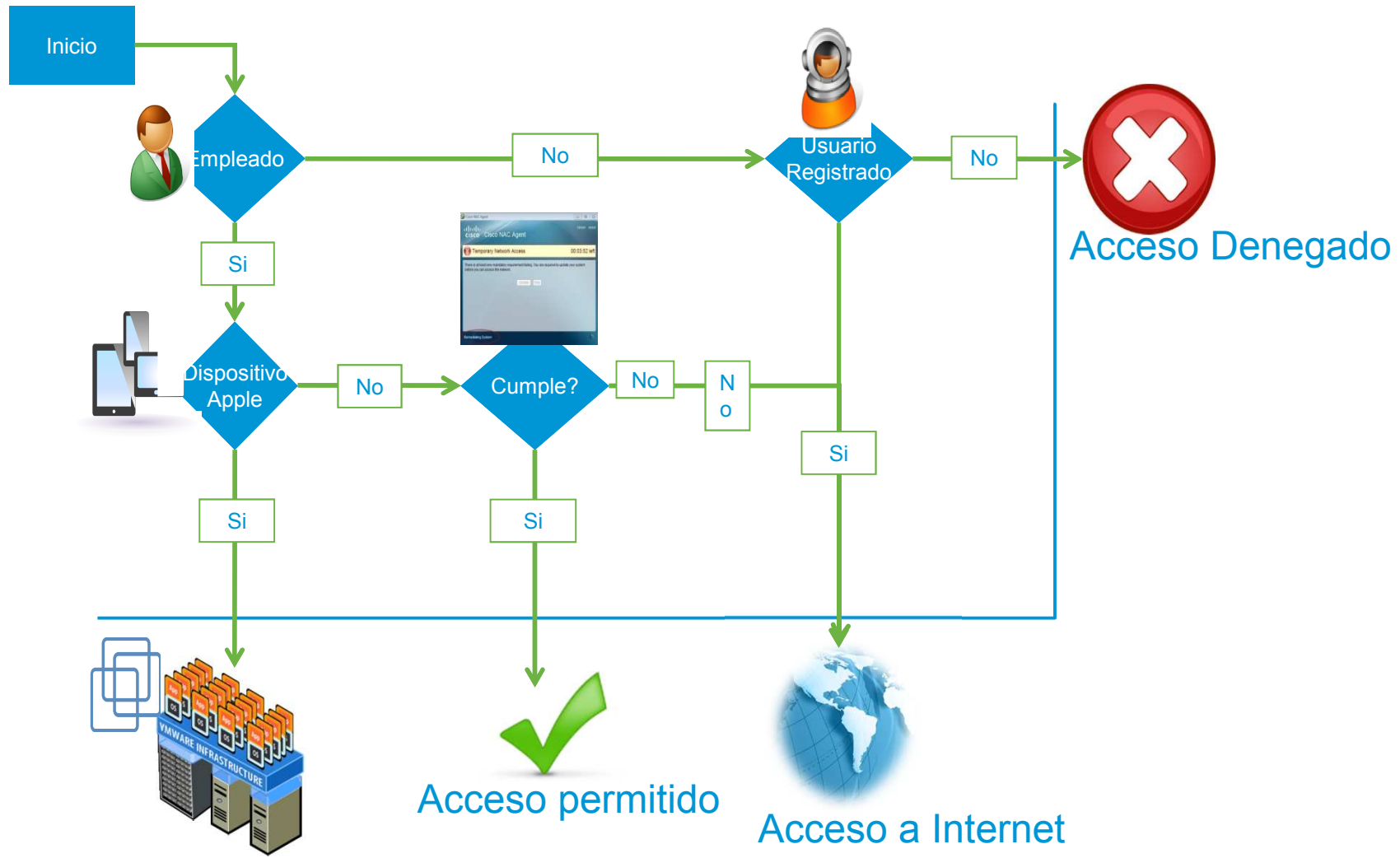
- Cómo los conjunto en una sola política?



# Política de usuario + máquinas



# Política de usuario + máquinas



# Redirección de URL



# Redirección URL

ISE usa redirección de URL para:

- Central Web Auth (CWA)
- Aprovisionamiento de software del cliente
- Descubrimiento de postura y valoración
- Registro de equipo
- BYOD On-Boarding
  - Aprovisionamiento de certificado
  - Configuración de suplicante

The collage illustrates the Cisco Identity Services Engine (ISE) workflow for device registration and network access. It includes screenshots of the Cisco NAC Web Agent showing security policy compliance status, the ISE Guest Portal for device registration, and a self-provisioning portal for user authentication and device setup. A small poster for the Chicago Polyphony Conference 2012 is also visible in the bottom left corner of the collage.

# Redirección de URL, Consideraciones



- **Descripción del problema:** Redirección de URL en dispositivos Apple puede fallar debido al Apple Captive Network Assistant (CNA)

- Acerca de CNA:

Característica de Apple iOS para facilitar el acceso a la red cuando un portal captivo requiere login mediante la apertura automática de un navegador web. Esta característica detecta la presencia de un portal captivo lanzando una petición a <http://www.apple.com/library/test/success.html>

Si la respuesta es recibida, entonces se asume que existe acceso a Internet y ninguna otra acción es requerida

Si no se recibe respuesta, se asume que el acceso a internet esta bloqueado por el portal captivo y CNE lanza automáticamente un portal que requiere login y password para acceder a la red

- **Solución:**

1. Deshabilitar el Auto-Login en la configuración de WLAN (requiere conocimiento e interacción del usuario)
2. Configurar el WLC para bypass CNA:

> `config network web-auth captive-bypass enable`

Comando disponible en WLC 7.2:

<http://www.cisco.com/en/US/docs/wireless/controller/7.2/command/reference/cli72commands.html#wp15129591>



# ISE Servicios de Profiling



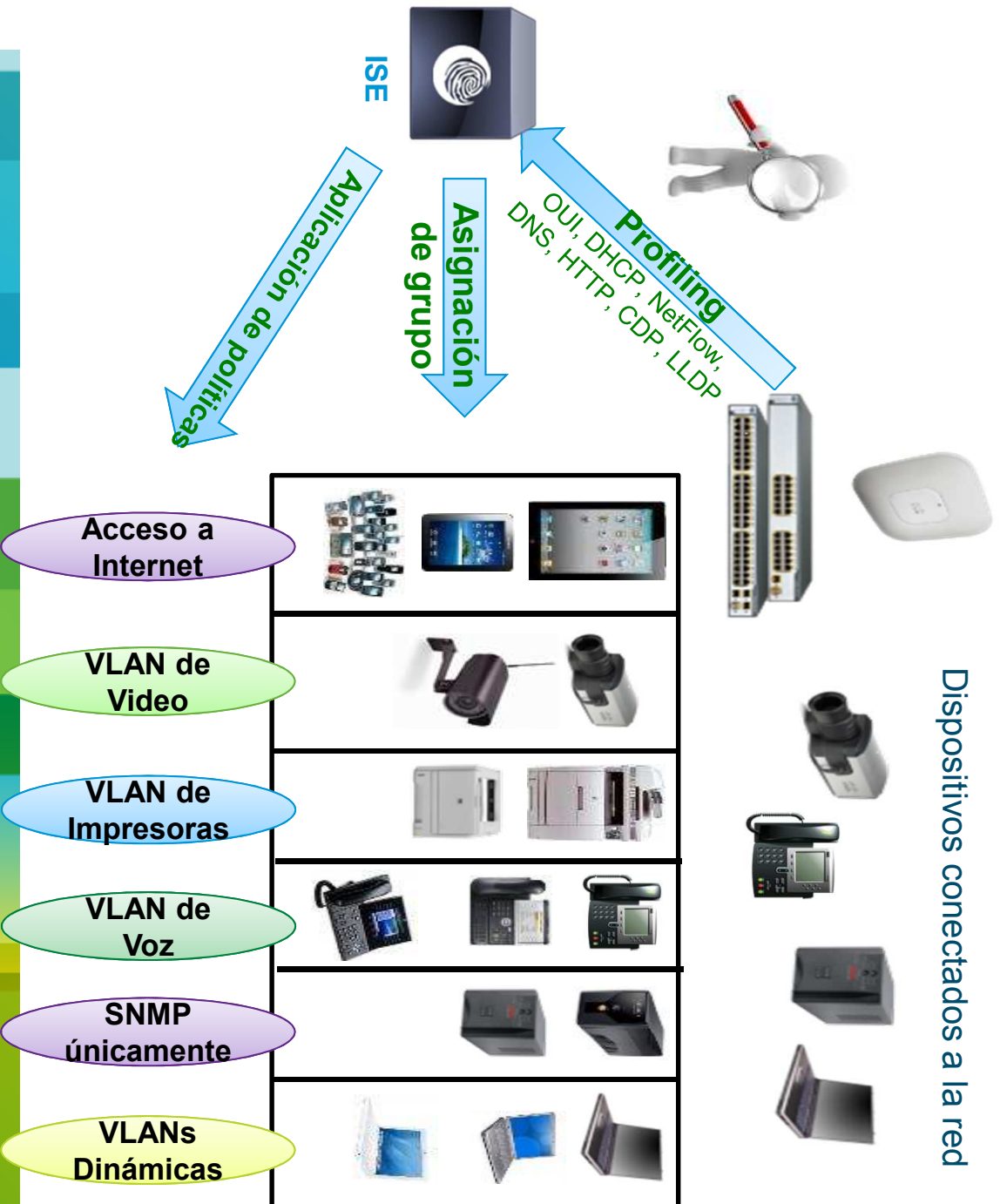
O

e



# ISE Profiler: En tres Pasos

Dispositivos conectados a la red



# Profiling – Mejores Prácticas



# Profiling – Consideraciones de Diseño

- Planeación de Diseño

1. Identificar los endpoints que requieran clasificación

2. Determinar los atributos requeridos

Los dispositivos mas populares ya cuentan con sus perfiles pre-construidos. Analiza los requerimientos analizando los perfiles por defecto. Qué probes se usan para coleccionar datos?

Casi siempre puedes determinar los requerimientos de profiling analizando los requerimientos de dispositivos similares.

Si no existe algún perfil similar, puedes habilitar probes temporalmente y ver que atributos puedes usar para el perfilamiento.

Algunos dispositivos pueden requerir análisis de trafico para determinar atributos únicos

3. Determina la mejor opción de los métodos disponibles para coleccionar la información de profiling requerida

- Configuración de dispositivo de acceso:

Tiempo de perfilamiento – impactado por el orden de MAB/802.1X y tipo de implementación (auth open vs closed)

Verificar que las políticas de acceso permitan la coleccion de atributos requeridos para matchear las condiciones de la política

- Excepciones a las políticas pueden ser requeridas para sobre escribir la asignación de grupos



# Profile Endpoints – Ejemplos de atributos

RADIUS	SNMP	MAC	DHCP	NMAP	NetFlow	CDP
<div>Called-Station-ID</div> <div>Calling-Station-ID</div> <div>CHAP-Challenge</div> <div>CHAP-Password</div> <div>Class</div> <div>Connect-Info</div> <div>Digest-Attributes</div> <div>Digest-Response</div> <div>EAP-Key-Name</div> <div>EAP-Message</div> <div>NAS-IP-Address</div> <div>NAS-Port</div> <div>NAS-Port-Id</div> <div>NAS-Port-Type</div> <div>Service-Type</div> <div>Framed-IP-Address</div>	<div>hrDeviceStatus</div> <div>ifDescr</div> <div>ifIndex</div> <div>ifOperStatus</div> <div>port</div> <div>portIfIndex</div> <div>sysContact</div> <div>sysDescr</div> <div>sysLocation</div> <div>sysName</div> <div>sysObjectID</div> <div>sysUpTime</div> <div>Vlan</div> <div>VlanName</div> <div>vlanPortVlan</div>	<div>MACAddress</div> <div>OUI</div> <div>IP</div> <div>EndpointSource</div> <div>FQDN</div> <div>Host</div> <div>ip</div> <div>mask</div> <div>PortalUser</div> <div>User-Agent</div>	<div>boot-file</div> <div>client-fqdn</div> <div>client-identifier</div> <div>device-class</div> <div>dhcp-class-identifier</div> <div>dhcp-client-identifier</div> <div>dhcp-message-type</div> <div>dhcp-parameter-request-list</div> <div>dhcp-requested-address</div> <div>dhcp-user-class-id</div> <div>domain-name</div> <div>host-name</div> <div>name-servers</div> <div>pxe-client-arch</div> <div>pxe-client-machine-id</div> <div>pxe-client-network-id</div>	<div>161-udp</div> <div>162-udp</div> <div>1900-udp</div> <div>21-tcp</div> <div>22-tcp</div> <div>23-tcp</div> <div>25-tcp</div> <div>3306-tcp</div> <div>3389-tcp</div> <div>443-tcp</div> <div>445-tcp</div> <div>445-udp</div> <div>500-udp</div> <div>520-udp</div> <div>53-tcp</div> <div>53-udp</div> <div>631-udp</div> <div>67-udp</div> <div>68-udp</div> <div>80-tcp</div> <div>8080-tcp</div> <div>operating-system</div>	<div>MAX_PKT_LENGTH</div> <div>MAX_TTL</div> <div>MIN_PKT_LENGTH</div> <div>MIN_TTL</div> <div>nextHop</div> <div>OUT_BYTES</div> <div>OUT_PKTS</div> <div>output</div> <div>OUTPUT_SNMP</div> <div>prot</div> <div>PROTOCOL</div> <div>sampling_interval</div> <div>source_id</div> <div>src_as</div> <div>SRC_MAC</div> <div>SRC_MASK</div> <div>SRC_TOS</div> <div>SRC_VLAN</div> <div>srcaddr</div> <div>srcport</div> <div>sys_uptime</div> <div>tcp_flag</div> <div>TCP_FLAGS</div>	<div>cdpCacheAddress</div> <div>cdpCacheCapabilities</div> <div>cdpCacheDeviceId</div> <div>cdpCachePlatform</div> <div>cdpCacheVersion</div> <div>LLDP</div> <div>lldpCacheCapabilities</div> <div>lldpCapabilitiesMapSupported</div> <div>lldpChassisId</div> <div>lldpManAddress</div> <div>lldpPortDescription</div> <div>lldpPortId</div> <div>lldpSystemCapabilitiesMapEnabled</div> <div>lldpSystemDescription</div> <div>lldpSystemName</div> <div>lldpTimeToLive</div>

Algunos atributos son mas interesantes que otros

# La guía no oficial para la selección de Probes

¿Qué probes debo usar para mi implementación?

- Generalmente hablando...

¿Qué probes son mas difíciles de implementar?

¿Qué probes tienen menor impacto en mi red?

(en términos de carga de trafico, carga en el servidor de ISE, componentes adicionales, etc.)

¿Qué valor agrega ese proble a mi capacidad de perfilamiento para mis endpoints?

<b>DDI</b>	<b>D</b> eployment <b>D</b> ifficulty Index	Easy	Medium	Difficult
<b>NII</b>	<b>N</b> etwork <b>I</b> mpact Index	Low Impact	Medium Impact	High Impact
<b>PVI</b>	<b>P</b> robe <b>V</b> alue Index	High Value	Medium Value	Low Value



# Wireless Profiling

## Mejores Prácticas

- Configurar Calling-Station-ID to MAC Address para no-1X WLANs:  
**Security > AAA > RADIUS > Authentication**

### RADIUS Authentication Servers

Call Station ID Type [1](#) System MAC Address ▼

- Deshabilitar DHCP Proxy para permitir el reenvío de DHCP -> IP  
Helpers:  
**Controller > Advanced > DHCP**

### DHCP Parameters

Enable DHCP Proxy ☐

DHCP Option 82 Remote Id field format AP-MAC ▼

DHCP Timeout (5 - 120 seconds) 120

# ISE Profiling

## Mejores Prácticas

- **Utilizar sensores cuando sea posible para optimizar la colección de datos**
- **Cuando sea posible asegurarse que los datos de perfilamiento para un dispositivo se mande al mismo PSN**
- **HTTP Probe:**
  - Usar redirección de URL sobre un puerto SPAN para centralizar el tráfico
  - En general, tratar de evitar el uso de SPAN. Si se usa, deberá usarse en puntos muy específicos de la red
- **DHCP Probe:**
  - Utiliza IP Helpers cuando sea posible
  - Tratar de evitar utilizar DHCP SPAN. Si se usa, asegúrate que las capturas se hagan cerca del servidor de DHCP
- **SNMP Probe:**
  - Tener cuidado con la alta cantidad de tráfico de SNMP que puede ser ocasionado por los accounting de radius
  - Para peticiones, no poner el intervalo muy bajo
  - SNMP traps son útiles cuando no usemos RADIUS
- **NetFlow:** Utilizarse solamente para casos específicos. Pudiera causar alta carga en la base de datos



# Integración de Cisco Identity Services Engine y mejores prácticas

Mejores prácticas



# Mejores prácticas en la instalación

## Conexión a la red productiva, NTP, DNS

- Conectividad de red

GE 0 debe tener una conexión de red válida y conectividad hacia su gateway (Ping).

- NTP

Configurar NTP y asegurarse que el horario sea correcto

Time Zone = UTC es una buena práctica para implementaciones con distintas zonas horarias

- DNS

DNS deberán ser alcanzables por los nodos de ISE y configurados para resolver el FQDN de los nodos de nuestra solución de ISE

- Usar minúsculas en el hostname.

- No usar certificados “self-signed” en redes en producción



# ISE Mejores Prácticas

## Integración con el directorio activo

- Cada nodo de ISE se unirá al directorio activo de forma separada y cada nodo usará su propia cuenta
- Una cuenta con privilegios de agregar y remover máquinas en el dominio es requerida
- Sincronización de reloj – una diferencia mayor a 5 minutos entre el AD y el ISE causará problemas para la integración
- Integración con múltiples dominios
  - Si hay relación de confianza entre dominios, solo necesitas unirte a un dominio
  - Si no hay relación de confianza entre dominios, la mejor solución dependerá del método de autenticación a utilizar

## Cuarta Pregunta

**¿Tiene visibilidad de los dispositivos que se conectan a su red y controla sus accesos a los recursos de red?**

- a) No
- b) Parcialmente
- c) En su totalidad
- d) Estáticamente
- e) Dinámicamente

# Referencias

- Support Forum  
<https://supportforums.cisco.com/>
- Design Guides  
[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)
- [http://www.cisco.com/web/solutions/trends/byod\\_smart\\_solution/index.html](http://www.cisco.com/web/solutions/trends/byod_smart_solution/index.html)
- [http://www.cisco.com/web/ES/products/wireless/enterprise\\_mobility.html](http://www.cisco.com/web/ES/products/wireless/enterprise_mobility.html)
- Support pages:  
[http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/solution\\_overview\\_c22-591771.html](http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns1051/solution_overview_c22-591771.html)
- [http://www.cisco.com/en/US/products/ps11640/tsd\\_products\\_support\\_design.html](http://www.cisco.com/en/US/products/ps11640/tsd_products_support_design.html)

# Sesión de Preguntas y Respuestas

El experto responderá verbalmente algunas de las preguntas que hayan realizado. Use el panel de preguntas y respuestas (Q&A) para preguntar a los expertos ahora



# Nos interesa su opinión!!!

Habr  un sorteo con las personas que llenen el cuestionario de evaluaci n.

Tres de los asistentes recibir n un  
**Regalo sorpresa**



Para llenar la evaluaci n haga click en el link que est  en el chat, tambi n aparecer  autom ticamente al cerrar el browser de la sesi n.



# Pregunte al Experto (con Israel González)



Si tiene preguntas adicionales pregunte aquí

<https://supportforums.cisco.com/thread/2229799>

Israel responderá del martes 23 de julio al viernes 2 de agosto del 2013.

Puede ver la grabación de este evento, y leer las preguntas y respuestas en 5 días hábiles en:

<https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/webcasts>



# Pregunte al Experto (en Español)



**Tema: Cómo proteger tu red con un Adaptive Security Appliance Cisco (ASA)**

Con el experto de Cisco: **Julio Carvajal**

Esta es su oportunidad de aprender y de hacer todas las preguntas que tenga acerca de Cómo proteger tu red con un Adaptive Security Appliance Cisco (ASA): Monitoreo y resolución de problemas en configuraciones.

**Finaliza el 25 de julio del 2013**



**Tema: Instalación y configuración de Servidores UCS**

Con el experto de Cisco: **Keny Perez**

Aprenda y haga preguntas acerca de Instalación y configuración de Servidores (UCS)

**Inicia el 26 de julio y estará disponible hasta el 9 de agosto del 2013**

**Participe en la discusión y pregúntale al experto en:**

[https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/pregunte\\_al\\_experto](https://supportforums.cisco.com/community/spanish/espacio-de-los-expertos/pregunte_al_experto)

# Pregunte al Experto (en Inglés)



**Tema: Un viaje por el Cisco Process Orchestrator**  
**Con el experto de Cisco: Shaun Roberts**

Aprenda y haga preguntas sobre el Cisco Process Orchestrator

**Inició el 15 Julio 2013**



**Tema: Implementación de Cisco FabricPath en el Centro de Datos NetworkFabricPath**  
**Con los expertos de Cisco: Vivek Ruhil**

Aprenda y haga preguntas sobre MPLS L3VPN conceptos, terminología, control y flujo de llamadas y de datos.

**Inició el 15 Julio 2013**



**Tema: Configuración y solución de problemas del equilibrador de carga Cisco Application Control Engine (ACE)**  
**Con los expertos de Cisco: Ajay Kumar and Telmo Pereira**

Aprenda y haga preguntas acerca de la resolución de problemas y configuración de la aplicación de control de motor de Cisco (ACE) equilibrador de carga

**Inició el 15 Julio 2013**

**Participe en la discusión y pregúntale al experto en:**

<https://supportforums.cisco.com/community/netpro/expert-corner#view=ask-the-experts>

# Califique el contenido de la Comunidad de Soporte de Cisco en Español.



**Ahora puede calificar discusiones, documentos, blogs y videos!!...**

Esto es con el fin de que nos ayude a distinguir contenido de calidad y también para reconocer los esfuerzos de los integrantes de la Comunidad de Soporte de Cisco en español.

<https://supportforums.cisco.com/community/spanish/general/blog/2013/06/21/ahora-ratings-en-documentos-blogs-y-videos>

# Soporte Técnico Móvil, anuncia su nuevo acceso a las Comunidades de Soporte Globales.



La Comunidad de Soporte de Cisco anuncia su evolución con el lanzamiento del nuevo Acceso Móvil hacia la Comunidades Globales > Español, Portugués, Japonés, Ruso, y Polaco.

<https://supportforums.cisco.com/docs/DOC-34800>



# Lo invitamos a colaborar activamente en CSC en español y en nuestras redes sociales



<https://supportforums.cisco.com/community/spanish>



CiscoLatinoamerica

Cisco Mexico

Cisco España

Cisco Cono Sur

Comunidad Cisco Cansac

CiscoSupportCommunity



@Cisco\_LA

@CiscoMexico

@cisco\_spain

@ciscocansacsm

@ciscoconosur

@cisco\_support

## Más redes sociales:



**CiscoLatam**  
**ciscosupportchannel**



**Cisco Technical Support**



**CSC-Cisco-Support-Community**

Gracias por su  
tiempo

Por favor tomen un momento para llenar su evaluación



