Check Point Security Gateway R75.40

Curso Práctico

DevilBSD <devilbsd@fusiondementes.net>

Tabla de contenidos

Topología del laboratorio

Importante

Este documento es continuamente actualizado, no olvides revisar de vez en cuando si hay novedades. Me gustaría sabersi el documento ha sido de ayuda o no, cualquier comentario es bueno saberlo. Las máquinas virtuales no estan disponibles todavía.

Para la correcta ejecución del laboratorio es necesario que tú equipo cumpla con los siguientes requerimientos básicos.

- Sistema Operativo Windows Vista o 7.
- Espacio libre en HD mayor a 30 Gb.
- Memoria RAM mínima de 4 Gb.
- Procesador CoreDuo @ 2GHz o superior.
- Conexión Wi-fi.
- VMWare Workstation 7.1.4 o superior **instalado**. **NO USAR VMWARE PLAYER**

El laboratorio cuenta con los siguiente elementos:

- **CheckPointGW:** En ésta máquina virtual se va a instalar Check Point R75.40 en modo StandAlone. A través de los diferentes laboratorios se activarán los productos: Firewall, VPN, Application Control & URL Filtering, Identity Awareness, Mobile Access Blade y Smart Event.
- **Samael:** Esta máquina virtual cuenta con servicios preconfigurados para los laboratorios como: Servidor SSH (OpenSSH), servidor WEB (Cherokee), recursos compartidos (SAMBA) y servidor SMS (SMSd).
- **Equipo Host:** El equipo host, además de correr las máquinas virtuales; se utiliza en el laboratorio para instalar SmartConsole, Endopoint Secure Access y para realizar varias pruebas.

Usuarios y Contraseñas

Importante

Para simplificar la configuración de los usuarios utilizados en el laboratorio, todas las contraseñas son: **vpn123**

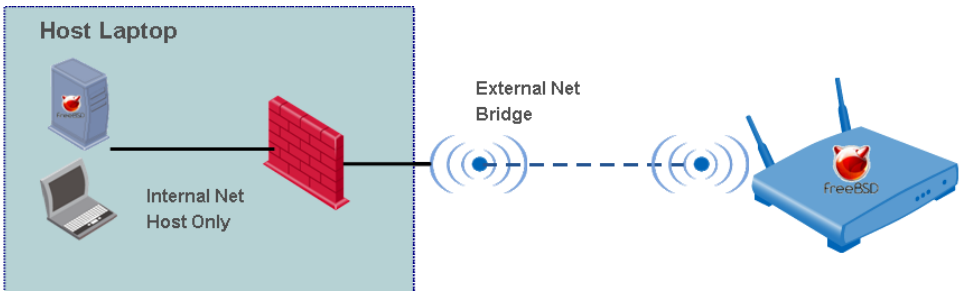
Tabla 1. Lista de usuarios.

Host	Usuario	Función
CheckPointGW	**`admin`**	Administrador con acceso a **`clish`**.
	`expert`	Administrador con acceso a **`bash`**
SmartConsole	**`scadmin`**	Administrador del cliente GUI.
Samael	**`root`**	Super Usuario del sistema
	`samael`	Usuario normal en grupo wheel
	`puffy`	Usuario con recurso compartido
	`theo`	Usuario con recurso compartido

Diagrama general del laboratorio.

Importante

Todo el tráfico hacia Internet saliente del *Equipo Host*, debe de pasar por *CheckPoint GW*. Es necesario remover el Default Gateway de las tarjetas físicas y configurarlo en la interfaz virtual ubicada en el segmento de red interno del gateway.



Antes de comenzar a realizar los laboratorios debes seguir los siguientes pasos para la configuración de las interfaces de red en VMWare tomando nota en la siguiente tabla.

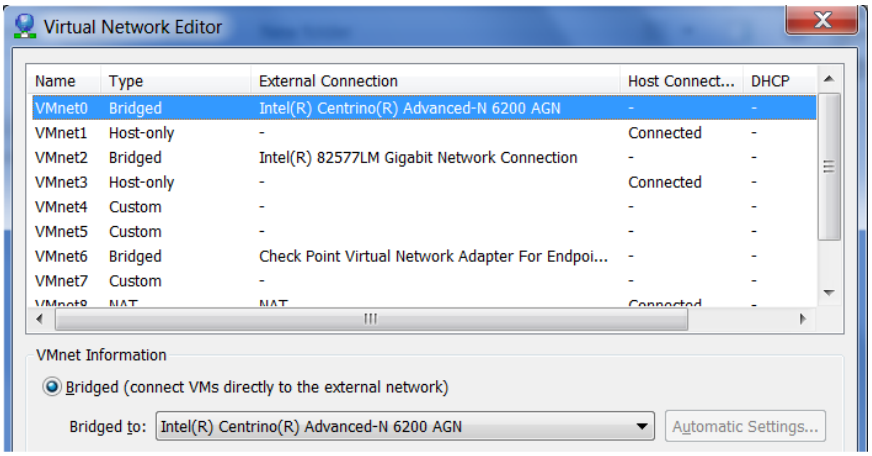
Tabla 2. Direccionamiento

HOST	Interfáz	Dirección IP	Default GW
Equipo Host	Wireless Network Connection	Asignada por DHCP	NINGUNO
	VMnet1	10.30.40.10/24	10.30.40.254
CheckPointGW	eth0	192.0.2.254	192.0.2.2
	eth1	10.30.40.254/24	NINGUNO
Samael	em0	10.30.40.20/24	10.30.40.254
ServidorSMS		Asignada por DHCP	
DNS	Todos los Sistemas Operativos	4.2.2.2	
IP pool (office mode)	Mobile Acces	172.16.10.0/24	

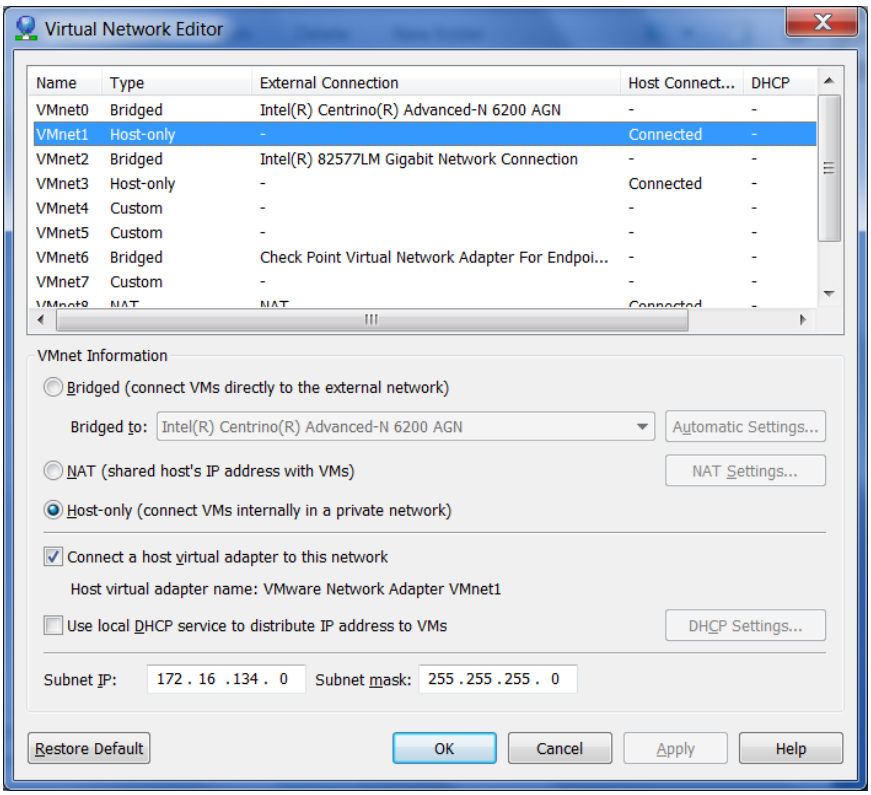
Configuración de Interfaces de red en VMWare

1. Abrir *Virtual Network Editor* desde: *Inicio -> Programa -> VMware -> Virtual Network Editor.*

2. Seleccionar *VMnet8*, configurar como tipo *NAT.*



3. Seleccionar *VMnet1*, configurar como tipo *Host-Only*, seleccionar la casilla *Connect a host virtual adapter to this network* y definir el segmento de red como 10.30.40.0/24. Esta interfaz va a ser la red interna.



Configuración de la interfaz de red Wireless en Windows.

1. Abrir *Network and Sharing center.*

2. Seleccionar *Wireless Network Connection*, en las propiedades de IPv4 fijar manualmente la IP y máscara asignada, Default Gateway y DNS.

3. Seleccionar *VMware Network Adapter VMnet1*,en las propiedades de IPv4 cambiar la dirección IP a 10.30.40.10/24 y Defaut GW 10.30.40.254Como servidor DNS utilizar: 4.2.2.2. En caso de que la interfaz no aparezca listada, será necesario reiniciar el equipo.

Configuracion de Interfaces en VM

La topología de las interfaces en las máquinas virtuales ya están configuradas según la tabla. Para confirmar las configuraciones sigue los siguientes pasos:

Tabla 3. Interfaces en VMware

VM	Device	Interfáz Virtual	Interfaz SO
CheckPointGW	Network Adapter	Custom (VMnet8) NAT	eth0
	Network Adapter 2	Custom (VMnet1) Host-Only	eth1
Samael	Network Adapter	Custom (VMnet1) Hosy-Only	em0

1. Abrir en el menú de VMware: *VM -> Settings.*.

2. Todos los dispositivos *Network Adapter* deben de tener seleccionados los checkbox *Connected* y *Connected at power on.*

Lab #1: Configuración e instalación básica del sistema.

Importante

Durante todo el curso necesitarás revisar las bitácoras para comprobar las configuraciones. ¡Mantén **SmartLog** siempre abierto!

Objetivo: Al final de éste laboratorio debes tener un Security Gateway R75.40 StandAlone, incluyendo un set de reglas básica que permitan a los hosts detrás del GW salira internet, así como publicar los servicios HTTP y SSH del servidor Samael.

Temas que abarca este laboratorio.

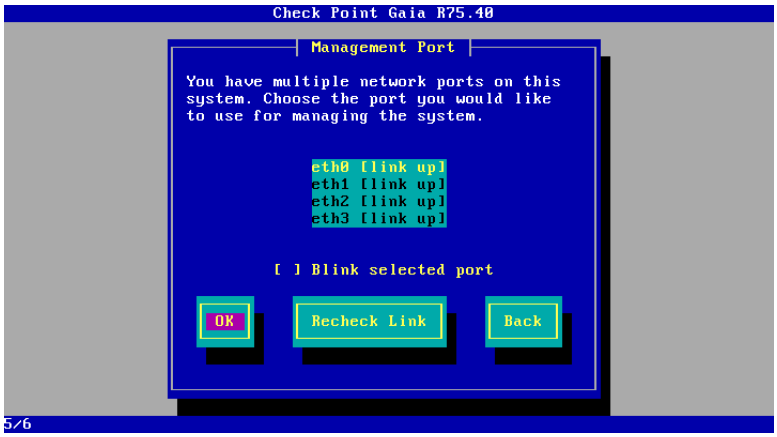
1. Instalación de sistema operativo GAiA.
2. Instalación de productos Check Point.
3. SmartLog.
4. Check Point Smart Console.
5. *Security Rule:* Objetos, grupos, reglas de seguridad, reglas implícitas, NAT, fases de la instalación de la política de seguridad

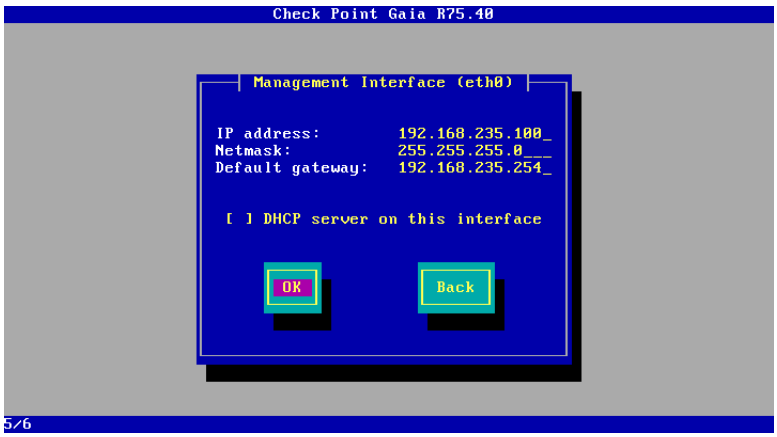
Tus actividades:

1. Instalar en la VM Check Point R75.40 con consola de administración. (StandAlone)
2. Instalar SmartConsole y actualizar la topología de red.
3. Configurar reglas implícitas para permitir ping y consultas DNS de los usuarios sin crear reglas explícitas.
4. Crear los objetos, grupos, reglas y NATs necesarios para que el equipo detrás del gateway pueda acceder a Internet.

Instalación de sistema operativo GAIA.

1. El programa de instalación comenzará al iniciar el equipo *CheckPointGW* desde el CD.
2. Selecciona **eth0** *(Interface en NAT)* y configura su direccionamiento externo así como su *Default Gateway*.

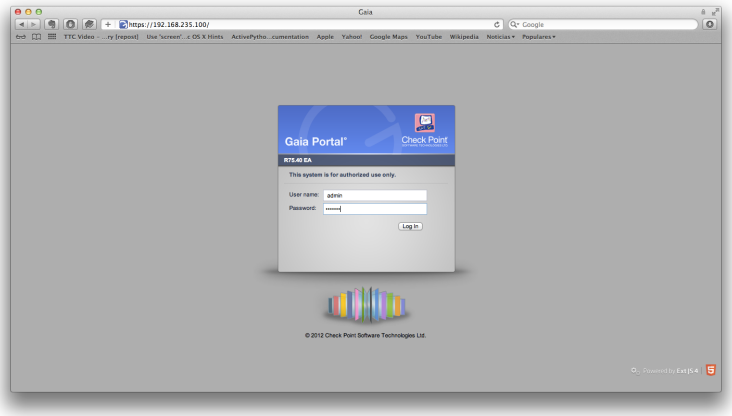




3. El programa de instalación particionara el disco duro y copiará los paquetes de instalación. Al terminar reiniciar el equipo.

First Time Wizard

1. Abre un navegador y conéctate al WebUI utilizando HTTPS a la dirección que configuraste como externa, inicia sesión con el usuario **`admin`** creado al momento de la instalación.



2. Después de iniciar sesión debes de realizar la configuración inicial del sistema. Presiona *Next* para comenzar con **Gaia First Time Configuration Wizard.**

3. Configura la fecha, hora y zona horaria de tu localidad. Presiona *Next* para continuar.

4. Configura el hostname del gateway y su DNS *(4.2.2.2)*. Presiona *Next* para continuar.

5. Comfirma los parametros de red para eth0, la interfáz eth1 se configurará más adelante.

6. Instala los productos referentes al Security Gateway y al Smart Management Server

7. Al terminar el asistente la instalación de los productos, reinicia el sistema

Configuración de la interfaz interna eth1.

1. Dentro de la administración Web, ir a *Network Management -> Interfaces* y seleccionar la interace eth1 y presionar edit

2. Configura el direccionamiento interno para eth1, ésta interface no lleva Default Gateway

Configuración de la Topología de Red en CheckPointGW

Para continuar con los pasos siguientes es necesario instalar SmartConsole R75.40 en el Equipo Host.

1. Abrir SmartDashboard desde *Inicio -> Todos los programas -> Check Point SmartConsole R75.40 -> SmartDashboard*

2. Iniciar sesión con el usuario **`scadmin`** en el servidor **`10.30.40.254`**

3. Abrir las *Propiedades Generales* del gateway haciendo doble click en el objeto. Seleccionar *Topology -> Get .. -> Interfaces with Topology.*

4. Para cada una de las interfaces definir *Topology* y *Antispoofing.*

5. Seleccionar *General Properties*. Dentro de la pestaña *Network Security* activar los blades *Firewall & IPSec VPN.*

Configuración de reglas Implícitas.

1. Para configurar las reglas implícitas; abrir *Policy ->Global Properties -> Firewall*

2. Dentro de *FireWall Implied Rules* activar y/o configurar las siguientes propiedades:

Tabla 4. Reglas Implícitas

Accept Domanin Name over UDP	First
Accept ICMP requests	First
Log Implied Rules	Activar checkbox

Configuracion de objetos, reglas y NATs

1. *Creación del objeto Red_Interna:* En el arbol de objetos seleccionar *Networks -> Network...* Configurar nombre y direccionamiento.

2. Agregar regla de NAT automática y configurar NAT Hide detrás del Gateway.

3. *Creación del objeto Host Samael:*En el arbol de objetos seleccionar *Node -> Host...* Configurar nombre y direccionamiento.

4. Configurar el conjunto siguiente de reglas:

Tabla 5. Rulebase inicial.

Source	Destination	Service	Action	Track

Red_Interna	Any	Any	accept	Log
(Not)Red_Interna	CheckPointGW	Any	drop	Log
Any	Any	Any	drop	Log

5. Instalar política y probar la configuración. Revisar las conexiones en *SmartView Tracker*.

Lab #4: Backup & Restore en SPLAT

Importante

Es posible respaldar la configuración de *Smart Center Server* utilizando **`upgrade_export`** o **`migrate_tools`**, sin embargo estas herramientas no respaldan las configuraciones del sistema operativo; aun así son escenciales para hacer migraciones de versiones o entre distintas plataformas.

*Objetivo:*Respaldar la configuración y restaurar el sistema desde una instalación nueva.

Temas que abarca este laboratorio.

1. **`backup`** & **`restore`**
2. Copiar información desde y a SPLAT

Tus actividades.

1. Obtener el respaldo de la configuración actual.
2. Reinstalar nuevamente SPLAT y los productos necesarios.
3. Restaurar el sistema al estado previo a la reinstalación.

Respaldo de configuración

1. Generar el respaldo utilizando el comando **`backup`** y transmitirlo a un servidor SCP:

   ```
   backup --scp 172.16.X.20 samael vpn123
   ```

2. Iniciar sesión en *Samael* con el usuario **`samael`** y verificar que el respaldo se encuentra en su directorio HOME, revisar la integridad con MD5.

Restauración del sistema

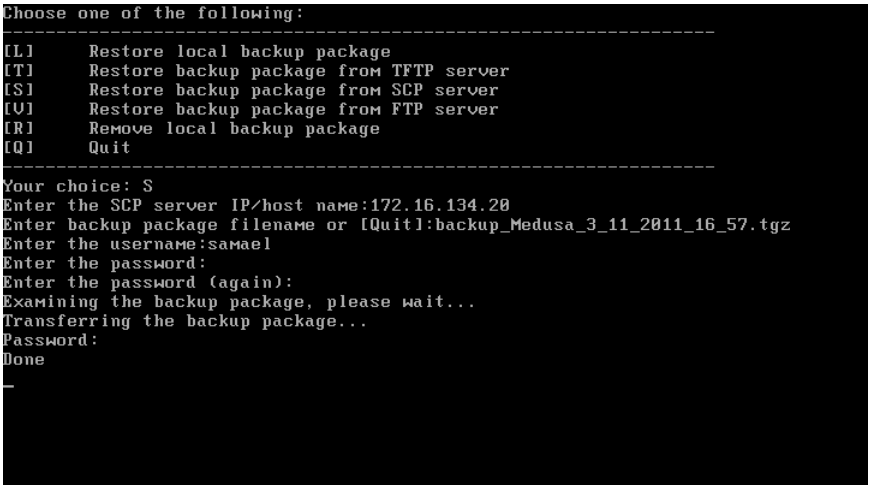
Atención

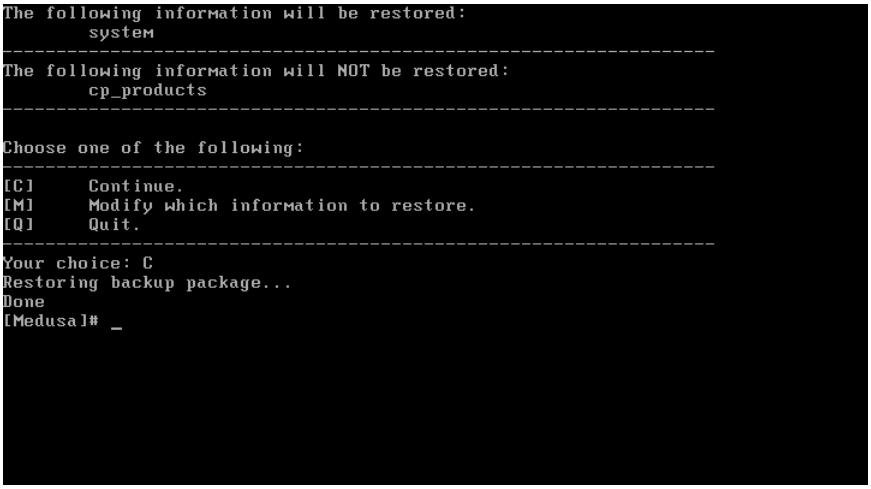
Antes de reinstalar completamente el sistema no se te olvide generar un SNAPSHOT de tu VM.

En este momento el archivo de resplado debe de estar en el servidor *Samael* y su integridad ya ha sido verificada. Seguir los siguientes pasos para restaurar el sistema.

1. Reinstalar completamente el sistema desde el CD.
2. Configurar la interfaz eth1. No es necesario realizar las configuraciones de hostname, DNS, routing, fecha, hora, etc. Pero sí es importante instalar los mismos productos que se instalaron originalmente. Reiniciar al terminar la instalación.

3. Iniciar sesión nuevamente, utilizar el comando **`restore`** para obtener el respaldo del servidor SCP.





4. Reiniciar el sistema y verificar el funcionamiento del Gateway.

Importante

El comando **`restore`** puede ser ejecutado antes o después de reinstalar los productos de CheckPoint. Si no se instalan los productos solamente va a restaurar la configuración del sistema operativo

Lab #5: Identity Awarness

Atención

Antes de continuar con éste y con los siguientes laboratorios. Es necesario seguir los pasos en la sección *Activar SmartEvent* del Laboratorio #__. En caso de no realizar estos pasos *SmartEvent* no tendrá datos al momento de comenzar con el laboratorio.

Objetivo: Autenticar a los usarios al momento de conectarse a la red, obtener las credenciales de la base de datos interna y ofrecer un servicio en línea para que usuarios que no se encuentren en la base de datos, puedan darse de alta y obtener un acceso temporal de 30 minutos. Los usuarios temporales solo deben tener acceso a DNS, HTTP y HTTPS

Temas que abarca este laboratorio.

1. Identity Awareness.

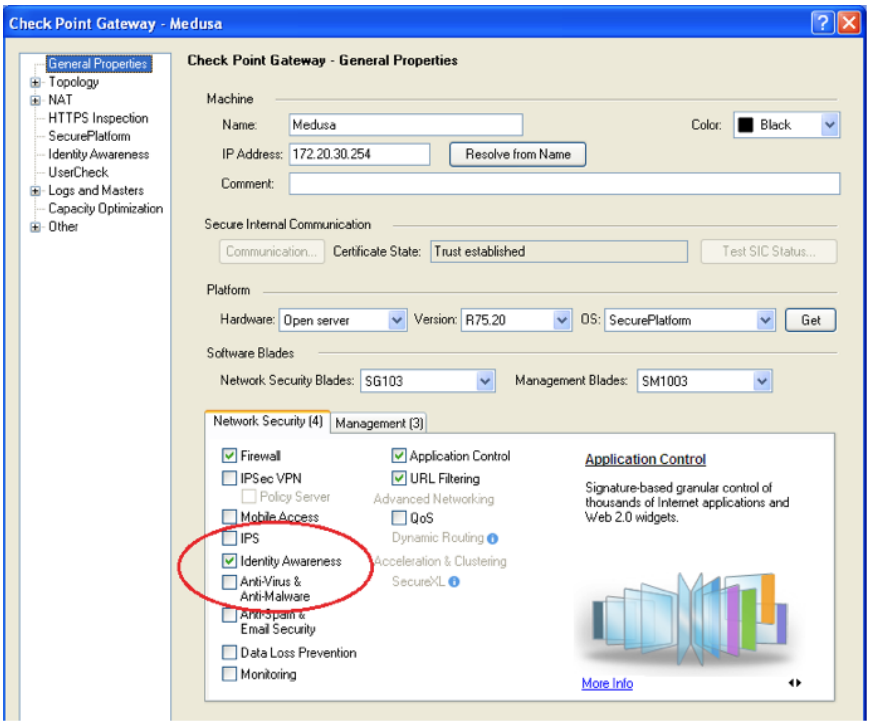
2. Captive Portal
3. User / Access Role

Tus actividades.

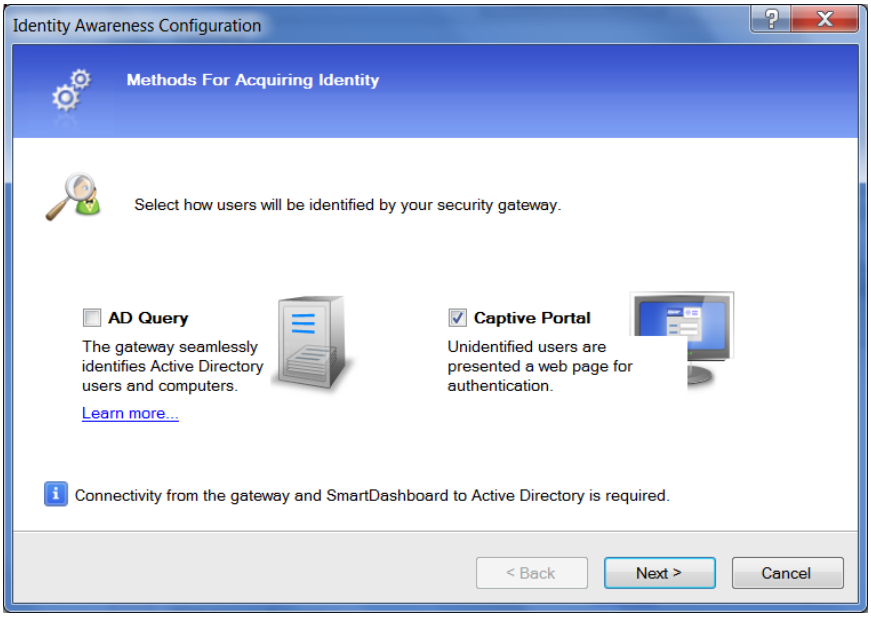
1. Crear los User/Access Roles que consideres necesarios.
2. Configurar IA con portal captivo para registrar usuarios que no están dados de alta
3. Modificar reglas de Firewall utilizando como fuente las identidades de los usuarios.

Activación de Identity Awareness

1. Abrir las propiedades generales del Gateway y activar Identity Awareness.

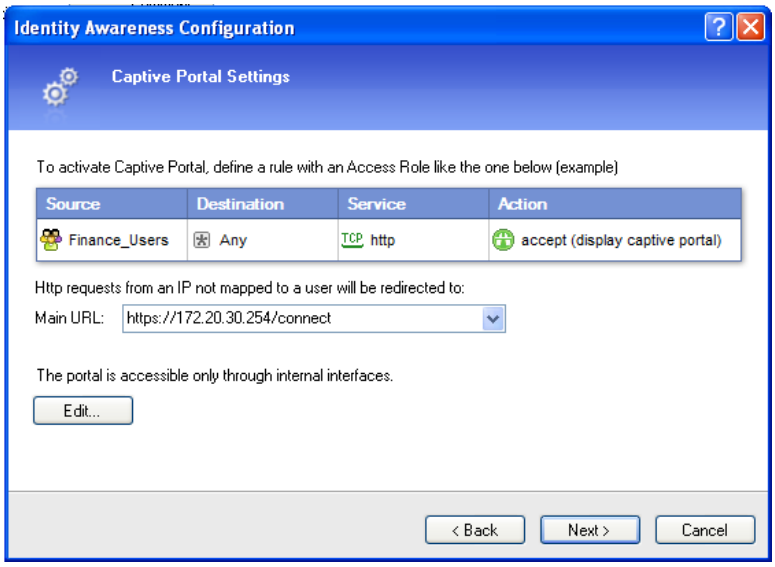


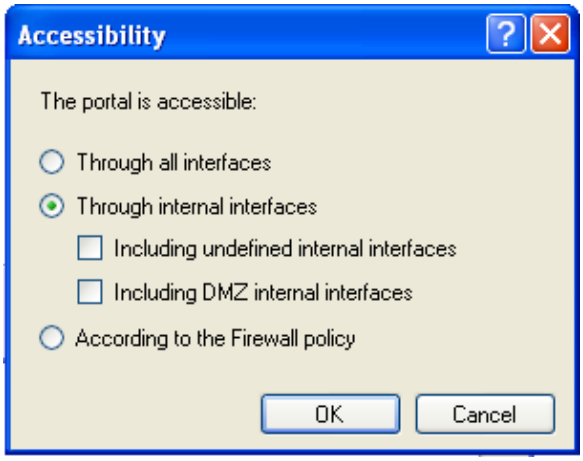
2. Seleccionar Captive Portal dentro de *Methods for Adquiring Identities.*



3. Recuerda especificar en la siguiente ventana que no utilizaremos ActiveDirectory para obtener las credenciales de los usuarios.

4. Revisar que el portal captivo escucha solamente en interfaces internas, de no ser así modificar la configuración





Configuración de *Captive Portal*

1. En las propiedades generales de Gateway seleccionar *Identity Awareness*. Abrir la ventana *Settings* ... de *Captive Portal.*

2. En la sección *Users Acces* activar *Unregistered guests login* y abrir sus *Settings*...

3. Cambiar el tiempo de acceso a 30 minutos, activar el checkbox del contrato de usuario final, Modificar en el formulario los campos que crean necesarios.

Definición de reglas & User/Access Role

Importante

Para que sea posible crear *User/Access Roles*, primero se deben de definir los usuarios y los grupos, para éste laboratorio se van a utilizar los usuarios y grupos creados en el laboratorio #3.

Definición de regla para usuarios internos.

1. Modificar la regla que da acceso a internet a la Red_Interna. Cambiar el source en *Add User/Access Role*.
2. En la ventana *Access Role* configurar las pestañas *Networks* y *Users.*
3. Dentro de *Networks*, seleccionar *Specific networks* y agregar el objeto de la red interna.
4. Dentro de Users seleccionar *Specific users/groups* y agregar el grupo de usuarios creado.
5. En Action seleccionar *accept (display captive portal)*

Definición de regla para usuarios invitados.

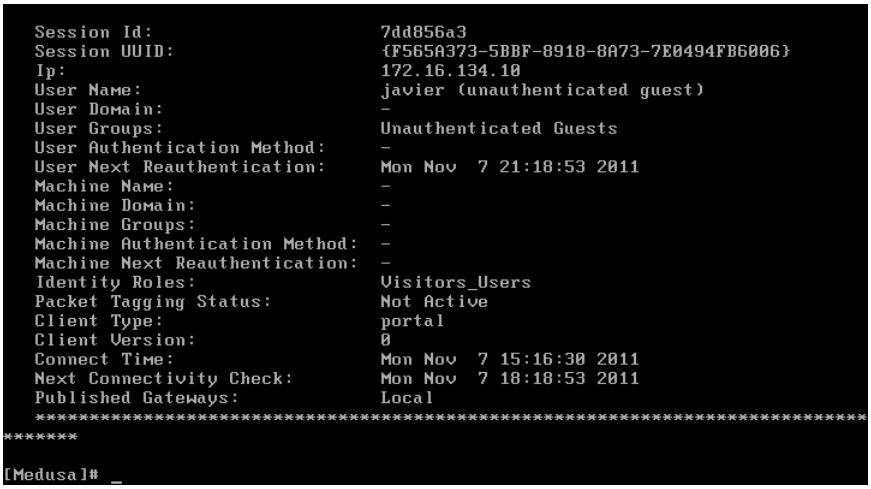
1. Modificar la regla que da acceso a internet a la Red_Interna. Cambiar el source en *Add User/Access Role*.
2. En la ventana *Access Role* configurar las pestañas *Networks* y *Users.*
3. Dentro de *Networks*, seleccionar *Specific networks* y agregar el objeto de la red interna.
4. Dentro de Users seleccionar *Any User*.
5. Agregar HTTP y HTTPS como servicios permitidos.
6. En Action seleccionar *accept (display captive portal)*
7. Instalar política y probar la configuración.

Comprobar la configuración.

Importante

La autenticación de los usuarios puede ser revocada con el comando: **`pdp control revoke_ip 10.30.40.10`**, al ejecutarse el sistema debe contestar **`Revoke command was sent to server for ip 10.30.40.10`**.

1. Al finalizar la instalación de la política abrir un navegador e intentar accesar a Internet.
2. La página debe de ser redirigida al portal captivo.
3. Escribir las credenciales del usuario y verificar la conexión a Internet. El usuario debe de poder utilizar protocolos diferentes a HTTP y HTTPS.
4. Revisar bitácoras en *SmartView Tracker*.
5. Revocar los permisos de la IP.
6. Volver a repetir la prueba, pero no utilizar las credenciales del usuario. En la ventana de autenticación seleccionar *I don't have a username and password*
7. Llenar el formulario e ingresar.
8. Ejecutar el comando **`pdp monitor all`** para ver el reporte de los usuarios activos.



Lab #6: Application Control, URL Filtering y HTTPS Inspection

Importante

La base de datos de aplicaciones puede consultarse en línea: http://appwiki.checkpoint.com

Objetivo: Configuración de reglas basadas en Usuarios, Aplicaciones Web y URLs. Evitar que los usuarios utilicen aplicaciones no permitidas utilizando SSL. Existen también usuarios que deben acceder a Youtube para lo cual deben de especificar una razón por la cual hacen uso de esa aplicación. Los usuarios con acceso a Facebook no podrán actualizar su estado.

Temas que abarca este laboratorio:

1. Application Control & URLF.
2. HTTPS Inspection
3. Cómo generar un certificado para HTTPS Inspection.
4. Categorización en la nube.
5. *Rate Limit* en el uso de aplicaciones.
6. UserCheck

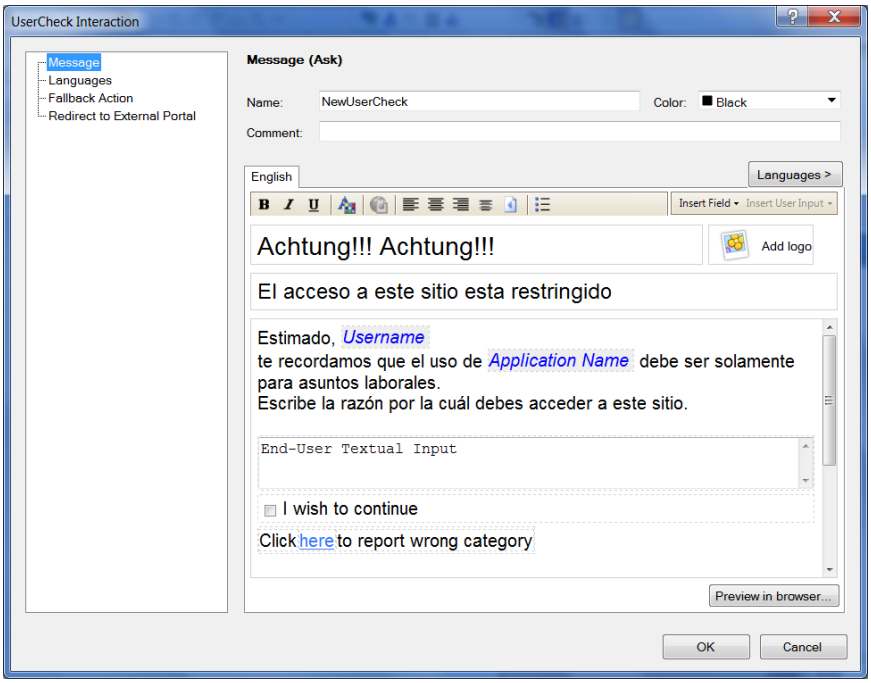
Tus actividades:

1. Personalizar UserCheck para solicitar información al usuario.
2. Definir nuevas políticas para controlar aplicaciones y widgets, así como su consumo de ancho de banda.
3. Abilitar la inspección para HTTPS.

Configuración de UserCheck

1. En propiedades generales del Gateway, activar *Application Control* y *URL Filtering.*
2. En la pestaña *Application & URL Filtering*, seleccionar *UserCheck -> New -> New Ask UserCheck*

3. Crear un nuevo sitio que muestre el nombre del usuario, la aplicaciòn que visita y que pida al usuario dar razón del uso de la aplicación. Seleccionar *Preview in browser...* para ver la presentación final al usuario.



Definición de un Rate Limit

1. Paso 1

2. Paso 2.

Definición de nuevas políticas

Importante

Los políticas que se definieron anteriormente permancecen sin cambios, las nuevas políticas son esclusivas para *AppControl & y URLF*.

1. Ir a la sección *Policy* dentro de la pestaña *Application & URL Filtering*, agregar 2 polìticas. Una debe permitir acceso a Youtube utilizando UserCheck. La segunda debe bloquear Meebo y Facebook-Posting.

Source	Destination	Applications/...	Action	Track
YoutubeUsers	Internet	YouTube	Ask NewUserCheck Once a day	Log
UserBlockedApps	Internet	Meebo MeeboMe Instant Mess... Web Based I... Facebook-po...	Block Blocked Message	Log
Any	Internet	Any Recogni...	Allow	Log

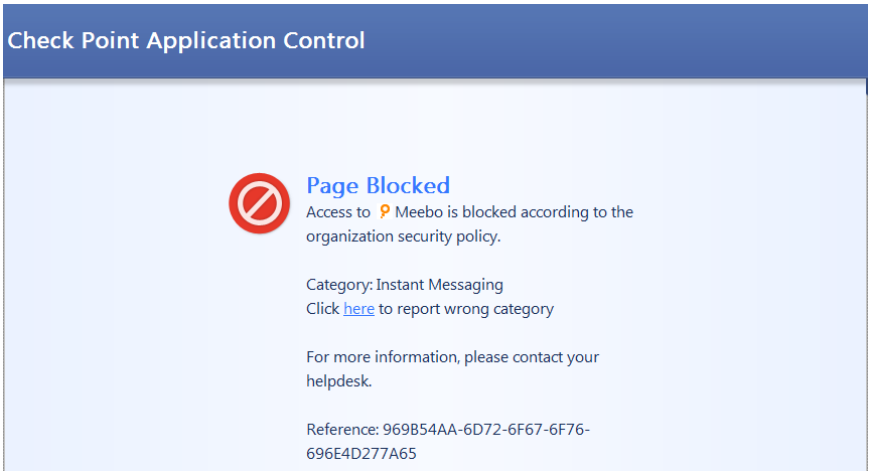
2. Instalar polìtica.

Probando UserCheck y el bloqueo de aplicaciones.

1. Probar las políticas de acuerdo a los usuarios configurados en cada política, de ser necesario revocar la IP

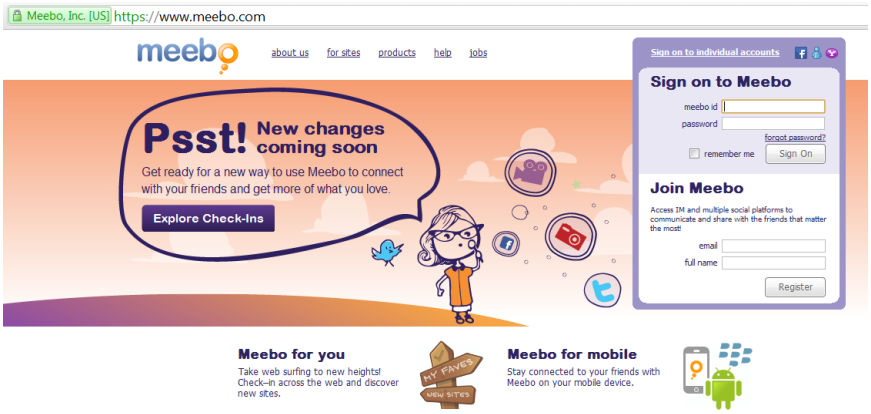
2. Abrir el navegador y visitar Youtube. UserCheck debe aparecer antes de brindar acceso al sitio.

3. Intentar abrir http://www.meebo.com. Este sitio debe de aparecer bloqueado.



4. Abrir una sesión en Facebook y actualiza tu estado.

5. Accesa a Meebo utilizando HTTPS.

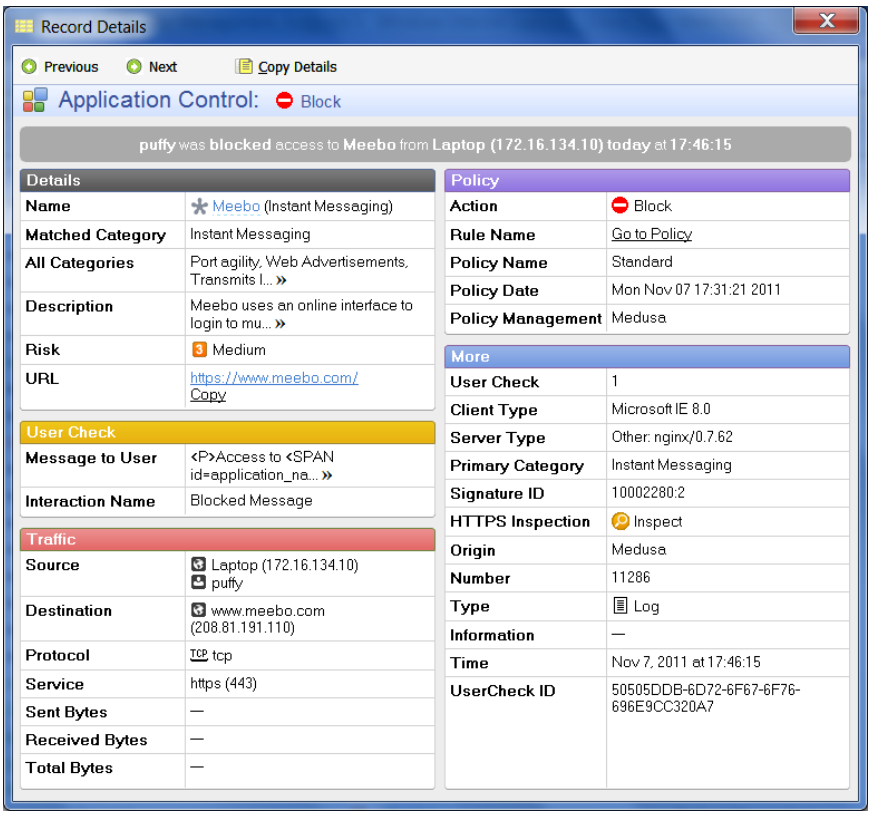


Activación de HTTPS Inspection

Importante

La inspección de HTTPS solamente es en sentido *outbound.*

1. En las propiedades generales del Gateway seleccionar *HTTPS Inspection.*
2. Crear un nuevo certificado, asiganarle un nombre y una contraseña.
3. Para Evitar el mensaje de error en el navegador cada que se visita un stio que utilice HTTPS es necesario instalar el certificado como una CA Raíz en el navegador.
4. Activar el checkbox *Enable HTTPS Inspection.*
5. Instalar polìtica
6. Volver a acceder a Meebo.com utilizando HTTPS.
7. Ubica el evento utilizando *SmartView Tracker*



Lab #7: Mobile Access Blade

Objetivo: Ofrecer un portal Web a los usuarios de la empresa. Por medio del portal el usuario podrá acceder a las aplicaciones web de la empresa, sus recursos compartidos así como aplicaciones nativas, no será necesario autenticarse siempre para poder acceder al recurso compartido. El usuario recibirá en su celular un OTP con una duración de 5 minutos el cual es necesario para poder ingresar a la aplicación. Es necesario ofrecer al usuario un entorno virtual seguro, en caso de encontrarse en un equipo público

Temas que abarca este laboratorio

1. Mobile Acces Blade
2. Web Applications, File Shares, Aplicaciones nativas.
3. Endpoint on Demand (EOD)
4. Secure Workspace
5. DynamicID
6. Check Point Mobile & Check Point VPN para iOS

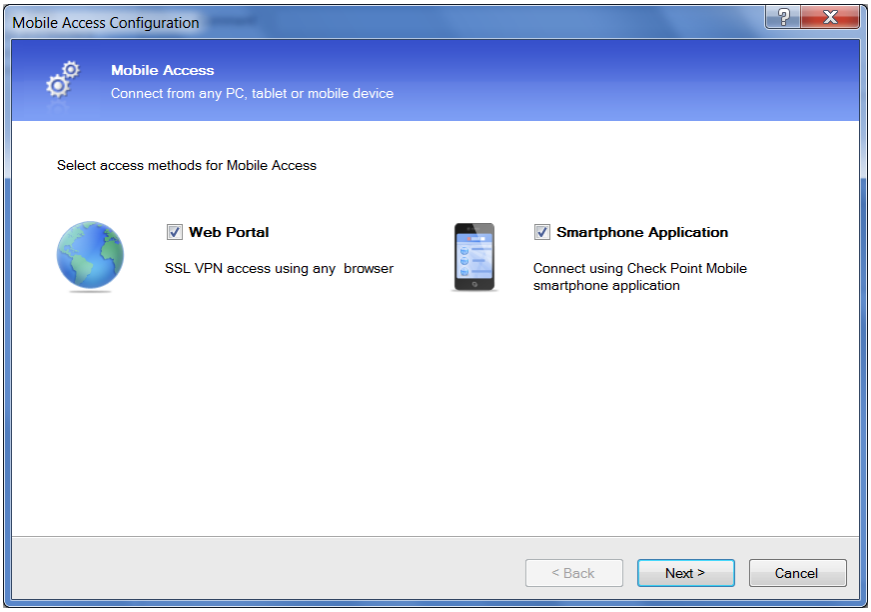
Tus actividades.

1. Configurar el portal para publicar las aplicaciones necesarias.
2. Generar las aplicaciones.
3. Activar EOD para permitir Secure Workspace
4. Configurar Dynamic ID

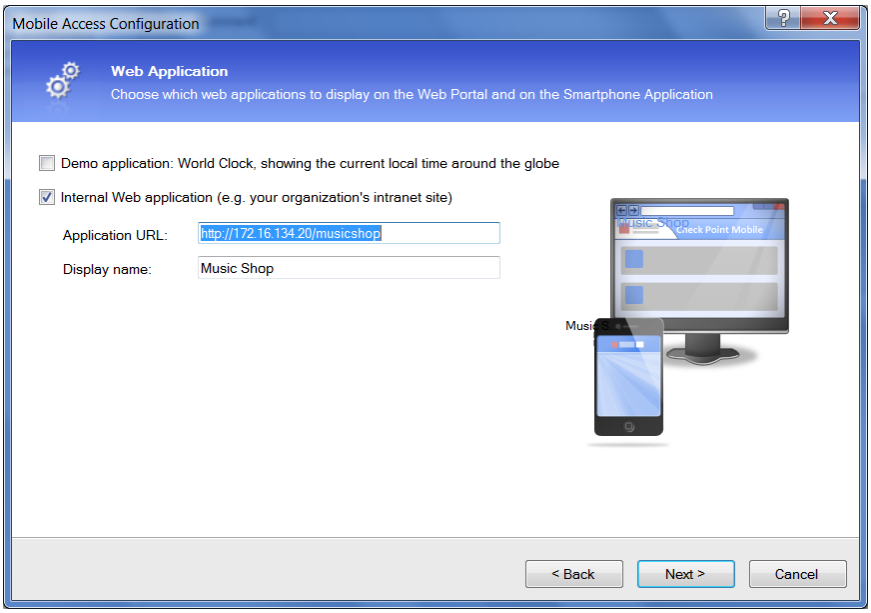
Activar Mobile Acces Blade

1. En las propiedades generales del Gateway, activar MAB, seguir las instrucciones del *Wizard.*

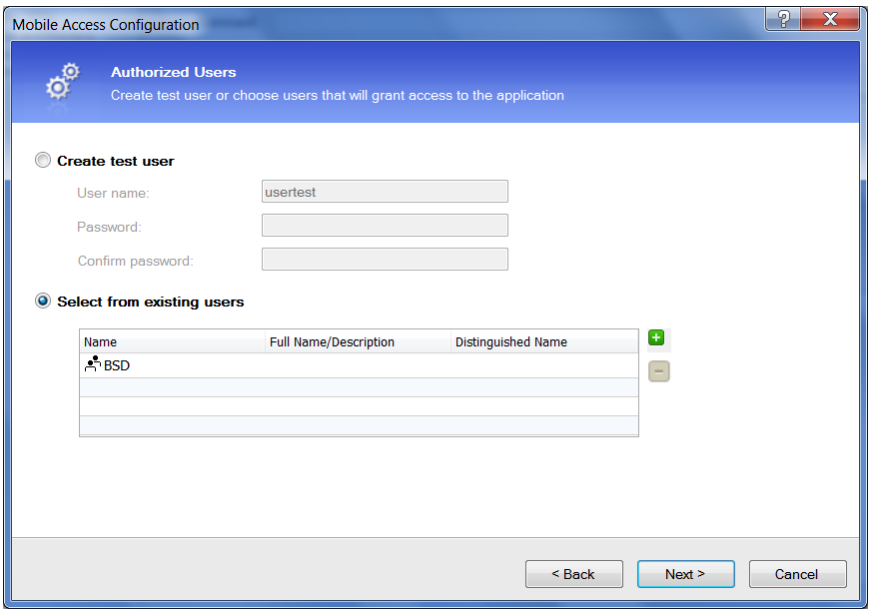
2. Seleccionar ambos métodos de acceso para MAB.



3. Utilizar la dirección http://10.30.40.20/musicshop para publicar la primera aplicaciòn.

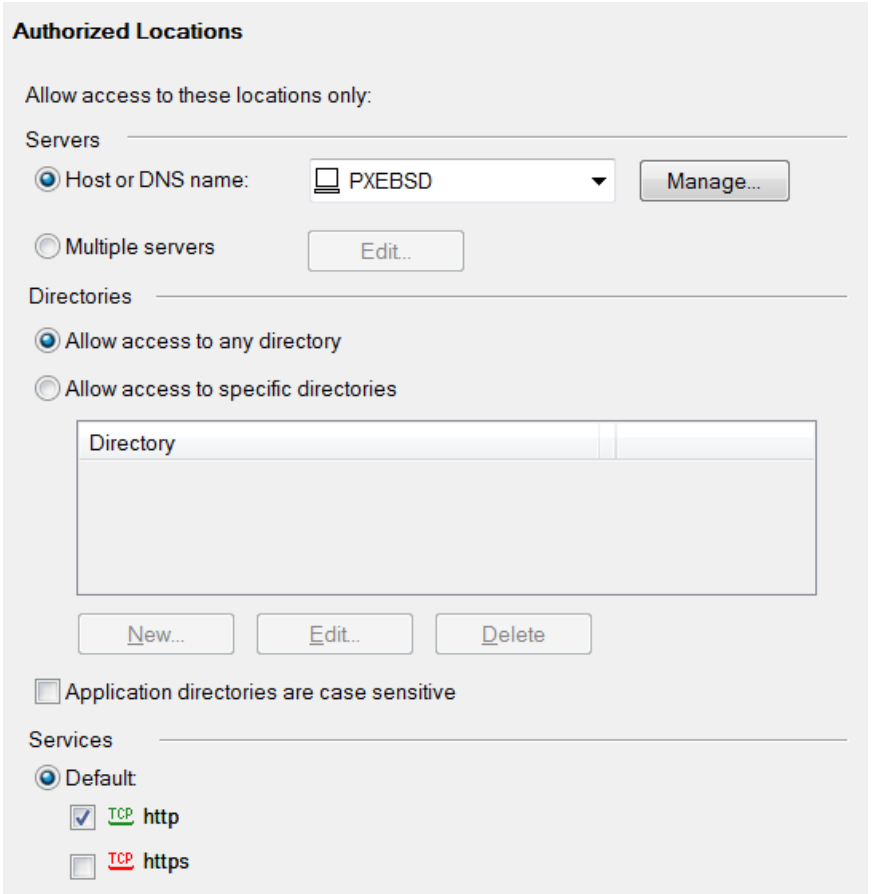


4. No crear un usuario nuevo, seleccionar los grupos previamente creados.

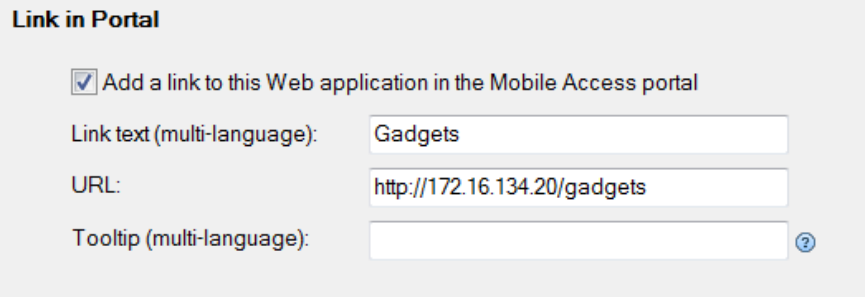


Creación de Aplicaciones Web

1. Ir a *Mobile Acces -> Applications -> Web Applications ->New.*.
2. Nombrar *Gadgets*, a la aplicación
3. Dentro de *Authorized Locations* seleccionar como servidor el objeto *Samael*



4. En la sección *Link in Portal*, configurar el URL de la aplicación *http://10.30.40.20/gadgets*

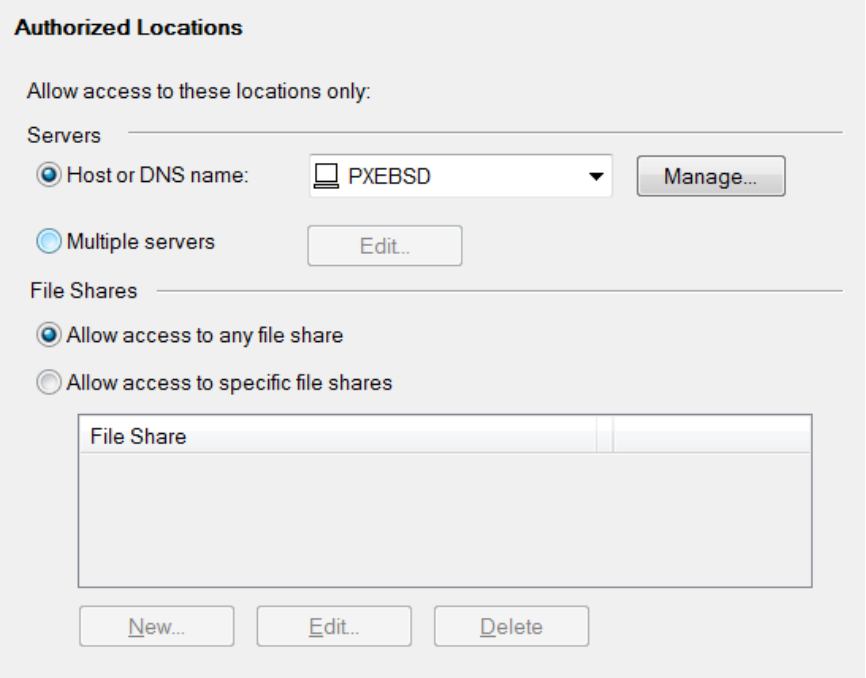


5. Crear de la misma manera aplicaciones para los sitios *moviecompany, nightclub y partytime.*

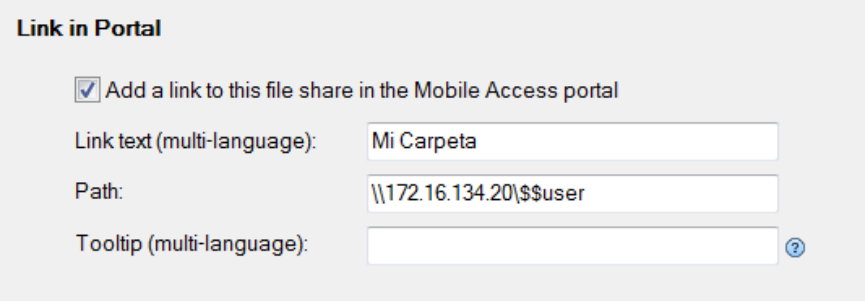
Creación de Recursos Compartido

1. Ir a *File Shares -> New...*

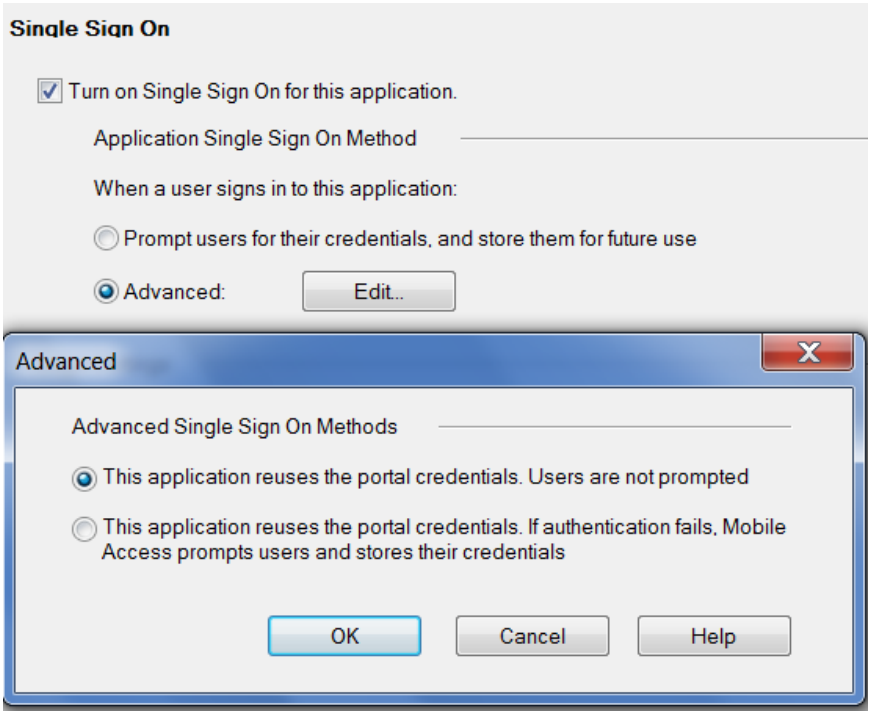
2. Seleccionar el servidor de recursos compartidos y permitir acceso a cualquier carpeta.



3. En *Link in Portal*, utilizar el Path **`\\10.30.40.20\$$user`**

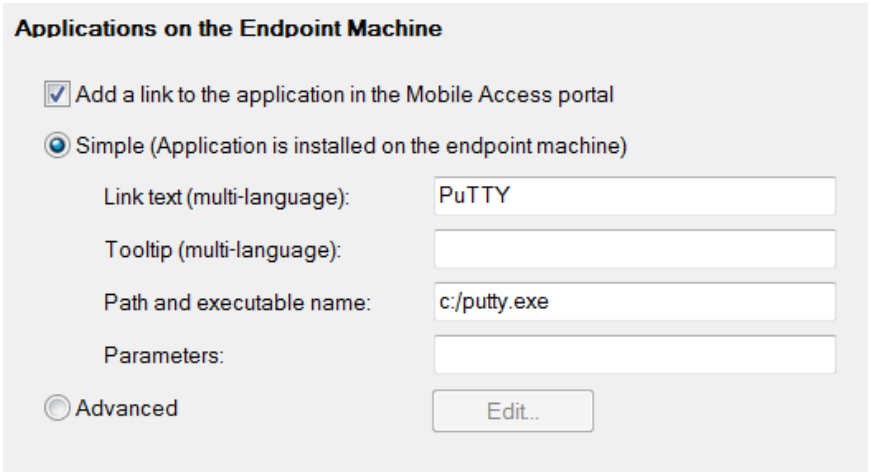


4. Configurar SSO dentro de *Additional Settings -> Single Sign On.*Seleccionar *Advanced -> Edit....* Seleccionar *This application reuses the portal credentials. Users are not prompted.*



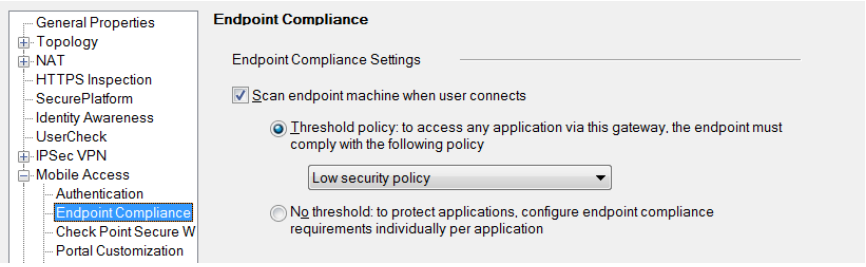
Creación de una aplicación nativa

1. Ir a *Native Applications -> New.*.
2. Seleccionar como Host *Samael* y como servicio *SSH.*
3. Seleccionar *Endpoint Applications*, agregar un Link a la aplicación y escribir el la ruta de la aplicación PuTTY que debe de estar en C:/

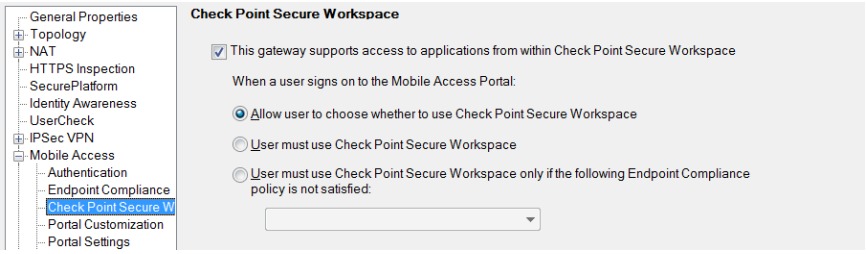


Activación de Endpoint Compliance & Secure Workspace

1. Dentro de las propiedades generales del Gateway ir a *Mobile Access -> Endpoint Compliance.* Activar Endpoint y escojer la política *Low security profile.*



2. Dentro de las propiedades generales del Gateway ir a *Mobile Access -> Checkpoint Secure Workspace.* Activar Secure Workspace y seleccionar *Allow user to choose whether to use CP Secure Workspace.*.



Configuración de Dynamic ID por SMS

Importante

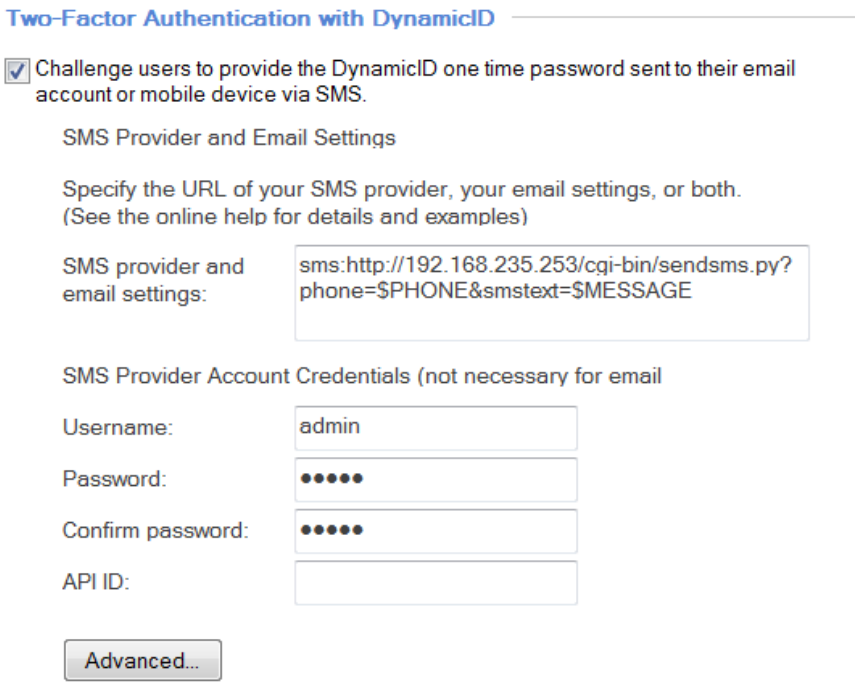
Para configurar Dynamic ID por SMs es necesario contar con un servicio de mensajería adicional a las funcionalidades del Gateway. Las configuraciones realizadas en este laboratorio cambiarán dependiendo del servicio SMS que se contrate.

1. Dentro de Mobile Access abrir *Users and Authentication -> Authenticaion -> Authentication to Gateway*

2. Activar el checkbox *Challenge users to provide....* El servicio donde se enviará el SMS es: **`sms:http://<IP-SMS-SERVER>/cgi-bin/sendsms.py?phone=$PHONE&smstext=$MESSAGE`**. El *Username y Password* para este laboratorio no on importantes, puedes poner cualquier texto pero no deben de quedar vacíos los campos.

Importante

Para probar la conexión con el servidor SMS, abrir un navegador y abrir el URL anterior mencionando número de celular y mensaje: **`http://<IP-SMS-SERVER>/cgi-bin/sendsms.py?phone="52155xxxxxxxx"&smstext="Testing SMS"`**

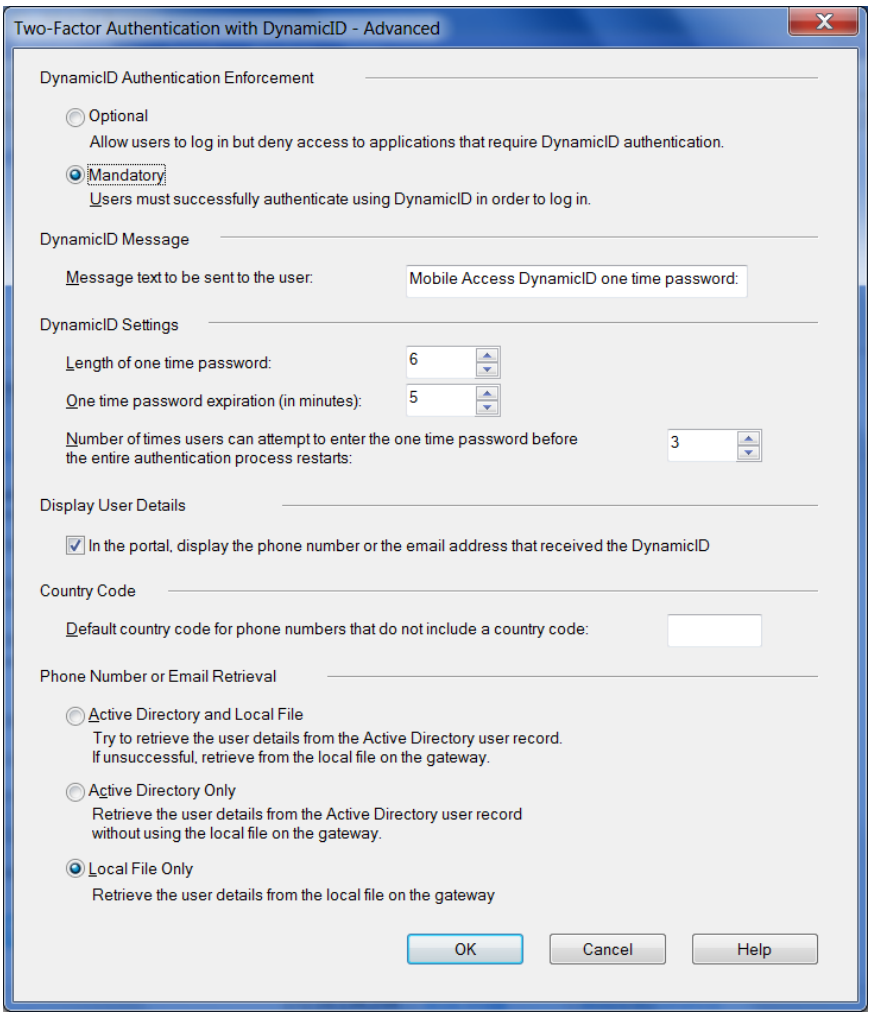


Asignar números telefónicos a los usuarios.

1. Los números telefónicos puedes ser asignados de varias formas, en las propiedades de los usuarios creados previamente por ejemplo o en un archvio de texto localizado en el Gateway. Para éste laboratorio debes modificar las propiedades del usuario mediante SmartDashboard e incluir el número de tu celular. El número de celular debe de tener el código de país*(52)* y de ciudad *(155)*.

2. **Opcionalmente** puedes realizar los siguientes pasos para añadir usuarios por línea de comando.

3. Abrir las propiedades avanzadas. Dentro de *DynamicId Authetication Enforcement* activar *Mandatory*. Dentro de la sección *Phone Number retrieval* seleccionar *Local File Only*.



4. Agregar usuario y número de teléfono al archivo *SmsPhones.lst*

```
$echo "puffy 5215512277151" > $CVPNDIR/conf/SmsPhones.lst
```

Politicas en Mobile Acces Blade

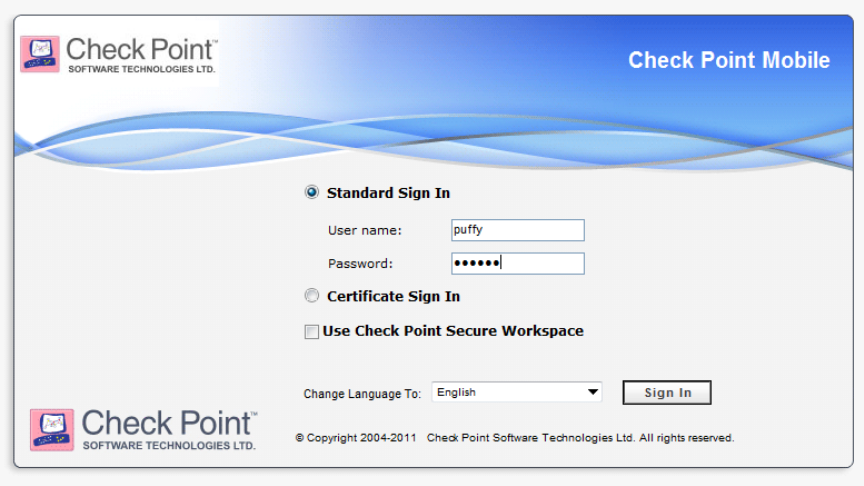
1. En la sección *Policy* Se deben agregar todas las aplicaciones a las que tiene autorizado el usuario.

N...	Users	Applications	Install On	Comment
1	BSD	webapp_172.16.134.20 FileShareSamba Gadgets SSH_BSD	Medusa	Rule created automatically by Mobile Access wizard.

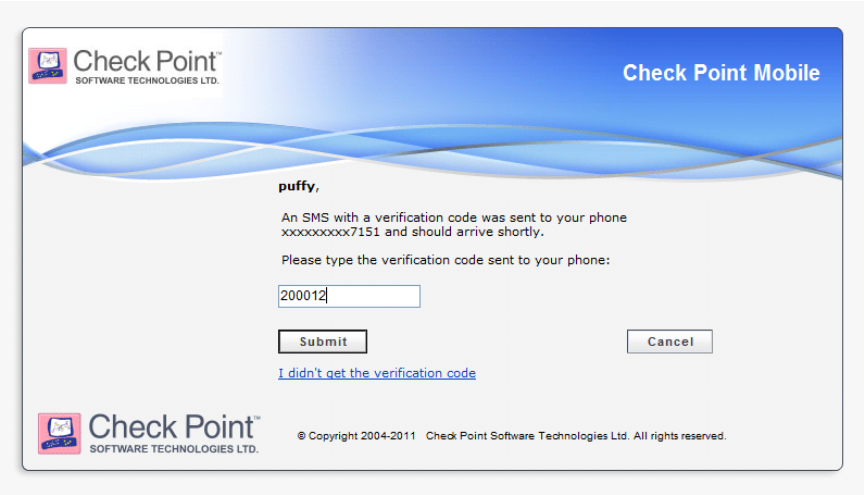
2. Instalar política el terminar todas las configuraciones.

Experiencia de usuario con Mobile Acces Blade

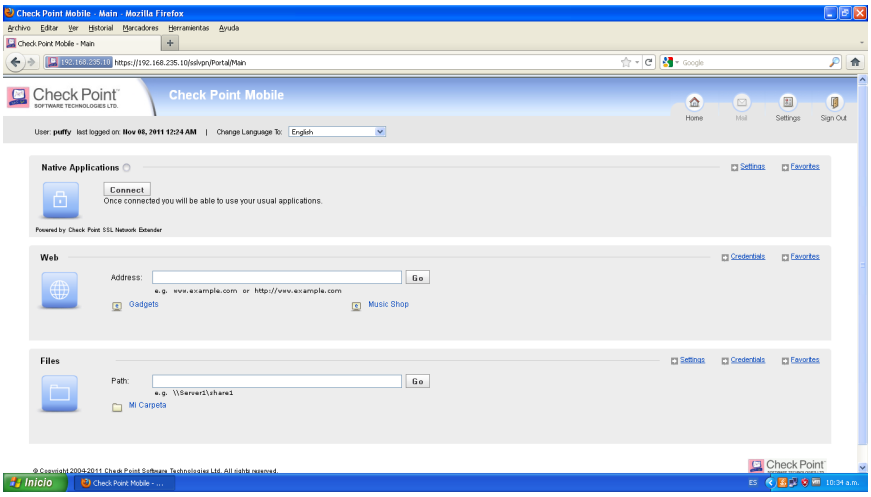
1. Abrir un navegador e ir a la dirección *https://192.0.2.254/sslvpn.* Aparece la pantalla de Login de *Checkpoint Mobile;* escribir nombre de usuario y contraseña. De forma alternativa se puede seleccionar la casilla *Use Checkpoint Secure Workspace.*



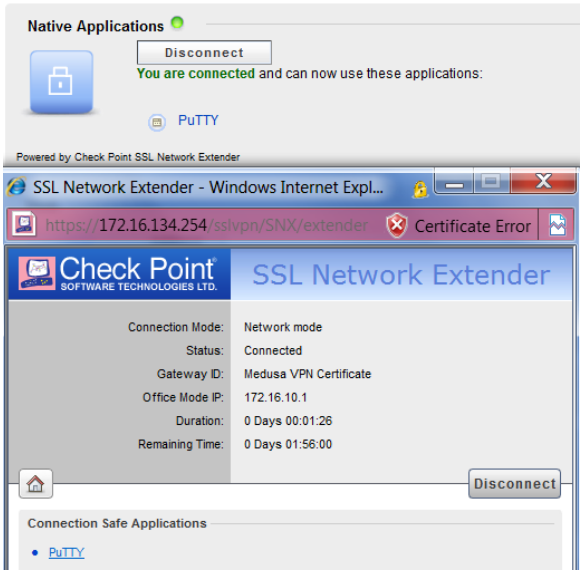
2. Si el inicio de sesión es exitoso, el Gateway enviará un SMS con un One-Time-Password que debes ingresar antes de los próximos 5 minutos.



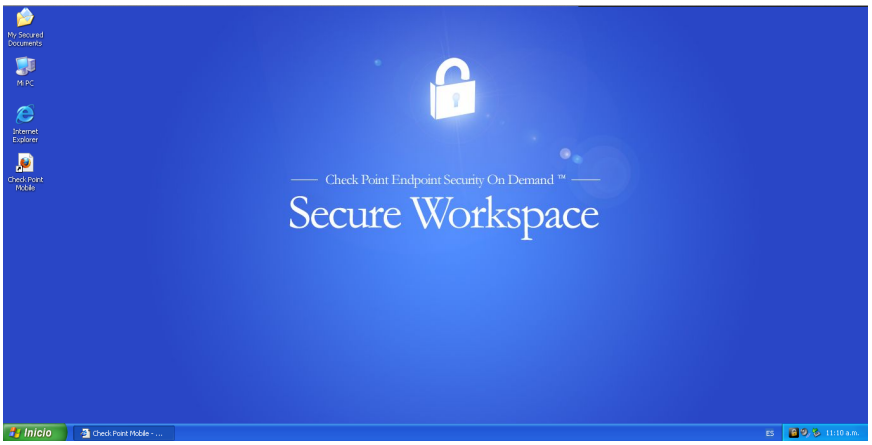
3. Al iniciar la sesión abrirá el portal de Checkpoint Mobile, en el cual podemos ver las aplicaciones web creadas, aplicaciones nativas y recursos compartidos



4. Para utilizar las aplicaciones nativas es necesario conectar la VPN SSL, dentro de la sección *Native Applications* presionar *Connect* para iniciar *SSL Network Extender*.



5. En caso de haber selecionado *Use Checkpoint Secure Workspace*, el portal se mostrará dentro del entorno virtual



Lab #8: SmartEvent

Activar SmartEvent

Objetivo: Activar SmartEvent y los eventos que permitan ver los usuarios activos, el uso de aplicaciones y el consumo de ancho de banda por usuario.

Temas que abarca este laboratorio:

1. Activación y configuración inicial de SmartEvent

2. Políticas y Queries

Tus actividades:

1. Activar SmartEvent y sus componentes.

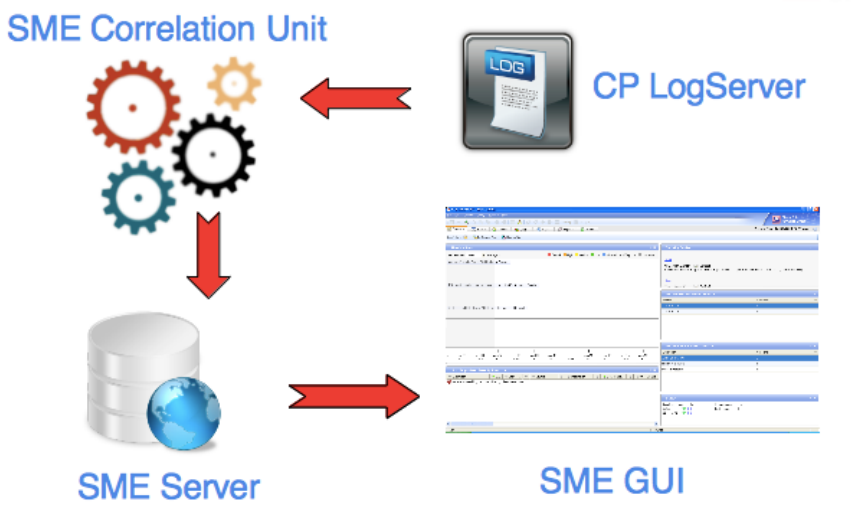
2. Activar eventos para Identity Awareness.

Importante

La activación de *SmartEvent* debe de realizarse antes de comenzar el laboratorio de *Identity Awareness*, de lo contrario no se tendra información para ser visualizada.

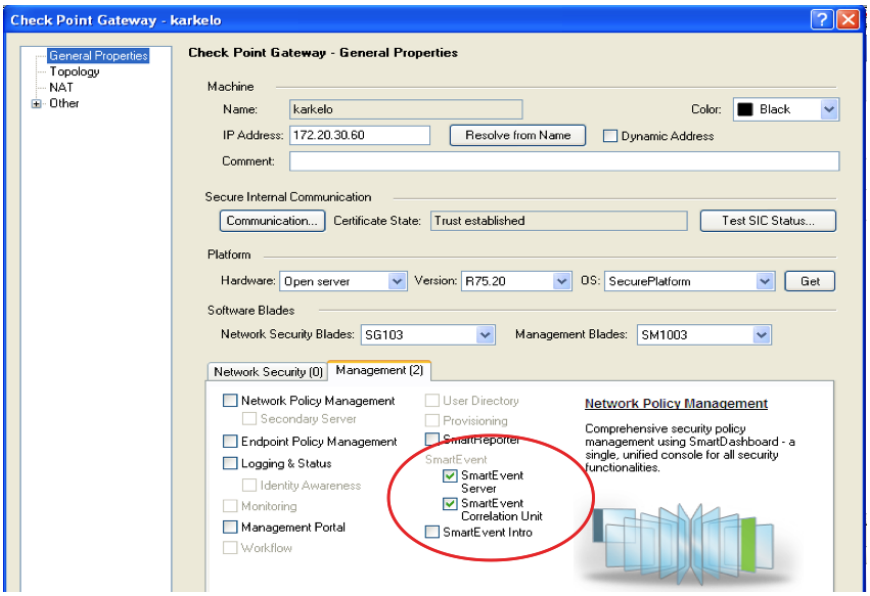
SmartEvent cuenta con 3 componentes:

- SmartEvent Correlation Unit
- SmartEvent Server
- SmartEvent GUI

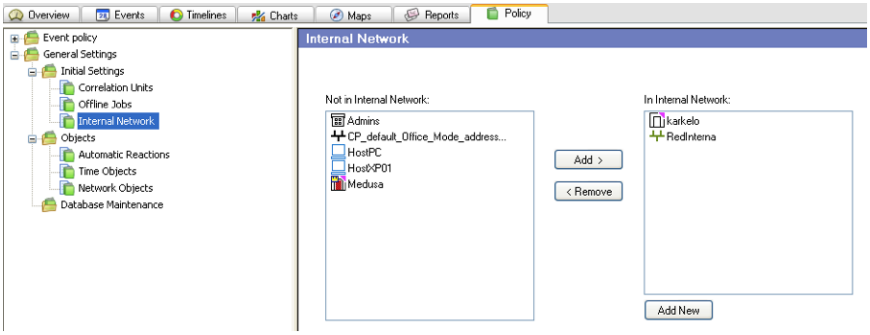


Todos los componentes ya se encuentran instalados en el *SmartCenter Server*, seguir los siguientes pasos para activarlo y comenzar la correlación de los eventos.

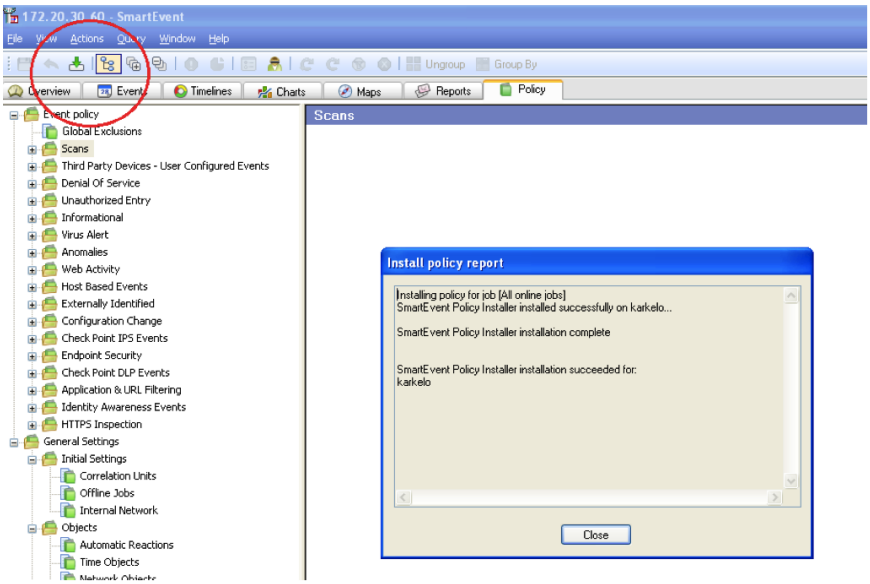
1. Editar las propiedades generales del Gateway.
2. Dentro de la pestaña *Management* activar los blades *SmartEvent & SmartEvent Correlation Unit.*



3. Abrir el cliente de *SmartEvent*.
4. *Definir red interna:* En esta pantalla debe de seleccionarse el objeto de red interna que se definió desde el primer laboratorio.

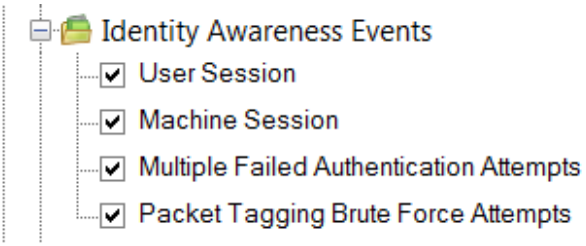


5. *Instalar Política:* el último paso es instalar la política en SME. Se puede aplicar directamente desde la configuración inicial o desde *Actions -> Install Event Policy.*



Activar Eventos para Identity Awareness

1. Seleccionar *Policy -> Identity Awareness Events* Activar los eventos *User Session* y *Machine Session*



2. Activar política en Smart Event

Acerca de este documento

Todo el contenido de este documento es material original del autor, no es de ninguna manera documentación oficial de Check Point Software Technologies. La mención de cualquier marca comercial es meramente de caracter informativo.

Revisiones.

- Rev 1.5 - Octubre 2012