

Estrategia Trusted Connection™ Serie de White Papers

Reducción del riesgo de sistemas fuera de control con ePolicy Orchestrator 3.5

Segundo de la Serie



McAfee®
System Protection

Soluciones líderes de mercado en prevención de intrusiones



NOTA DE DERECHOS DE AUTOR

Copyright © 2004 Network Associates Technology, Inc. Todos los derechos reservados. Ninguna parte de esta publicación podrá ser reproducida, transmitida, transcrita, almacenada en sistemas de acceso, o traducida en cualquier idioma, de cualquier forma o por cualesquier medios, sin el permiso por escrito de Network Associates Technology, Inc. o de sus proveedores o empresas afiliadas. Para obtener dicho permiso, escriba al departamento jurídico de Network Associates: 5000 Headquarters Drive, Plano, Texas 75024, EE.UU., o llame a +1-972-963-8000.

Índice

| | |
|--|----|
| ¿Qué es la estrategia Trusted Connection de McAfee? | 3 |
| Introducción | 4 |
| ¿Qué es McAfee ePolicy Orchestrator? | 5 |
| Detección de sistemas fuera de control en ePolicy Orchestrator 3.5 | 5 |
| Panorama de la arquitectura | 6 |
| El sensor de sistemas fuera de control | 8 |
| El Servidor | 8 |
| Distribución de sensores de sistemas fuera de control | 9 |
| Medidas de reacción a sistemas fuera de control | 10 |
| Sistemas y dispositivos imposibles de administrar | 12 |
| Preguntas más frecuentes | 13 |
| Acónimos utilizados en este documento | 14 |

Aviso Legal

© Copyright 2004 Network Associates Technology, Inc. Todos los derechos reservados.

Este documento contiene información confidencial y/o reservada o secretos comerciales de Network Associates, Inc. Ninguna parte de esta publicación puede ser reproducida, transmitida, transcrita, almacenada en sistema de acceso, distribuida, revista, modificada o traducida en cualquier idioma, de cualquier forma o por cualesquier medios, sin el permiso escrito de Network Associates Technology, Inc., de sus proveedores o de sus empresas afiliadas. Para obtener dicho permiso, escriba al departamento jurídico de Network Associates: 5000 Headquarters Drive, Plano, Texas 75024, EE.UU., o llame a +1-972-963-8000.

Network Associates, Inc. no hace ninguna declaración ni ofrece cualquier garantía respecto al contenido de esta obra, eximiéndose específicamente de cualquier garantía explícita o implícita de posibilidad de comercialización o adecuación a cualquier finalidad específica. Network Associates reserva para sí el derecho de revisar esta obra y de realizar alteraciones en su contenido, a cualquier momento, sin ninguna obligación de notificar a cualquier persona o empresa respecto a las revisiones o alteraciones.



Reducción del riesgo de sistemas fuera de control con ePolicy Orchestrator 3.5

Panorama Técnico

Este *white paper* es el segundo de la serie de la Estrategia Trusted Connection de McAfee. La serie fue creada para presentar ideas y detalles sobre partes específicas de la Estrategia Trusted Connection™ de McAfee.

Este trabajo se refiere a la *Reducción del riesgo de sistemas fuera de control con ePolicy Orchestrator 3.5*. El número de referencia de este documento es White Paper 2.

La información presentada en este documento es un panorama de cómo usar ePolicy Orchestrator 3.5 para monitorear — en tiempo real — sistemas fuera de control o desprotegidos que se conectan a la red interna. Aquí, el objetivo no es demostrar estrategias de bloqueo automático, que se presentarán en *white papers* o perfeccionamientos del producto subsecuentes.

¿Qué es la Estrategia Trusted Connection de McAfee?

La estrategia Trusted Connection de McAfee es una forma de asegurar la conformidad de los sistemas con la seguridad antes que se conecten a la red de la empresa. Esta estrategia está basada en varias iniciativas tecnológicas de McAfee Security y en asociaciones fundamentales con los principales fabricantes de VPN, acceso remoto, sistemas inalámbricos y redes, del mercado.

El objetivo de esta estrategia es permitir que los usuarios de McAfee verifiquen la conformidad de los sistemas con la seguridad antes que se conecten a la red, además de ponerlos automáticamente en conformidad, si fuese necesario, desde puntos externos e internos de acceso. Con dichas soluciones, los administradores de TI pueden asegurar que sólo los sistemas configurados de forma segura puedan conectarse a su red corporativa, logrando mayor control y mejorando la protección preventiva contra vulnerabilidades y contra la transferencia de virus, *worms* y Troyanos.

Introducción

Una de las dificultades que enfrenta cualquier organización en la administración de la seguridad de sus sistemas y para asegurar la protección total de la empresa es que, para fiscalizar la conformidad con las políticas, es necesario saber que el sistema existe. Dicha situación es complicada por el hecho de que, en la mayoría de las redes, la única exigencia para la conexión es el acceso físico. No se necesita ninguna autenticación adicional. Por lo tanto, cualquier visitante que entre en el edificio de una empresa y use sin intención una conexión de red disponible representa una considerable amenaza para dicha empresa.

Esa situación puede ocurrir con:

- Contratistas, empleados subcontratados o socios de negocios — cuyas computadoras no son administradas por su infraestructura de seguridad — conectándose a la red.
- Recursos o sistemas desconocidos o no autorizados en la empresa que se conectan a la red, aunque puedan pasar inadvertidos.
- Visitantes en salas de reunión que se conectan a la red para sincronizar sus *e-mails*.

Una única computadora que no cuente con una protección administrada adecuada puede constituir una amenaza para toda la red, y eso significa que conocer todos los sistemas conectados a la red es esencial para el éxito de la protección de la empresa. Los sistemas que se conectan a la red y que no son conocidos o que no siguen la política de seguridad definida son considerados *sistemas fuera de control*.

Existen varias estrategias de creación y mantenimiento de una lista de todos los sistemas conectados a una red, pero cada una de ellas presenta considerables desventajas:

| Estrategia | Desventaja |
|--|--|
| Mantener manualmente una lista de todos los sistemas de una red | No es posible en la mayoría de las redes de hoy, pues el entorno de red es muy dinámico para que una única persona (incluso más de una persona) mantenga actualizado dicho tipo de lista. |
| Registro de los sistemas con <i>scripts</i> de login | Los <i>scripts</i> de login se ejecutan <i>tras</i> la autenticación de un usuario en alguna entidad (por ejemplo, un dominio del Windows). Por lo tanto, el <i>script</i> de login no es prerequisite para que un sistema se conecte a la red. |
| Exploraciones periódicas a través de una herramienta de exploración activa (por ejemplo, Nmap) o una herramienta semejante de exploración de vulnerabilidades | Si las exploraciones son periódicas, sólo serán descubiertos los sistemas fuera de control conectados en el exacto momento de la exploración. El aumento de la frecuencia de las exploraciones para compensar ello no es viable, pues pueden ser: <ul style="list-style-type: none"> ▪ Muy lentas. ▪ Invasivas, generando mucho tráfico de red y, a veces, generando un tráfico que afecta negativamente a los servicios sometidos a la exploración. <p>La ejecución de las Exploraciones también puede ser impedida por programas de <i>firewall</i> de <i>desktop</i>, si ellos han sido configurados para ignorar todas las conexiones hechas desde fuera, haciendo al sistema invisible para programas de exploración.</p> |
| Importación periódica de un directorio (por ejemplo, Active Directory) | Aunque este método reduzca mucho el tiempo que gasta la administración con el mantenimiento del directorio, posee las mismas limitaciones de las dos estrategias anteriores. Como en la exploración activa, es periódico y, como en los <i>scripts</i> de login, no permite que ePolicy Orchestrator vea los sistemas de la red que no estén registrados en el Active Directory. |

Para resolver dichas dificultades y las limitaciones de las soluciones existentes, McAfee presenta un enfoque innovador de detección y administración de sistemas fuera de control, con el lanzamiento del McAfee ePolicy Orchestrator 3.5.

¿Qué es McAfee ePolicy Orchestrator?

McAfee ePolicy Orchestrator (ePO) es la solución líder de mercado para administración de sistemas – que proporciona a la empresa una defensa preventiva contra amenazas y ataques. Brindando una amplia e incomparable administración de seguridad de sistemas al menor costo de propiedad, asegura la conformidad con la política de seguridad de sistemas y la eficacia de la protección de los sistemas, impidiendo las dispendiosas interrupciones de los negocios causadas por infecciones y ataques de *malware*. Con el eje central de las soluciones de protección de sistemas de McAfee, los administradores pueden tomar la iniciativa de reducir el riesgo de sistemas fuera de control y no conformes, mantener actualizada la protección, configurar y fiscalizar las políticas de protección y monitorear las condiciones de seguridad 24 horas al día, 7 días por semana, desde una única consola centralizada y con verdadera flexibilidad de nivel corporativo.

Detección de sistemas fuera de control en ePolicy Orchestrator 3.5

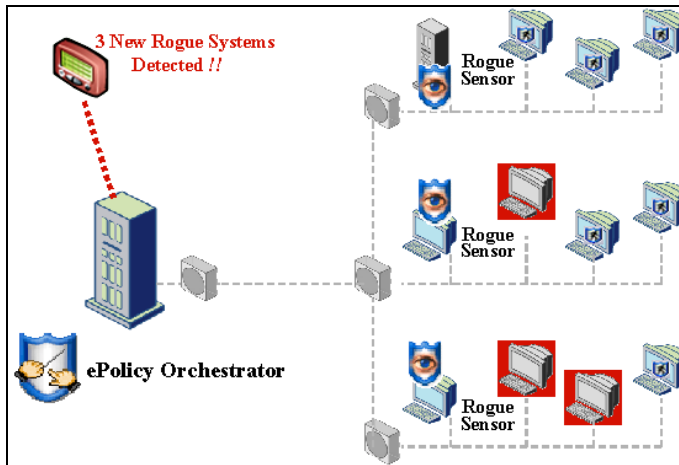
La detección de sistemas fuera de control y un nuevo recurso de la próxima versión del ePolicy Orchestrator 3.5. Dicho recurso fue creado para aumentar la conformidad con las políticas en las empresas, identificando todos los sistemas fuera de control o desprotegidos, además de permitir que ePolicy Orchestrator invoque una reacción por políticas en dichos sistemas.

En el centro de la solución está un sensor lógico (*software*) que utiliza el monitoreo pasivo para detectar todos los sistemas que participan de la red. Específicamente, el sensor escucha transmisiones de L2 (para saber más, véase [Sobre el modelo de referencia OSI en 7 niveles](#) en la página 7). Las computadoras que participan de una red tienden a hacer transmisiones múltiples frecuentes, especialmente cuando entraron en una red poco tiempo atrás. Por lo tanto, los nuevos sistemas son normalmente detectados por el sensor en cuestión de segundos luego de la primera conexión a la red. Los sensores distribuidos por toda la empresa relatan todos los sistemas detectados al servidor ePolicy Orchestrator y el servidor determina cuáles de dichos dispositivos están fuera de control.

Panorama de la arquitectura

El diagrama dado a continuación presenta un panorama de la arquitectura de detección de sistemas fuera de control.

Figura 1: Panorama de la arquitectura



Al menos un sensor de sistemas fuera de control debe estar instalado en cada segmento L2 en toda la empresa, ya que los sensores detectan sistemas por transmisiones (que se propagan sólo a través de un segmento L2). A medida que se detectan los sistemas, el sensor utiliza el protocolo HTTPS para enviar mensajes que describen los sistemas al servidor ePolicy Orchestrator. El sensor nunca intenta clasificar los sistemas como “fuera de control” o “administrados”; simplemente relata todo lo que ve.

Cuando el servidor ePolicy Orchestrator recibe un mensaje de **sistema detectado**, inspecciona la base de datos para determinar si el sistema debe ser clasificado como “fuera de control” o “administrado”. Un sistema es considerado fuera de control si:

- No está presente en la base de datos de sistemas administrados de ePolicy Orchestrator, y
- El agente ePolicy Orchestrator del sistema no está comunicándose activamente con el servidor.



ePolicy Orchestrator fiscaliza la política en los sistemas a través de un pequeño agente de software que funciona en los sistemas administrados. Dichos agentes son responsables de la verificación periódica del servidor ePolicy Orchestrator para obtener las configuraciones de políticas más recientes. Si un agente deja de verificar y confirmar su configuración de política, esto se considerará una violación de la política porque el servidor ePolicy Orchestrator no podrá confirmar si las configuraciones del sistema están actualizadas.

La dirección MAC (Control de Acceso a los Medios) detectada del sistema es usada como principal clave en la búsqueda de la base de datos de sistemas administrados de ePolicy Orchestrator; el *hostname* también puede ser usado para reducir falsos positivos en los casos que un sistema utiliza varias interfaces de red, por ejemplo, un *laptop* con conexión inalámbrica y Ethernet (consulte detalles en las [Preguntas más frecuentes](#) en la página 13).

Un sensor informa sobre un cierto sistema la primera vez que lo detecta (por ejemplo, cuando el primer paquete transmitido que contenga la dirección MAC de dicho sistema es recibido por el sensor) y, enseguida, empieza a informar sólo una vez por período de tiempo (configurable, que es de 1 hora si no se define nada en contrario). Siempre que el servidor recibe un mensaje de **sistema detectado** respecto a un sistema detectado anteriormente, recalcula y actualiza el estado de “fuera de control” y otra información asociada al sistema. Dicho modelo de procesamiento tiene algunas consecuencias altamente deseables:

- La información de los sistemas fuera de control en la base de datos del ePolicy Orchestrator representa el estado de la red en el momento, no una instantánea de algún momento anterior, lo que ocurre con las herramientas de exploración activas.
- El administrador puede saber si un sistema fuera de control aún está activo, cuándo estuvo activo por última vez y por cuánto tiempo estuvo en la red. La sección de sistemas fuera de control de la consola del ePolicy Orchestrator clasifica sistemas **inactivos** (sistemas que no se han comunicado durante un cierto período de tiempo – que se puede configurar) separadamente de los **sistemas activos fuera de control**, de forma que el administrador puede dedicarse a las amenazas actuales contra la red.
- La arquitectura del servidor queda muy sencilla porque el estado de cada sistema fuera de control y otras propiedades permanecen actualizados sin ningún procesamiento explícito en segundo plano. El Servidor procesa los sucesos a medida que llegan.

Sobre el modelo de referencia OSI en 7 niveles

El modelo de referencia OSI (Interconexión de Sistemas Abiertos) es un modelo teórico de cómo las aplicaciones en red se comunican entre sí. Dicho modelo describe una pila de protocolos en 7 niveles, donde cada nivel representa un protocolo de red que aprovecha los recursos del nivel inmediatamente inferior. Aplicaciones tales como HTTP funcionan en el **Nivel 7**, mientras que los medios físicos son representados en el **Nivel 1**. Los niveles importantes para la comprensión de este documento son los siguientes:

Nivel 2 — Nivel del Enlace de Datos: Ethernet es un ejemplo de protocolo de L2. Los dispositivos son dirigidos a través de su dirección MAC (Control de Acceso a los Medios) de 6 octetos. Ethernet permite el envío de paquetes a un único dispositivo o la transmisión múltiple simultánea (*broadcast*) de dichos paquetes a todos los dispositivos de la red. Los dispositivos que recibirán los paquetes transmitidos entre ellos son considerados pertenecientes al mismo dominio de transmisión múltiple simultánea; un dominio de transmisión múltiple simultánea es, a veces, denominado “segmento”. Se pueden usar *hubs*, *switches* y puentes para conectar dispositivos en un dominio de transmisión múltiple simultánea. Los enrutadores no enrutan paquetes transmitidos simultáneamente; Por lo tanto, una red de L2 puede contener muchos *switches* y *hubs*, pero no tendrá ningún enrutador.

Nivel 3 — Nivel de Conexión en Red: El IP (Protocolo de Internet) está en este nivel. Los dispositivos en una red IP (v4) son dirigidos a través de una dirección IP de 4 octetos. El ARP (Protocolo de Conversión de Direcciones) es usado para convertir direcciones IP de L3 en direcciones MAC de L2; esto es necesario porque, en un segmento, L3 depende de L2 para transmitir paquetes al *host* remoto. El ARP depende de la función de transmisión múltiple simultánea del L2 para preguntarles a todos los sistemas de la red: *A los que tengan la dirección IP 1.2.3.4, ¿cuál es su dirección MAC?* Varias redes IP son conectadas a través de enrutadores.

Para saber más a este respecto, existen varios sitios Web útiles (por ejemplo, http://www.webopedia.com/quick_ref/OSI_Levels.asp).

El sensor de sistemas fuera de control

Como ya fue mencionado, el sensor detecta sistemas al escuchar las transmisiones simultáneas del L2. Dos de los protocolos de red comunes que utilizan transmisiones simultáneas son el ARP, usado para convertir direcciones IP de L3 en direcciones MAC de L2, y el DHCP (Protocolo de Configuración Dinámica de *Hosts*), usado para atribuir dinámicamente direcciones IP a *hosts*. Es muy raro que un sistema se conecte y use una red sin utilizar uno de dichos protocolos. Evidencias empíricas también demuestran que las computadoras usadas activamente tienden a realizar transmisiones simultáneas con una cierta frecuencia.

El sensor no es totalmente pasivo en su recopilación de información. Aunque el IP y el MAC sean recopilados pasivamente, el sensor realiza una consulta activa para obtener el *hostname* y las propiedades. Cuando el sensor recibe un paquete de transmisión múltiple simultánea, extrae la dirección IP de origen y la dirección MAC. Antes que la existencia del sistema sea informada al servidor, el sensor recopila más información en el *host*, que se incluye en el mensaje **sistema detectado**, por ejemplo:

- El nombre del DNS.
- El nombre del NetBIOS.
- Varias otras propiedades del NetBIOS.

El sensor de *sistemas fuera de control* es un servicio lógico ligero que funciona en sistemas no dedicados y es instalado y administrado a través de los parámetros de configuración del ePolicy Orchestrator, definidos con la consola del ePolicy Orchestrator y fiscalizados en cada sistema por los agentes ePolicy Orchestrator. La instalación del sensor puede ocurrir de una de las siguientes formas: a través del ePolicy Orchestrator, con un instalador autónomo o con una imagen de disco copiada. Independientemente de la forma de instalación, el sensor requiere la presencia del ePolicy Orchestrator para operar correctamente.

El Servidor

La información en todos los sistemas detectados y su estado de “fuera de control” son almacenados en la base de datos del ePolicy Orchestrator. El Servidor también controla en cuáles subredes los sistemas han sido encontrados y cuáles sensores están informando activamente su presencia en cada subred. Dicha información es exhibida en una ventana HTML incorporada a la consola del ePolicy Orchestrator. La página **Máquinas Fuera de Control** presenta un resumen general de los sistemas fuera de control y administrados detectados en la red, además de permitir la profundización hasta un modo de exhibición de lista filtrada y detalles sobre cada sistema. El modo de exhibición de lista puede ser organizado por subred o filtrado y clasificado por prácticamente cualquier tipo de información conocida sobre los sistemas.

Figura 2: Máquinas Fuera de Control: Lista de Máquinas

The screenshot shows the 'Rogue Machines' interface in McAfee ePolicy Orchestrator. The 'Machine List' table is as follows:

| <input type="checkbox"/> | Status | Rogue Type | Friendly Name | IP | Last Detect Time |
|--------------------------|--------|------------|---------------|---------------|--------------------|
| mdb-padre 192.168.1.0/24 | | | | | |
| <input type="checkbox"/> | Rogue | No Agent | Apple | 192.168.1.100 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Pear | 192.168.1.101 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Walnut | 192.168.1.102 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Salmon | 192.168.1.103 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Thyme | 192.168.1.104 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Cookie | 192.168.1.105 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Pork | 192.168.1.106 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Ginger | 192.168.1.107 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Egg | 192.168.1.108 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Grape | 192.168.1.109 | 5/24/04 3:27:44 PM |
| <input type="checkbox"/> | Rogue | No Agent | Salsa | 192.168.1.110 | 5/24/04 3:27:44 PM |

At the bottom of the table, there are links for 'Check All' and 'Uncheck All', and a status indicator '11 items in 1 page.'. Below the table, there is a 'Checked machines:' section with a dropdown menu set to 'Add to ePO tree' and an 'Apply' button.

Distribución de sensores de sistemas fuera de control

Debido a la necesidad de un sensor por subred, ¿cómo puede el administrador distribuir sensores fácilmente en todas las subredes administradas y, después, estar seguro de que, a cualquier momento en el futuro, todos los segmentos seguirán contando con al menos un sensor instalado? La consola del ePolicy Orchestrator posee varias formas de solucionar directamente dicha cuestión.

- Subredes con al menos un sensor instalado y que envían información activamente son consideradas protegidas.
- Subredes sin ninguna actividad de sensor durante un cierto período de tiempo (que se puede configurar) son consideradas desprotegidas.

La sección de sistemas fuera de control de la consola del ePolicy Orchestrator exhibe una lista de todas las subredes conocidas por ePolicy Orchestrator, además de su situación de protección. Los administradores pueden configurar ePolicy Orchestrator para que se envíe un aviso cuando cualquier subred anteriormente protegida se quede desprotegida. Esto puede ocurrir si se desactiva un sistema que hospeda un sensor o si dicho sistema cambia de subred. Dicha situación también se puede solucionar con la instalación de más de un sensor por subred.

Debido a que una subred necesita quedarse en un único dominio de transmisión múltiple simultánea (por ejemplo, una subred no puede abarcar dos o más dominios de transmisión múltiple simultánea), si usted asegura que todas las subredes están protegidas, también podrá asegurar que todos los dominios de transmisión múltiple simultánea estarán protegidos. En toda la sección de sistemas fuera de control de la consola del ePolicy Orchestrator, la protección por los sensores se describe en términos de subredes, no de segmentos o dominios de transmisión múltiple simultánea.

Figura 3: Máquinas Fuera de Control: Lista de Subredes

The screenshot shows the 'Subnet List' window in the McAfee ePolicy Orchestrator interface. The window has a navigation bar with tabs for 'Machines', 'Subnets', 'Events', 'Responses', and 'Configuration'. Below the navigation bar, there are buttons for 'Refresh (Auto)', 'Configure Table', and 'Custom Filter'. The main content area contains a table with the following data:

| <input type="checkbox"/> | Status | Address/Mask | Network Name | Sensors | Last Sensor Comm. |
|--------------------------|-----------|---------------|--------------|---------|--------------------|
| <input type="checkbox"/> | Uncovered | 10.13.50.0/24 | QA | 0 | |
| <input type="checkbox"/> | Covered | 10.13.51.0/24 | Dev | 1 | 5/24/04 3:41:19 PM |
| <input type="checkbox"/> | Uncovered | 10.13.52.0/24 | HR | 1 | 5/19/04 3:48:14 PM |
| <input type="checkbox"/> | Uncovered | 10.13.53.0/24 | Support | 0 | |
| <input type="checkbox"/> | Uncovered | 10.13.54.0/24 | Sales | 0 | |
| <input type="checkbox"/> | Covered | 10.13.55.0/24 | Marketing | 2 | 5/24/04 3:47:35 PM |

Below the table, there are buttons for 'Check All' and 'Uncheck All'. At the bottom right, it says '176 items in 12 pages. Go to page: 1'. Below the table, there is a 'checked subnets:' label and a 'Deploy Sensors' button.

En la ventana **Subnet List (Lista de Subredes)**, el administrador puede seleccionar subredes que no están protegidas e instalar sensores en ellas a través de los recursos de instalación de software de ePolicy Orchestrator. En las subredes seleccionadas, los sistemas usados para hospedar el software del sensor se pueden seleccionar manualmente en una lista o, automáticamente, por el servidor ePolicy Orchestrator, utilizando criterios definidos por el administrador. Entre los posibles criterios de selección automática de sistemas están los siguientes: versión del sistema operativo, velocidad del procesador, memoria del sistema o la hora de la última comunicación del agente ePolicy Orchestrator.

Medidas de reacción a sistemas fuera de control

Existen varias medidas distintas que un administrador puede tomar para reaccionar a la detección de sistemas fuera de control. Cada una de dichas medidas se puede tomar manualmente, a través de la selección del sistema en la lista de sistemas fuera de control de la interfaz de usuario y, enseguida, seleccionando la medida, o a través de la implementación automática de una reacción predefinida.

Las medidas automáticas poseen un conjunto de condiciones asociadas. Con la detección de nuevos sistemas fuera de control, se invocan las medidas sólo si se cumplen las condiciones. La condición de una medida puede depender de un aspecto cualquiera de la información conocida sobre un sistema fuera de control, pudiendo ser simplemente una comparación de un único campo o un comando compuesto complejo. Un ejemplo de condición puede ser la frase en español: *Si el IP de un nuevo sistema fuera de control está en el intervalo entre 192.168.1.0/24 y el sistema operativo es Windows, envíe un agente ePolicy Orchestrator a dicho sistema.* Una medida automática y sus condiciones asociadas se llaman colectivamente "reacción automática" en la sección de sistemas fuera de control de la consola del ePolicy Orchestrator.

Figura 3: Máquinas Fuera de Control: Incluir o Editar Respuesta Automática

Add or Edit Automatic Response

Name:

Event: **Rogue Machine Detected**

Enabled:

Conditions:

Match All (AND) Match Any (OR)

| Property | Comparison | Value | Delete |
|-------------|-------------|-----------------------------|-------------------------------------|
| IP | is in range | 192.168.1.0 - 192.168.1.255 | <input checked="" type="checkbox"/> |
| OS Platform | contains | Windows | <input checked="" type="checkbox"/> |

Actions:

| Method | Parameters | Delete |
|-----------------------|------------|-------------------------------------|
| Mark as Exception | (none) | <input checked="" type="checkbox"/> |
| Add to ePO tree | | |
| Mark for Action | | |
| Mark as Exception | | |
| Push ePO Agent | | |
| Query ePO agent | | |
| Remove Host | | |
| Send E-mail | | |
| Send ePO Server Event | | |
| Unmark For Action | | |
| Unmark as Exception | | |

Estas son algunas de las acciones que se pueden realizar en los sistemas detectados como fuera de control:

- **Distribuir el Agente ePO:** Esta es la forma más directa de resolución de sistemas descontrolados. Luego de la instalación del agente, ello ya aplica las políticas del ePolicy Orchestrator y el sistema objetivo es considerado administrado. Cuando ocurre esto, el servidor lo saca de la lista de sistemas fuera de control.
- **Enviar E-mail:** Con la nueva función de alerta del ePolicy Orchestrator, el administrador puede recibir avisos por email o SNMP cuando se encuentre un nuevo sistema fuera de control.
- **Ejecutar una herramienta externa:** Otras opciones aparecen en el menú suspenso si usted posee alguna herramienta externa (de otro fabricante) instalada. Una herramienta externa puede ser cualquier aplicación ejecutable instalada en el servidor ePolicy Orchestrator. Esta acción permite la personalización de la solución o la notificación (un recurso que no existe originalmente en el ePolicy Orchestrator). Esto también permite la integración de herramientas de sondeo de otros fabricantes para que el administrador pueda recopilar más información sobre un cierto sistema fuera de control antes de tomar otras medidas.
- **Marcar como Excepción:** Marcar un sistema como una excepción altera su estado en la base de datos de sistemas fuera de control para indicar que ePolicy Orchestrator no lo puede administrar y, por lo tanto, no se lo debe considerar fuera de control. Consulte [Sistemas y dispositivos imposibles de administrar](#) en la página 12 para saber más sobre falsos positivos, además de detalles sobre excepciones
- **Marcar para Acción:** Marcar un sistema como “aguardando acción posterior” es una forma que los administradores tienen para marcar sistemas fuera de control que todavía no se pueden solucionar, pero que desean revisar posteriormente para que puedan tomar otras medidas. La lista de sistemas puede ser clasificada o filtrada según la existencia o no de una marca de acción en dichos sistemas. Dicha marca se exhibe al lado del nombre del sistema en la consola del ePolicy Orchestrator.

Sistemas y dispositivos imposibles de administrar

La clasificación de sistemas imposibles de administrar como “fuera de control” ocurrirá en todas las redes. Sin embargo, algunas de dichas clasificaciones pueden ser falsos positivos. Esto ocurre porque no es necesario que muchos de los dispositivos participantes de una red sean administrados por ePolicy Orchestrator. Algunos ejemplos de falsos positivos: enrutadores, impresoras, varios tipos de dispositivos físicos (*appliances*) de red, y sistemas que funcionan con sistemas operativos que ePolicy Orchestrator no reconoce. Para impedir que dichos sistemas sean clasificados como “fuera de control”, la base de datos de sistemas fuera de control trabaja con la noción de “sistemas excepcionales”, que se pueden marcar en la consola del ePolicy Orchestrator.

Cuando el administrador marca como excepciones los sistemas “fuera de control” que no pueden ser administrados, dichos sistemas dejan de aparecer en la lista de sistemas fuera de control del ePolicy Orchestrator. La información recopilada por el sensor (nombre del DNS, nombre del NetBIOS y otra información del NetBIOS, por ejemplo, sistema operativo, comentarios y dominio) y el nombre OUI (Identificador Exclusivo dentro de la Organización) de IEEE. El OUI ocupa los tres primeros octetos de una dirección MAC, y es registrado para una empresa u organización (normalmente, un fabricante de tarjetas de red). El OUI puede auxiliar al administrador a identificar excepciones. Herramientas de sondeo de otros fabricantes y otras aplicaciones externas también se pueden usar para recopilar más información. Entonces, se capturan y exhiben los datos generados junto con la información de otros sistemas fuera de control.

Además de seleccionar manualmente los sistemas como excepciones, el administrador también puede crear reglas para marcar sistemas como excepciones cuando cumplan ciertos criterios, utilizando el mecanismo de reacción automática descrito anteriormente. Por ejemplo, si una empresa utiliza enrutadores de Cisco y no usa ninguna tarjeta de red de dicho fabricante, una de las posibles reacciones automáticas es *“Si el nombre del OUI de un nuevo sistema fuera de control contiene 'Cisco', márkelo como excepción.*

Inmediatamente tras la primera instalación de sensores de sistemas fuera de control, se prevén algunos falsos positivos que no se necesitan administrar por ePolicy Orchestrator. Durante dicho período de ajuste, el administrador debe marcar manualmente dichos sistemas como excepciones o guardar reacciones automáticas para ayudar a automatizar el proceso. Después que se encuentre la mayoría de las excepciones, la mayor parte de las detecciones de nuevos sistemas fuera de control será legítima. En ese momento, el administrador puede permitir el uso de reglas o notificaciones más agresivas de solución automática.

Preguntas más frecuentes

¿Operan correctamente los sensores en una red conmutada?

Sí, porque los *switches* propagan tráfico de transmisión múltiple simultánea de L2. Los *switches* sólo limitan los dispositivos en un dominio de transmisión múltiple simultánea que pueden ver paquetes de difusión punto a punto (*unicast*).

¿Operan correctamente los sensores en una LAN virtual (VLAN)?

Sí. Desde el punto de vista de la detección de sistemas fuera de control, no hay diferencia entre una VLAN y una LAN. Los *switches* que operan con VLAN deben encaminar paquetes de transmisión múltiple simultánea a cada uno de los otros dispositivos de la VLAN, y se debe instalar un sensor por VLAN.

¿Operan correctamente los sensores con *switches* en tronco (por ejemplo, 802.1q)?

Sí. Los *switches* con tronco, que permite la extensión de una VLAN a varios *switches* a través de la transmisión del tráfico de la VLAN por medio de un único enlace punto a punto, necesitan asegurar que el tráfico de transmisión múltiple simultánea sea propagado a todos los dispositivos de la VLAN. Desde el punto de vista de la detección de sistemas fuera de control, una VLAN que se extiende a *switches* con tronco no es distinta a una VLAN en un *switch* o una LAN normal.

¿Operan correctamente los sensores con tarjetas de red (NIC) que no operan en el modo promiscuo?

Sí. El uso del *driver* de una tarjeta de red en el modo promiscuo es necesario sólo para el recibimiento de paquetes de difusión punto a punto cuyo destino no sea el sistema local. Debido a que el sensor escucha sólo paquetes de transmisión múltiple simultánea, no necesita abrir el *driver* en el modo promiscuo.

¿Detecta el sensor sistemas que se conectan a través de una VPN?

No. Los servidores de VPN actúan como enrutadores (L3). Por lo tanto, no propagan transmisiones múltiples simultáneas en L2. Sin embargo, como parte de la estrategia Trusted Connection, McAfee estableció varias asociaciones con grandes proveedores de VPN, incluso Check Point, Nortel, Neoteris, Cisco y Aventail para permitir la detección y el bloqueo de sistemas que no alcancen un nivel predefinido de conformidad de seguridad. En el inicio, dichas asociaciones se dedican a la conformidad antivirus, pero, con el tiempo, buscamos aumentar la profundidad de dichas asociaciones.

¿Detecta el sensor sistemas que se conectan a través de un Punto de Acceso Inalámbrico (WAP)?

Sí, si hay un sensor en la subred inalámbrica, detectará todos los sistemas que se conectan a través de un WAP. Si un WAP actúa como enrutador o dispositivo de NAT y el sensor está en el lado externo, detectará la presencia del propio WAP, pero no podrá ver nada dentro de la red inalámbrica.

¿Es necesario que el sensor opere en un sistema dedicado?

No. Aunque sea deseable que los sensores operen en sistemas que no sean apagados regularmente por largos períodos de tiempo, no es obligatorio que el sensor opere en servidores o sistemas dedicados. El consumo de memoria y procesador de un sensor es muy pequeño; normalmente, la utilización no alcanza al 1% en una máquina de 500 MHz, y el consumo normal de memoria es de 5-10 megabytes. El sensor no necesita hardware especial.

¿Puede la detección de sistemas fuera de control manejar sistemas que siempre se conectan con varias tarjetas de red, tales como un *laptop* con una tarjeta inalámbrica y un conector Ethernet y una estación de anclaje?

Sí. Aunque la dirección MAC sea la clave principal usada para buscar sistemas detectados en la base de datos del ePolicy Orchestrator, la detección de sistemas fuera de control también puede ser configurada para buscar sólo el *hostname*, tanto por el *hostname* como por el dominio. En este caso, independientemente de dónde se detecte el *laptop* en la red inalámbrica o en la LAN, si es administrado por el ePolicy Orchestrator, será encontrado en la base de datos e identificado correctamente como “administrado”.

¿Cómo maneja la detección de sistemas fuera de control de sistemas administrados por otro servidor ePolicy Orchestrator?

Dichos sistemas serán considerados fuera de control, pero el sistema de detección de sistemas fuera de control puede ser configurado para identificar dichos sistemas como poseedores de *agentes externos*. El Servidor de detección de sistemas fuera de control consultará la presencia de un agente de ePolicy Orchestrator en dichos sistemas y, si se encuentra un agente, el sistema será identificado como poseedor de un agente externo. El nombre del servidor externo del ePolicy Orchestrator será registrado y exhibido en la sección de detección de sistemas fuera de control de la consola del ePolicy Orchestrator.

Acrónimos utilizados en este documento

| | |
|--------------|---|
| ARP | Protocolo de Conversión de Direcciones |
| HTTPS | Protocolo (Seguro) de Transferencia de Hipertexto |
| LAN | Red Local |
| Lx | Nivel x (donde x es un número) del modelo de referencia OSI |
| MAC | Control de Acceso a los Medios |
| NAT | Conversión de Direcciones de Red |
| NIC | Tarjeta de Red |
| Nmap | Herramienta de Mapeo de Red |
| OSI | Interconexión de Sistemas Abiertos |
| OUI | Identificador Exclusivo dentro de la Organización |
| VLAN | Red Local Virtual |
| VPN | Red Privada Virtual |
| WAP | Punto de Acceso Inalámbrico |