¿Cómo usted bloquea las aplicaciones desconocidas en el dispositivo de seguridad de la red de Cisco?

Contenido

Pregunta

¿Cómo usted bloquea las aplicaciones desconocidas en el dispositivo de seguridad de la red de Cisco?

Nota: Este artículo sobre Knowledge Base se refiere al software que no es mantenido ni es soportado por Cisco. La información se proporciona como cortesía para su conveniencia. Para la asistencia adicional, entre en contacto por favor al proveedor de software.

1. La primera defensa es utilizar las cadenas del “agente de usuario” para bloquear tales aplicaciones. Puesto que no conocemos todos los agentes de usuario para estos aplicación, usted necesitará buscarlos en los links abajo.
   Podemos agregar el “agente de usuario” bajo <for de la columna del ***administrador de seguridad > de las políticas de acceso > de los protocolos y de los agentes de usuario de la red el*** policy> requerido del acceso.--**> Add la** cadena del agente de usuario bajo ***“agentes de usuario de encargo del bloque: ”*** (uno por la línea).

2. Si se habilitan los controles de la visibilidad de la aplicación (AVC) *(bajo el > Security (Seguridad) GUI mantiene > reputación Web y anti-Malware)*, después podemos bloquear el acceso basado en los tipos de aplicación como los proxys, capacidad de compartir archivos, las utilidades de Internet. Podemos hacer esto bajo el ***administrador de seguridad > políticas de acceso de la red > <for de la columna de las “aplicaciones” el policy> requerido del acceso***.
3. Si no existe el agente de usuario, usted puede intentar agregar el tipo MIME (ejemplo*:* aplicaciones de los torrentes del bit).
   Podemos agregar “IMITAMOS” los tipos *bajo el <for de la columna del* ***administrador de seguridad de la red >*** *de las* ***directivas >*** *de los* ***objetos del Acceso Web el*** *policy> requerido del acceso*.---**>** Add en el objeto/el tipo MIME en **“la** sección de los **tipos MIME de encargo del bloque** como application/x-bittorrent (uno por la línea).

4. Asegúrese de que las categorías como la evitación del filtro, las actividades ilegales estén bloqueadas en políticas de acceso. Si algunas aplicaciones utilizan los URL sabidos o los IP Addresses para sus conexiones, después podemos bloquear sus categorías predefinidas assocaited URL o configurarlas en una categoría de encargo bloqueada URL usando su

dirección IP, el FQDN, o un regex que corresponde con los dominios. Podemos hacer esto *bajo el* ***administrador de seguridad > políticas de acceso de la red > "****columna de las* ***categorías URL"****.*

5. Algunas aplicaciones pueden utilizar el HTTP CONECTAN el método para conectar con diversos puertos. Permita solamente sabido que los puertos o los puertos específicos necesarios en su entorno en el HTTP CONECTAN los dominios de la configuración de los puertos.
   El HTTP CONNECT se puede configurar *bajo <for de la columna del* ***administrador de seguridad > de las políticas de acceso > de los protocolos y de los agentes de usuario de la red el*** *policy> requerido del acceso.*--> **Add los** puertos permitidos bajo el **"HTTP CONECTAN los puertos: "**

6. Para las aplicaciones donde usted sabe solamente sobre los IP Address de destino que son accedidos, usted puede utilizar la característica del control de tráfico L4 para bloquear el acceso para la dirección IP en cuestión. Podemos agregar el IP de destino *bajo el* ***administrador de seguridad de la red >*** *el* ***control de tráfico L4 >*** *los* ***direccionamientos sospechosos adicionales de Malware.***

Si usted está inconsciente cuyo el "agente de usuario" o el "tipo MIME" está siendo utilizado por ciertas aplicaciones, después usted puede hacer cualquiera del siguiente para encontrar esta información:

- Funcione con a una captura de paquetes con WireShark (etéreo) en la máquina y el filtro de cliente para el protocolo "HTTP".
- Ejecute la captura en WSA (bajo el "soporte y la ayuda" > "captura de paquetes"), filtrado en la dirección IP del cliente.

Lista de agentes de usuario:
==========
http://www.user-agents.org/

Lista de tipos MIME:
==========
http://www.webmaster-toolkit.com/mime-types.shtml

http://www.microsoft.com/technet/isa/2004/plan/commonapplicationsignatures.mspx