¿Cómo la manija Skype del dispositivo de seguridad de la red de Cisco (WSA) trafica?

Contenido

Pregunta:

Pregunta:

¿Cómo la manija Skype del dispositivo de seguridad de la red de Cisco (WSA) trafica?

Entorno: Cisco WSA, Skype

Skype es una red propietaria de la telefonía por Internet (VoIP). Skype actúa sobre todo como programa entre iguales, así no comunica directamente con un servidor central para actuar. Skype puede ser determinado difícil de bloquear, pues intentará conectar en muchas maneras diferentes.

Skype conecta en el siguiente orden de preferencia:

1. Paquetes UDP directos a otros pares que usan los números del puerto al azar
2. Paquetes TCP directos a otros pares que usan los números del puerto al azar
3. Paquetes TCP directos a otros pares que usan el puerto 80 y/o el puerto 443
4. Los paquetes tunneled vía a Web Proxy (Proxy Web) usando un HTTP CONECTAN con el puerto 443

Cuando están desplegados en un entorno proxy explícito, los métodos 1-3 nunca serán enviados a Cisco WSA. Para bloquear Skype, debe primero ser bloqueado de otra ubicación en la red. Los pasos de Skype 1-3 se pueden bloquear usando:

- Firewall: Utilice el NBAR para bloquear la versión 1 de Skype. Más información está disponible en http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- IPS de Cisco (ASA): Cisco ASA puede potencialmente detectar y bloquear Skype vía las firmas.

Cuando Skype recurre a usar un proxy explícito, Skype no proporciona deliberadamente a ningún cliente los detalles en el pedido de conexión HTTP (ninguna cadena del agente de usuario tampoco). Esto hace difícil distinguir entre Skype y un pedido de conexión válido. Skype conectará siempre con el puerto 443 y la dirección destino es siempre una dirección IP.

Ejemplo:

CONECTE 10.129.88.111:443 HTTP/1.0
Conexión proxy: señal de mantenimiento

La política de acceso siguiente bloqueará cualquier pedido de conexión con el WSA que hace

juego los IP Addresses y el puerto 443. Esto hará juego todo el tráfico de Skype. Sin embargo, los programas de NON-Skype que intentan hacer un túnel a una dirección IP en el puerto 443 serán bloqueados también.

Bloqueando Skype - Entorno explícito con el proxy HTTPS inhabilitado

Cree una categoría de la aduana URL para hacer juego el tráfico IP y del puerto 443:

1. Navegue al “administrador de seguridad” - > las “categorías de encargo URL” - > “agregan la categoría de encargo”.
2. Complete el “nombre de la categoría” y amplíese “avanzó”.
3. Utilice el "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" en la ventana de la expresión normal.

Fije esta categoría para negar en las políticas de acceso:

1. Navegue al “administrador de seguridad de la red” - > las “políticas de acceso”.
2. Haga clic el link bajo “la columna de las categorías URL” para el grupo de políticas apropiado.
3. En la sección de filtración “de la categoría de encargo URL”, elija el “bloque” para la nueva categoría de Skype.
4. Someta y confíe los cambios

Nota: ¡Los pedidos de conexión explícitos pueden ser bloqueados solamente si inhabilitan al servicio de representación HTTPS!

Cuando se habilita el desciframiento WSA HTTPS, el tráfico de Skype puede romperse muy probablemente porque no es puramente tráfico HTTPS (el desafío usando CONECTA y el puerto 443). Esto dará lugar a un error 502 generado por el WSA y la conexión será caída. Cualquier tráfico de la Web real HTTPS a una dirección IP continuará trabajando (aunque será desencriptado en el WSA).

Bloqueando Skype - Entorno explícito/transparente con el proxy HTTPS habilitado

Cree una categoría de encargo para hacer juego el tráfico IP y del puerto 443:

1. Navegue al “administrador de seguridad” - > las “categorías de encargo URL” - > “agregan la categoría de encargo”.
2. Complete el “nombre de la categoría” y amplíese “avanzó”.
3. Utilice el "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" en la ventana de la expresión normal.

Fije esta categoría para desencriptar en las políticas de descifrado:

1. Navegue al “administrador de seguridad de la red” - > las “políticas de descifrado”.
2. Haga clic el link bajo “la columna de las categorías URL” para el grupo de políticas apropiado.
3. En la sección de filtración “de la categoría de encargo URL”, elija el “Decrypt” para la nueva categoría de Skype.
4. Someta y confíe los cambios.

Nota: Puesto que el tráfico de Skype se envía a un IP, será considerado como parte de los “URL Uncategorized”. El mismo efecto que arriba ocurrirá dependiendo de si la acción debe

desencriptar o passthrough.