Guía de diseño del dispositivo de seguridad de la red

Contenido

Introducción

Este documento describe cómo diseñar el dispositivo de seguridad de la red de Cisco (WSA) y los componentes asociados para el rendimiento óptimo.

Antecedentes

Cuando usted diseña una solución para el WSA, requiere la consideración apropiada, no sólo con respecto a la configuración del dispositivo sí mismo, pero también los dispositivos de red asociados y sus características. Cada red es una Colaboración de los dispositivos múltiples, y si uno de ellos no participa correctamente en la red, después del usuario que las experiencias pudieron disminuir.

Hay dos componentes principales que deben ser considerados cuando usted configura el WSA: el soporte físico y el software. El hardware viene en dos diversos tipos. El primer es el tipo físico de hardware, tal como los modelos S170, S380, y de las S680 Series, así como otro extremo de los modelos de la vida (EoL), tales como los modelos S160, S360, S660, S370, y de las S670 Series. El otro tipo de hardware es virtual, por ejemplo los modelos de la serie S000v, S100v, y S300v. El operating system (OS) que se ejecuta en este hardware se llama *AsyncOS para la red*, que se basa en FreeBSD en su base.

El WSA ofrece el servicio de representación y también analiza, examina, y categoriza todo el tráfico (HTTP, HTTPS, y File Transfer Protocol (FTP)). Todo el funcionamiento de estos protocolos encima del TCP y confía pesadamente en el Domain Name System (DNS) para la

operación correcta. Por estas razones, la integridad de la red es vital para la operación correcta del dispositivo y su comunicación con las diversas partes de la red, tanto en el interior como en el exterior del control de la empresa.

Diseño

Utilice la información que se describe en esta sección para diseñar el WSA y los componentes relacionados para el rendimiento óptimo.

Red

Una red sin error, rápida es vital para la operación correcta del WSA. Si la red es inestable, la experiencia del usuario pudo disminuir. Los problemas de red se detectan cuando las páginas web duran para alcanzar o son generalmente inalcanzables. La inclinación inicial es culpa el dispositivo, pero es generalmente la red que se comporta mal. Así, la consideración apropiada y la auditoría se deben hacer para asegurarse de que la red ofrece el mejor servicio para los protocolos de la aplicación de alto nivel tales como HTTP, HTTPS, FTP, y DNS.

Consideraciones generales

Aquí están algunas consideraciones generales que usted puede implementar para asegurar el mejor comportamiento de la red:

- Asegúrese de que la red de la capa 2 (L2) sea estable, de que la operación del atravesar-árbol está correcta, y que no hay cómputos y cambios de la topología frecuentes del atravesar-árbol.
- El Routing Protocol se utiliza que debe también proporcionar la convergencia rápida y la estabilidad. Los temporizadores rápidos del Open Shortest Path First (OSPF) o el Enhanced Interior Gateway Routing Protocol (EIGRP) son buenas opciones para tal red.
- Utilice siempre por lo menos dos Interfaces de datos en el WSA: uno que hace frente a los ordenadores del usuario final, y otro para la operación saliente (conectada con el proxy ascendente o Internet). Esto se hace para eliminar el recurso posible obliga, por ejemplo cuando el número de puertos TCP se agota o cuando se convierten los buffers de la red por completo (con el uso del las solas interfaces para tanto en el interior como en el exterior especialmente).
- Dedique la interfaz de administración para el tráfico de la Administración-solamente para aumentar la Seguridad. Para alcanzar esto vía el GUI, navegar a la **red > a las interfaces** y marcar la casilla de verificación **separada de la encaminamiento (puerto M1 restringido a los servicios de administración del dispositivo solamente)**.
- Utilice a los servidores DNS rápidos. Cualquier transacción vía el WSA requiere por lo menos una búsqueda de DNS (si no en el caché). Un servidor DNS que es lento o se comporta mal las influencias cualquier transacción y se observa como conectividad a Internet retrasada o

lenta.

- Cuando se utilizan las tablas de ruteo separadas, estas reglas se aplican:

  Todas las interfaces se incluyen en la tabla de ruteo predeterminada de la *Administración* (M1, P1, P2).

  Solamente las Interfaces de datos se incluyen en la tabla de ruteo de los *datos*.

  Note: La separación de tablas de ruteo está no por la interfaz, sino bastante por el servicio. Por ejemplo, el tráfico entre el WSA y el controlador de dominio del Microsoft Active Directory (AD) obedece siempre las rutas que se especifican en la tabla de ruteo de la Administración, y es posible configurar las rutas que señalan de la interfaz P1/P2 en esta tabla. No es posible incluir las rutas en la tabla de ruteo de los datos que utilizan las interfaces de administración.

Balanceo de Carga

Aquí están algunas consideraciones del balanceo de carga que usted puede implementar para asegurar el mejor comportamiento de la red:

- El del del â de la rotación DNS esto es el término usado cuando un solo nombre de host se utiliza como proxy, pero tiene expedientes del múltiplo A en el servidor DNS. Cada cliente resuelve esto a una diversa dirección IP y utiliza diversos proxys. Una limitación es que los cambios de los expedientes DNS están reflejados en los clientes sobre la reinicialización (DNS local que oculta), así que ofrece un nivel bajo de robustez si un cambio debe ser realizado. Sin embargo, esto es transparente a los usuarios finales.

- El del del â de los archivos del control de dirección del proxy (PAC) éstos es los archivos proxy-automáticos del scripting que determinan cómo cada URL se debe dirigir en un hojeador basado en las funciones escritas dentro de él. Tiene la característica para remitir el mismo URL siempre directamente o al mismo proxy.

- El del del â de la detección automática esto describe el uso de los métodos DNS/DHCP para obtener los archivos PAC (descritos en la consideración anterior). Generalmente, estas primeras tres consideraciones se combinan en una solución. Sin embargo, esto puede ser complicado y muchos agentes de usuario, tales como Microsoft Office, descargador de Adobe, los Javascript, y Flash, no pueden leer los archivos PAC en absoluto.

- del del â del protocolo web cache control (WCCP) este protocolo (especialmente la versión de WCCP 2) proporciona un robusto y mismo una forma muy eficaz de crear el balanceo de carga entre varios WSAs y también incorporar la Alta disponibilidad.

- El separado Cisco del del â de los dispositivos del balanceo de carga recomienda que usted utiliza los carga-balanceadores como máquinas dedicadas.

Firewall

Aquí están algunas consideraciones del Firewall que usted puede implementar para asegurar el mejor comportamiento de la red:

- Asegúrese de que el Internet Control Message Protocol (ICMP) esté permitido en la red de cada fuente. El es vital, mientras que el WSA depende del mecanismo de detección máximo de la unidad de la transición de la trayectoria (MTU), según lo descrito en el RFC 1191, que depende de los pedidos de eco ICMP (tipo 8) y Respuestas de eco (tipo 0), y se requiere la inalcanzable-fragmentación ICMP (el tipo 3, el código 4). Si usted inhabilita la detección de MTU de trayecto en el WSA con el comando CLI del **pathmtudiscovery**, después el WSA utiliza el MTU predeterminado de 576 bytes, según el RFC 879. Esto afecta el rendimiento debido a los gastos indirectos crecientes y un nuevo ensamble de los paquetes.

- Asegúrese de que no haya encaminamiento asimétrica dentro de la red. Mientras que esto no es un problema en el WSA, cualquier Firewall que se encuentre a lo largo de la trayectoria cae los paquetes porque no ha recibido los ambos lados de la comunicación.

- Con los Firewall, es muy importante excluir los IP Addresses WSA de las amenazas como estaciones regulares del ordenador del extremo. El Firewall pudo poner los IP Addresses WSA debido a demasiadas conexiones (según el conocimiento general del Firewall).

- Si el Network Address Translation (NAT) se emplea para cualquier dirección IP WSA en el dispositivo de las instalaciones del cliente, asegúrese de que cada WSA utilice a una dirección global externa separada en el NAT. Si usted utiliza el NAT para WSAs múltiple que tiene una sola dirección global externa, usted puede ser que encuentre estos problemas:

  Todas las conexiones de todo el WSAs al mundo exterior utilizan a una sola dirección global externa, y el Firewall se ejecuta rápidamente de los recursos.

  Si hay un punto del tráfico hacia ese destino único, el servidor de destino pudo ponerlo y cortar la empresa entera del acceso a este recurso. Esto pudo ser un recurso valioso como el almacenamiento de la nube de la compañía, las conexiones de la nube de la oficina, o las actualizaciones de Software anti virus de la por-Computadora.

Identidades

Recuerde que el *lógico Y el* principio se aplica en todos los componentes de la identidad. Por ejemplo, si usted configura el agente de usuario y la dirección IP, significa el agente de usuario de esta dirección IP. No significa el agente de usuario *o* esta dirección IP.

Utilice una identidad para la autenticación del mismo tipo sustituto (o no del sustituto) y/o del agente de usuario.

Es importante asegurarse que cada identidad que requiera la autenticación incluye las cadenas del agente de usuario para los navegadores/los agentes de usuario que soportan la autenticación de representación, tal como Internet Explorer, Mozilla Firefox, y Google Chrome conocidos. Hay algunas aplicaciones que requieren el acceso a internet pero no soporta la autenticación proxy/WWW.

Las identidades son de arriba a abajo correspondido con con la búsqueda para las coincidencias

que termina en la primera entrada correspondida con. Por este motivo, si usted hace la *identidad 1* y la *identidad 2* configurar, y una identidad 1 de las coincidencias de la transacción, no se marca contra la identidad 2.

Acceso/desciframiento/encaminamiento/directivas salientes de Malware

Estas directivas son aplicadas contra diversos tipos de tráfico:

- Las políticas de acceso son aplicadas contra el HTTP llano o las conexiones FTP. Determinan si la transacción debe ser validada o ser caída.

- Las políticas de descifrado determinan si las transacciones HTTPS se deben desencriptar, caer, o pasar a través. Si se desencripta la transacción, después la parte de consecutiva puede ser visto como pedido de HTTP llano y se corresponde con contra las políticas de acceso. Si usted debe caer una petición HTTPS, cáigala en las políticas de descifrado, no en las políticas de acceso. Si no, consume más CPU y memoria para una transacción caída primero que se desencriptará y después que se caerá.

- Los políticas de ruteo determinan a la dirección ascendente de una transacción una vez que él que el suyo permitió con el WSA. Esto aplica si hay proxy ascendentes o si el WSA está en el modo del *conector* y envía el tráfico a la torre de la Seguridad de la red de la nube.

- Las directivas salientes del malware son aplicadas contra las cargas HTTP o FTP de los usuarios finales hacia los servidores Web. Esto se ve generalmente es una petición post HTTP.

Para cada tipo de directiva, es importante recordar que el *lógico O el* principio se aplica. Si usted hace las identidades múltiples referir, después la transacción debe hacer juego las identidades unas de los se configuran que.

Para un control más granular, utilice estas directivas. Las identidades incorrecto configuradas por la directiva pueden crear los problemas, donde está más beneficioso utilizar varias identidades referidas a una directiva. Recuerde que las identidades no afectan el tráfico, apenas identifican los tipos de tráfico para coincidencias posteriores en una directiva.

A menudo las épocas, las políticas de descifrado utilizan las identidades con la autenticación. Mientras que esto no es incorrecto y es a veces necesario, el uso de una identidad con la autenticación referida a la política de descifrado significa que todas las transacciones que hacen juego la política de descifrado están desencriptadas para que ocurra la autenticación. La acción del desciframiento se pudo caer o pasar a través, pero puesto que hay una identidad con la autenticación, el desciframiento ocurre para caer o pasar más adelante con el tráfico. Esto es costoso y debe ser evitada.

Se han observado algunas configuraciones que contienen 30 o más identidades y 30 o más políticas de acceso, donde todas las políticas de acceso incluyen todas las identidades. En este caso, no hay necesidad de utilizar este muchas identidades si se corresponden con en todas las políticas de acceso. Mientras que esto no daña la operación del dispositivo, crea la confusión con las tentativas de resolver problemas y es costoso con respecto al funcionamiento.

Categorías de encargo URL

El uso de las categorías de encargo URL es una herramienta potente en el WSA que se entiende mal y se emplea mal generalmente. Por ejemplo, hay las configuraciones que contienen todos los sitios video para las coincidencias en la identidad. El WSA tiene una herramienta incorporada que automáticamente las actualizaciones cuando los sitios video cambian los URL, que ocurre con frecuencia. Así, tiene sentido de permitir que el WSA maneje las categorías URL automáticamente, y utiliza las categorías de la aduana URL para los sitios especiales, no todavía categorizados.

Tenga muy cuidado con las expresiones normales. Si las coincidencias del carácter especial tales como punto (.) y estrella (*) se utilizan, puede ser que demuestren ser mismo CPU y memoria extensos. El WSA amplía cualquier expresión normal para hacerla juego contra cada transacción. Por ejemplo, aquí está una expresión normal:

```
example.*
```

Esta expresión hará juego cualquier URL que contenga el *ejemplo de la* palabra, no sólo el dominio de *example.com*. Evite el uso del *punto* y *protagonice* en las expresiones normales y utilícelas solamente como último recurso.

Aquí está otro ejemplo de una expresión normal que pudo crear los problemas:

```
www.example.com
```

Si usted utiliza este ejemplo en las expresiones normales clasifiado, no sólo hará juego *www.example.com*, pero también *www.www3example2com.com*, como el punto aquí significa cualquier *carácter*. Si usted desea de hacer juego solamente *www.example.com*, escape el punto:

```
www\.example\.com
```

En este caso, no hay razón para utilizar la característica de las expresiones normales cuando usted puede incluir esto dentro del dominio de la categoría de la aduana URL con este formato:

```
www.example.com
```

Anti-Malware y reputación

Si se habilita más de un motor de análisis, considere la opción habilitar analizar adaptante también. La exploración adaptante es un motor potente pero pequeño en el WSA que las pre-exploraciones cada petición y determinan el motor completo que debe ser para peticiones de exploración usadas. Esto aumenta levemente el funcionamiento en el WSA.