Evaluar el impacto en el rendimiento y las prácticas recomendadas para el descifrado SSL/TLS en FTD

Contenido

Problema

Un usuario está planificando la activación del descifrado SSL/TLS en un dispositivo Firewall Threat Defence (FTD) y debe comprender el impacto potencial en el rendimiento del dispositivo antes de la implementación. Entre las principales preocupaciones se incluyen:

- Impacto en el rendimiento del firewall, la latencia y el rendimiento general del procesamiento del tráfico.
- Se espera un aumento del uso de la memoria y la CPU tras habilitar el descifrado.
- Directrices de dimensionamiento y valores de referencia de rendimiento para modelos específicos de FTD.
- Límites recomendados para sesiones descifradas simultáneas.
- Prácticas recomendadas y requisitos previos para la implementación de producción.

Entorno

- Firepower 4115. Otras plataformas de hardware también pueden verse afectadas.
- FTD versión 7.4.2 (Compilación 172). Otras versiones de software también pueden verse afectadas.
- Consideración de la función de descifrado SSL/TLS.
- Planificación de la implementación del entorno de producción.

Resolución

El descifrado SSL/TLS añade sobrecarga de procesamiento al Firepower 4115, pero el impacto real depende en gran medida de la cantidad de tráfico que se descifra y de la inspección que se aplica después del descifrado.

Análisis del impacto en el rendimiento

Los impactos del descifrado SSL/TLS incluyen:

- Menor rendimiento efectivo.
- Mayor latencia.
- Aumento del uso de CPU de Snort/inspección.
- Aumento de memoria y CPU que no se puede predecir con precisión como porcentaje fijo sin un análisis del perfil de tráfico real.

Parámetros de rendimiento de FPR 4115

Especificaciones de referencia publicadas de Cisco Firepower 4115:

- Rendimiento de descifrado de hardware TLS: 6.5 Gbps.
- Rendimiento de FW + AVC: 33 Gbps.
- Número máximo de sesiones simultáneas con AVC: 15 millones.
- Número máximo de nuevas conexiones por segundo con AVC: 210 000.

Nota importante sobre el tamaño: La referencia de descifrado de hardware TLS de 6,5 Gbps se basa en condiciones de prueba específicas. El rendimiento de producción puede ser menor si descifra un gran porcentaje del tráfico, inspecciona el tráfico descifrado con políticas de intrusión/archivo/malware o procesa muchas sesiones TLS de corta duración.

Cisco no publica un número separado de "sesiones descifradas simultáneas máximas" para Firepower 4115 en FTD 7.4.2. En la práctica, la capacidad se valida utilizando la combinación de tráfico, las sesiones simultáneas, la velocidad de conexión, los conjuntos de cifrado y la carga de políticas de inspección.

Enfoque de implementación de producción recomendado

Paso 1: Comience con un programa piloto limitado

- Inicialmente, no habilite reglas amplias de "descifrado de todos".
- Comience con los usuarios, subredes o categorías de destino seleccionados.
- Mantenga una gestión conservadora por defecto con No descifrar para el tráfico que no requiere inspección.

Paso 2: Excluir el tráfico que normalmente se interrumpe con el descifrado

- Sitios de banca/financieros.
- Portales sanitarios.
- Aplicaciones ancladas a certificados.
- Algunas aplicaciones de software como servicio (SaaS) y seguridad de terminales/nube.
- Aplicaciones vitales para la empresa a menos que se prueben explícitamente.

Paso 3: Mantenga las reglas de SSL simples y ordenadas cuidadosamente

- Ponga las exclusiones específicas de No descifrar por encima de las reglas de descifrado más amplias.
- Evite las coincidencias excesivamente amplias o complejas siempre que sea posible.
- No utilice la versión de TLS ni las condiciones de conjunto de cifrado para las reglas de descifrado, renuncia o clave conocida, ya que Cisco documenta que esto puede provocar un comportamiento impredecible.

Paso 4: Validar preparación del certificado

- Para el descifrado y la renuncia salientes, los extremos del cliente deben confiar en el certificado de CA de firma.
- Para el descifrado de clave conocida entrante, el firewall debe tener el certificado de servidor/material de clave privada correcto.

Paso 5: Supervisar durante la implementación

- Realice un seguimiento de la CPU en general y, lo que es más importante, de la utilización de la CPU Snort/inspection.
- Seguimiento de conexiones simultáneas y nuevas conexiones por segundo.
- Revise los errores de estado/protocolo de enlace del flujo SSL en los eventos de conexión.
- Esté atento a los indicadores de sobresuscripción de TLS y a los fallos específicos de la aplicación.

Para obtener más información sobre cómo supervisar la comprobación de la CPU:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Piense como un ingeniero del TAC: Una guía de los problemas más comunes de Cisco Secure Firewall

Para realizar un seguimiento de las conexiones y las nuevas conexiones por segundo, compruebe:

- Prácticas Recomendadas de Registro

Para realizar el seguimiento de los errores de estado/protocolo de enlace del flujo SSL en la comprobación de eventos de conexión y la comprobación de indicadores de sobresuscripción TLS:

- Solucionar problemas de sobresuscripción TLS/SSL

Paso 6: Retroceda o restrinja el ámbito si ve:

- Saturación sostenida de CPU de inspección.

- Aumento de la latencia visible para el usuario.
- Fallos de intercambio de señales TLS.
- Las aplicaciones empresariales fallan después del descifrado.
- Sobresuscripción o errores SSL excesivos.

Paso 7: Consideración del impacto de TLS 1.3

La adopción de TLS 1.3 puede afectar la visibilidad y el comportamiento, ya que ciertas características de entrada en contacto e inspección difieren de TLS 1.2.

Causa

El descifrado SSL/TLS requiere recursos informáticos adicionales para descifrar, inspeccionar y volver a cifrar los flujos de tráfico. El impacto en el rendimiento varía significativamente en función de los patrones de tráfico, las políticas de inspección aplicadas al tráfico descifrado y la configuración de implementación específica. Sin una planificación adecuada y una implementación gradual, las organizaciones pueden experimentar una degradación inesperada del rendimiento en los entornos de producción.

Contenido relacionado

- Guía de configuración de dispositivos de Cisco Secure Firewall Management Center: reglas de descifrado
- Guía de políticas de descifrado de Cisco Secure Firewall
- Práctica recomendada para el orden de reglas de políticas de descifrado
- Simplificación del descifrado con Secure Firewall 7.7 de Cisco
- Prácticas recomendadas de reglas de descifrado
- Hoja de datos de Cisco Firepower serie 4100
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).