Detector y guardia (redes Riverhead) FAQ de la anomalía del tráfico

Contenido

Introducción

Este documento aborda las preguntas más frecuentes (FAQ) relacionadas con Cisco Traffic Anomaly Detector and Guard (Redes Riverhead).

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Q. ¿Cuál es la contraseña predeterminada para el detector de anomalía en el tráfico de Cisco y el guardia?

A. La contraseña predeterminada para el detector de anomalía en el tráfico de Cisco y el guardia es **admin/rhadmin**.

Q. Cambié la información de la fecha a partir del 08062004 a una fecha futura de

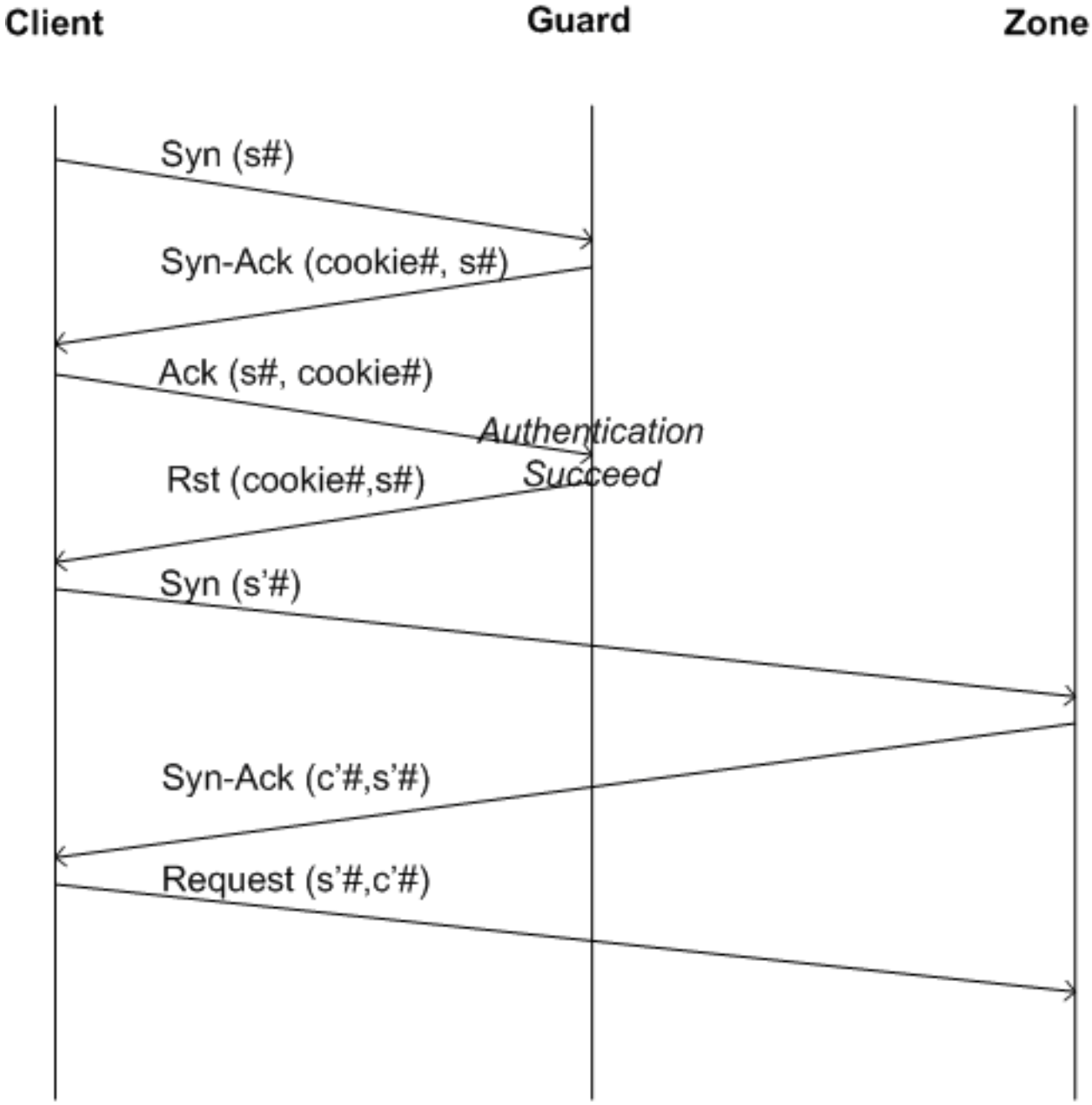
12012004 usando el “comando CLI de la fecha el 12012004". Entonces probé el cambio de fecha a una zona vía SNMP OID rhZoneLastChangeTime. Esto trabajada bien exceptúa cuando la fecha se cambia a una fecha anterior que la fecha cambiada último. Después, cambié el datar de 08062004 en el CLI. Sin embargo, la respuesta SNMP OID a preguntar para el rhZoneLastChangeTime seguía siendo 12012004 (la vieja fecha). Después de que una recarga, la respuesta OID mostrara el cambio de fecha (más reciente) correcto. ¿Es una falla?

A. Éste es el Id. de bug Cisco CSCuk52710 (clientes registrados solamente). No se recomienda generalmente para cambiar la época del dispositivo al revés. Esto puede dar lugar a la coincidencia de un ciertos datos del historial. Una solución alternativa para este problema es recomenzar el SNMP-servidor siempre que la hora se fije al revés:

```
admin@Guard-conf#no service snmp-server admin@Guard-conf#service snmp-server
```

Esto borra el caché SNMP y trae los datos actualizados al solicitante.

Q. ¿Cuál es la diferencia entre el Restablecimiento TCP y la Seguro-restauración TCP?



- **Restauración:** Conveniente para todas las aplicaciones TCP que revisan para conectar cuando se recibe un paquete RST (o permitir al usuario para volver a conectar). La conexión se cierra con un paquete RST y no se envía ninguna etiqueta. Vea la figura para el flujo de paquetes del algoritmo de la restauración.
- **Seguro-restauración:** Mientras que el método antedicho requiere la conciencia del nivel de la aplicación, la seguro-restauración requiere solamente la conformidad del stack RFC TCP, pero agrega un segundo retardo 3 a la primera vez de configuración de conexión. Es conveniente para la mayoría de los protocolos TCP automáticos (tales como correo). Como contestación al cliente SYN, el guardia envía un ACK con un mún número de acuse de recibo que sostenga un Cookie. Si el cliente es obediente con el RFC 793, contesta con un paquete RST que contenga el mún número de acuse de recibo y retransmita el SYN original después de un 3-segundo descanso. Cuando el guardia recibe el paquete RST con el mún número de acuse de recibo, autentica la conexión y no interfiere con la conexión siguiente. La advertencia principal en esta solución es que algunos Firewall caen silenciosamente el ACK malo-numerado aunque éste no es conforme a RFC. la orden n para proporcionar una solución en estos casos, si el guardia recibe un segundo paquete SYN de la misma fuente en

el plazo de 4 segundos del primeros, sin el RST mientras tanto, el segundo SYN se trata de la misma forma que se trata en el método de la restauración.

Q. Después de que una actualización que recibo “no pueda conectar con el módulo de administración; EL SISTEMA NO ESTÁ COMPLETAMENTE - OPERATIVO: La conexión rechazada no puede escribir mensaje de error al socket”. ¿Cómo resuelvo este problema?

A. Además del `no puede conectar con el módulo de administración; EL SISTEMA NO ESTÁ COMPLETAMENTE - OPERATIVO: La conexión rechazada no puede escribir al` mensaje de `error de socket`, este error se genera cuando usted reinicia:

```
myguard@GUARDUS#reboot Are you sure? Type 'yes' to reboot yes sh: /sbin/reboot: Input/output
error myguard@GUARDUS# myguard@GUARDUS#show diagnostic-info Can't connect to managment module;
SYSTEM IS NOT FULLY OPERATIONAL: Connection refused Can't write to socket Management module is
busy. Please try again in 10 seconds Failed to get counters myguard@GUARDUS# myguard@GUARDUS#
Message from syslogd@GUARDUS at Sun Sep 19 17:38:51 2004 ... GUARD-US RHWatchdog: RHWatchdog:
subsystem failure - CM
```

Esto parece un error de sistema de archivos en el guardia. Para solucionar los errores FS, reinicie al guardia y mire el **con atención el proceso fsck**. Si usted consigue en el modo de usuario único, publique el **fsck - y/**comando de pedir un funcionamiento manual del **fsck**.

Q. Cuando configuro una zona usando la plantilla predeterminada, no puedo encontrar la plantilla de política HTTP bajo zona cuando publico “el comando de las directivas de la demostración”. Veo cada otra plantilla de política a excepción del HTTP. ¿Cómo puedo encontrarlo?

A. La política predeterminada está disponible cuando usted publica el **wr t |** ordene e incluya el HTTP. Esto le muestra algo similar a **HTTP -1 10.0 de la plantilla de política habilitados**. El detector de anomalía en el tráfico de Cisco y el guardia entonces mira el tráfico que se basa en la forma del umbral que la política HTTP está basada encendido.

Q. ¿Cómo realizo la recuperación de contraseña del usuario raíz?

A. Refiera al guardia de Cisco y a la recuperación de contraseña del detector de la anomalía del tráfico para las instrucciones en la recuperación de contraseña del **usuario raíz**.

Q. ¿Puedo importar los Certificados de encargo SSL al guardia de la anomalía de Cisco?

A. No, guardia de la anomalía de Cisco soporta solamente el certificado uno mismo-firmado SSL.

Q. Recibí este mensaje de error. ¿Cómo puedo resolver el problema? **RHWatchdog: RHWatchdog: Hardware Monitoring card reports HW errors.**

A. Vuelva a sentar la fuente de alimentación para resolver el problema.

Información Relacionada

- Guardia de Cisco y Documentación técnica de las aplicaciones mitigantes
- Soporte Técnico y Documentación - Cisco Systems