Detector da anomalia do tráfego e protetor (redes Riverhead) FAQ

Índice

Introdução

Este documento trata das perguntas mais frequentes (FAQ) relativas ao Traffic Anomaly Detector and Guard da Cisco (redes Riverhead).

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Q. Que é a senha padrão para o detector e o protetor da anomalia do tráfego de Cisco?

A. A senha padrão para o detector e o protetor da anomalia do tráfego de Cisco é **admin/rhadmin**.

Q. Eu mudei a informação da data de 08062004 a uma data futura de 12012004 usando da “o comando CLI data 12012004". Eu testei então a alteração de dados a uma zona através do SNMP OID rhZoneLastChangeTime. Isto trabalhou bem a não

ser que quando a data é mudada a uma data mais cedo do que a última data mudada. Em seguida, eu mudei datar de 08062004 no CLI. Contudo, a resposta do SNMP OID a perguntar para o rhZoneLastChangeTime permaneceu 12012004 (a data velha). Depois que um reload, a resposta OID mostrou (a última) alteração de dados correta. Isto é um bug?

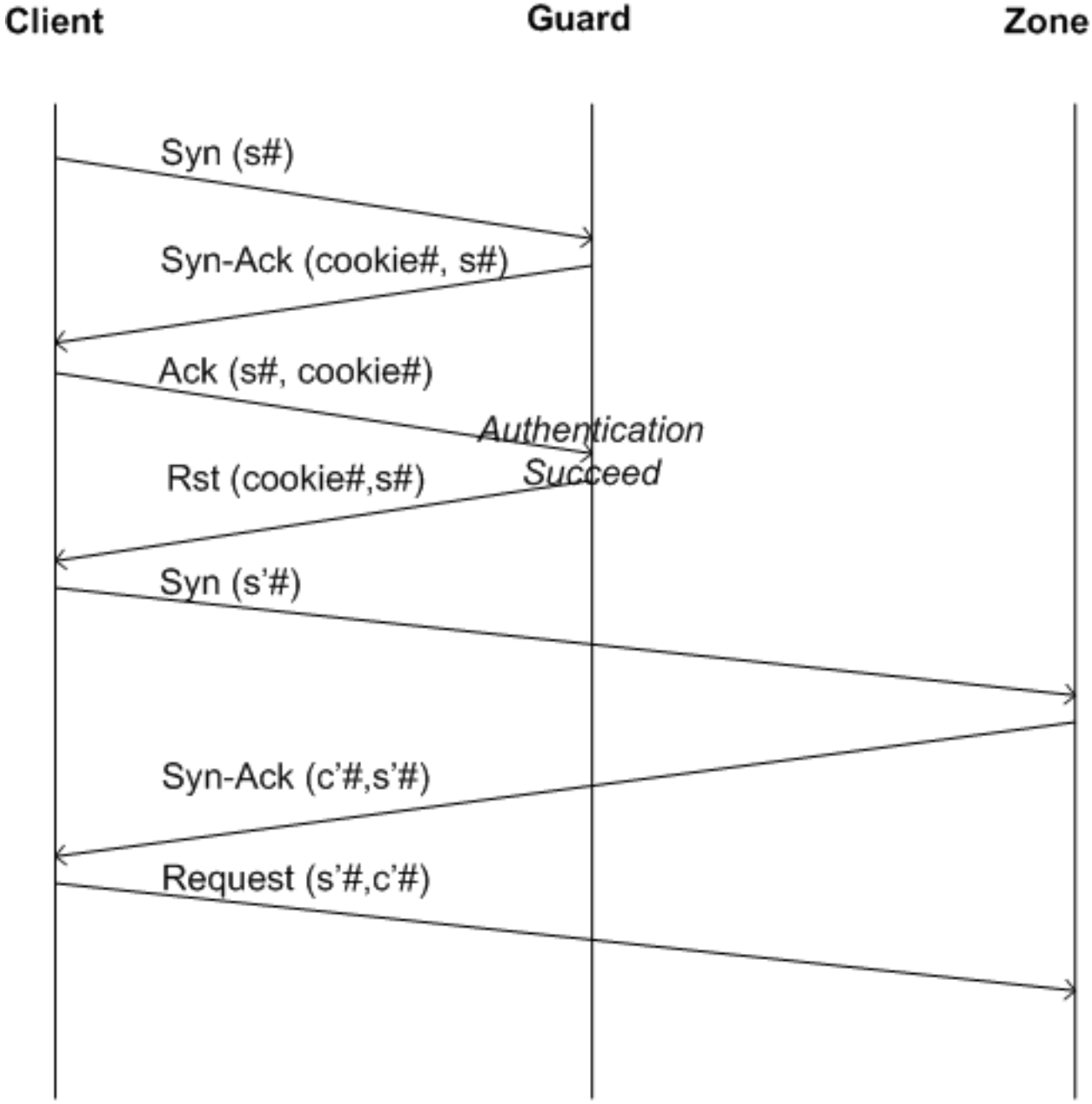
A. Esta é a identificação de bug Cisco CSCuk52710 (clientes registrados somente). Geralmente não se recomenda mudar para trás a época do dispositivo. Isto pode conduzir à sobreposição de alguns dados históricos. Uma ação alternativa para este problema é reiniciar o servidor snmp sempre que a hora é ajustada para trás:

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

admin@Guard-conf#service snmp-server
```

Isto cancela o esconderijo SNMP e traz os dados actualizados ao solicitador.

Q. Que é a diferença entre o TCP Reset e a Seguro-restauração TCP?



- **Restauração:** Apropriado para todos os aplicativos de TCP/IP que experimentam de novo para conectar quando um pacote de RST for recebido (ou para permitir o usuário de reconectar). A conexão é fechada com um pacote de RST e nenhuma etiqueta é enviada. Veja a figura para o fluxo de pacote de informação do algoritmo da restauração.
- **Seguro-restauração:** Quando o método acima exigir a conscientização do nível de aplicativo, a seguro-restauração exige somente a conformidade da pilha RFC TCP, mas adiciona um segundo atraso 3 à primeira vez de instalação de conexão. É apropriado para a maioria de protocolos de TCP automáticos (tais como o correio). Como uma resposta ao cliente SYN, o protetor envia um ACK com um número de reconhecimento ruim que guarde um Cookie. Se o cliente é complacente com RFC 793, responde com um pacote de RST que contenha o número de reconhecimento ruim e retransmita o SYN original após um 3-segundo intervalo. Quando o protetor recebe o pacote de RST com o número de reconhecimento ruim, autentica a conexão e não interfere com a conexão seguinte. A advertência principal nesta solução é que alguns Firewall deixam cair silenciosamente o ACK ruim-numerado mesmo que este não seja em conformidade com RFC. a ordem n para fornecer nesses casos uma solução, se o protetor recebe um segundo pacote SYN da mesma fonte dentro de 4 segundos do primeiros,

sem o RST in-between, o segundo SYN está tratada da mesma forma enquanto é tratada no método da restauração.

Q. Depois que uma elevação que eu recebo “não pode conectar ao módulo de gerenciamento; O SISTEMA NÃO É PLENAMENTE OPERACIONAL: A conexão recusada não pode escrever Mensagem de Erro ao soquete”. Como posso corrigir este problema?

A. Além do que `não pode conectar ao módulo de gerenciamento; O SISTEMA NÃO É PLENAMENTE OPERACIONAL: A conexão recusada não pode escrever à` mensagem de `erro de soquete`, este erro é gerada quando você recarrega:

```
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
```

Isto olha como um erro de sistema de arquivos no protetor. A fim resolver os erros FS, recarregue o protetor e olhe o **processo fsck próximo**. Se você obtém no modo do usuário único, emita o **fsck - y/**comando pedir uma corrida manual do **fsck**.

Q. Quando eu configuro uma zona usando o molde do padrão, eu sou incapaz de encontrar o template de política HTTP sob a zona quando eu emito da “o comando das políticas mostra”. Eu ver cada outro molde de política à exceção do HTTP. Como posso eu o encontrar?

A. A política padrão está disponível quando você emite o **wr t |** comande e inclua o HTTP. Isto mostra-lhe algo similar a **HTTP -1 10.0 do molde de política permitidos**. Cisco trafica o detector da anomalia e o protetor a seguir olha o tráfego que é baseado no formulário do ponto inicial que a política HTTP está baseada sobre.

Q. Como eu executo a recuperação de senha do usuário de raiz?

A. Refira o protetor de Cisco e a recuperação de senha do detector da anomalia do tráfego para instruções na recuperação de senha do **usuário de raiz**.

Q. Posso eu importar Certificados feitos sob encomenda SSL ao protetor da anomalia de Cisco?

A. Não, protetor da anomalia de Cisco apoia somente o certificado auto-assinado SSL.

Q. Eu recebi este Mensagem de Erro. Como posso eu resolver a edição?

```
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
```

A. Assente a fonte de alimentação para resolver a edição.

Informações Relacionadas

- Cisco guardam e a documentação técnica das ferramentas de mitigação
- Suporte Técnico e Documentação - Cisco Systems