502/504 erros GATEWAY_TIMEOUT ao consultar às sites determinado

Índice

Pergunta:

Por que nós vemos 502/504 erros GATEWAY_TIMEOUT ao consultar às sites determinado?

Sintomas: Os usuários estão recebendo 502 ou 504 erros de timeout do gateway de Cisco WSA ao consultar a determinados Web site

Os usuários estão recebendo 502 ou 504 erros de timeout do gateway ao consultar aos Web site. Os logs do acesso mostrariam 'NONE/504 ou 'NONE/502

Linha de registro do acesso da amostra:

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - www.example.com DIRETO - .....

Há muitas razões pelas quais WSA pode retornar um erro de timeout de 502 ou 504 gateways. Embora estas respostas de erro sejam similares, é importante compreender as diferenças sutil entre elas.

Estão aqui alguns exemplos dos tipos de encenações que podem ocorrer:

- **502**: O WSA tentou estabelecer uma conexão de TCP com o servidor de Web, mas não recebeu um SYN/ACK.
- **504**: O WSA está recebendo um TCP Reset (RST) que termina a conexão com o servidor de Web.
- **504**: O WSA não está obtendo uma resposta de um serviço requerido antes da comunicação com o servidor de Web, tal como o DNS está falhando.
- **504**: O WSA estabeleceu uma conexão de TCP com o servidor de Web e enviou um pedido GET, mas o WSA nunca recebe a resposta HTTP.

Estão abaixo os exemplos de cada encenação e de mais detalhes em relação aos problemas potenciais:

502: O WSA tentou estabelecer uma conexão de TCP com o servidor de Web, mas não recebeu um SYN/ACK.
Se o servidor de Web não responde aos pacotes SYN do WSA, depois que uma certa

quantidade de tentativas, o cliente estará enviada a um erro de timeout de 502 gateways.

As causas típicas para esta são:
1. O servidor de Web ou a rede do servidor de Web estão tendo edições.
2. Uma questão de rede na rede WSA está impedindo que os pacotes SYN obtenham ao Internet.
3. Um Firewall ou um dispositivo similar estão deixando cair os pacotes SYN WSA ou o SYN/ACK do servidor de Web
4. A falsificação de IP é permitida no WSA, mas não configurada corretamente (nenhuma reorientação do caminho de retorno)

Passos de Troubleshooting:

A primeira etapa é verificar se o WSA pode ping ICMP o servidor de Web. Isto pode ser feito usando o seguinte comando CLI:
Sibilo www.example.com WSA>
Se o sibilo falha, não significa que o server está para baixo. Pode-se significar que os pacotes ICMP estão obtendo obstruídos em algum lugar no trajeto. Se o sibilo sucede, a seguir nós podemos saber certamente que o WSA tem um nível layer3 básico da Conectividade ao servidor de Web.
Um teste do telnet verificará se o WSA tem a capacidade para estabelecer uma conexão de TCP na porta 80 ao servidor de Web. Veja as instruções mais neste artigo executando um teste do telnet.

Bloco das questões de rede ou do Firewall
Se o sibilo é bem sucedido, mas o telnet falha, há uma boa possibilidade que um dispositivo de filtragem, tal como um Firewall, está impedindo que este tráfego obtenha através da rede. Recomenda-se que os logs e/ou as capturas de pacote de informação do Firewall do Firewall estão analisados para uns detalhes mais adicionais.
A falsificação de IP permite, mas configurado não corretamente
Se explicitamente proxying através do WSA ou do teste do telnet é bem sucedido, este mostra que o WSA pode se comunicar diretamente ao servidor de Web, mas quando proxys de um cliente com o WSA com falsificação de IP, há um problema.

Sem falsificação do IP de cliente:
- O WSA envia um SYN ao servidor de Web usando seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT como a fonte. Quando o pacote volta, vai diretamente ao WSA.

Com falsificação do IP de cliente:
- O WSA envia o SYN, mas pelo contrário, usa o IP do cliente como a fonte. Sem uma instalação de rede especial, o pacote de informação de retorno será enviado ao cliente em vez do WSA.
- A fim usar a falsificação do IP de cliente, a rede deve ser configurada em uma maneira muito específica a fim facilitar que os pacotes estão reorientados corretamente. Se os pacotes do caminho de retorno do servidor de Web estão sendo enviados ao cliente em vez do WSA, o WSA nunca verá os server SYN/ACK e enviará um erro de timeout de 502 gateways de volta ao cliente.

504: O WSA está recebendo um TCP Reset (RST) que termina a conexão com o servidor de Web.

Se o WSA recebe um pacote TCP Reset em sua conexão de upstream ao servidor de Web, o WSA enviará um erro de timeout de 504 gateways ao cliente.

As causas típicas para esta são:
1. Cisco mergulha 4 que o monitor de tráfego (L4TM) está obstruindo o proxy WSA de conectar o servidor de Web.
2. Um Firewall, o IDS, o IPS, ou o outro dispositivo da inspeção de pacote de informação estão obstruindo o WSA.

Passos de Troubleshooting:
Determine primeiramente se o TCP RST está vindo do L4TM ou de um outro dispositivo.
Se o L4TM está obstruindo este tráfego, o tráfego aparecerá nos relatórios GUI sob o "*monitor -> o monitor de tráfego L4*". Se não, o RST está vindo de um dispositivo diferente.
Obstrução L4TM:
Recomenda-se que se o L4TM está obstruindo, não obstrua nas portas que o proxy WSA igualmente está executando sobre. Há umas razões múltiplas para esta:
1. O proxy WSA fornece uma mensagem de erro compatível no caso do problema, em vez apenas do TCP que restaura a conexão. Isto ajudará a confusão do limite dos utilizadores finais quando são obstruídos.
2. O proxy WSA tem a capacidade para fazer a varredura e obstruir do índice específico, visto que o L4TM obstrui todo o tráfego que combina um endereço IP de Um ou Mais Servidores Cisco ICM NT põr.
A fim configurar o L4TM para não obstruir em portas de proxy, vá ao "*GUI - serviços do > segurança - > o monitor de tráfego L4*".
Se o local é um site ruim conhecido, mas há umas razões pelas quais o tráfego deve ser permitido, o local pode estar listado branco em:
"*GUI - > gerenciador de segurança da Web - > monitor de tráfego L4 - > permita a lista*"

Obstrução do Firewall/IDS /IP:
Se um outro dispositivo nos trabalhos em rede está obstruindo o WSA da conexão ao servidor de Web, recomenda-se analisar o seguinte:
1. Logs do bloco do Firewall
2. Captações do ingresso/pacote de saída durante o problema

Os logs do bloco podem rapidamente confirmar se o dispositivo está obstruindo o WSA. Às vezes um Firewall, um IPS, ou um IDS obstruirão o tráfego e não o registrarão apropriadamente. Se este é o caso, a única maneira de provar de onde o TCP RST está vindo, é obter o ingresso e a saída captura do dispositivo. Se um RST está sendo mandado a interface de ingresso e nenhum pacote viajou através do lado de saída, o dispositivo de segurança é definidamente a causa.

504: O WSA estabeleceu uma conexão de TCP com o servidor de Web e enviou um pedido GET, mas o WSA nunca recebe a resposta HTTP.

Se o WSA envia um HTTP GET, mas nunca recebe uma resposta, enviará um erro de timeout de 504 gateways ao cliente.

As causas típicas para esta são:

- Um Firewall, o IDS, o IPS, ou o outro dispositivo da inspeção de pacote de informação estão permitindo a conexão de TCP, mas estão obstruindo o índice HTTP de alcançar o servidor de Web. Neste caso, o teste do telnet pode ajudar a isolar-se que o tipo de dados HTTP está

sendo obstruído.
Os logs do bloco do Firewall podem rapidamente confirmar se/porque o dispositivo está obstruindo o WSA. Às vezes um Firewall, um IPS, ou um IDS obstruirão o tráfego e não o registrarão apropriadamente. Se este é o caso, a única maneira de provar de onde o TCP RST está vindo, é obter o ingresso e a saída captura do dispositivo. Se um RST está sendo mandado a interface de ingresso e nenhum pacote viajou através do lado de saída, o dispositivo de segurança é definidamente a causa.

Conectividade de teste com um servidor de Web usando o telnet

Do WSA CLI, execute o **comando telnet**:

Telnet WSA>
Selecione por favor de que o conecte querem ao telnet.
1. Automático
2. Gerenciamento (192.168.15.200/24: wsa.hostname.com)
3. P1 (192.168.113.199/24: data.com)
[1]> **3**

Incorpore o hostname ou o endereço IP de Um ou Mais Servidores Cisco ICM NT remoto.
[]> **www.example.com**

Entre na porta remota.
[25]> **80**

Tentando 10.3.2.99…
Conectado a www.example.com.
O caractere de escape é “^]”.

Note: A mensagem “conectada” no vermelho, indica que TCP estabelecido com sucesso entre o WSA e o servidor de Web.

Um pedido do HTTP pode manualmente ser enviado através desta sessão de Telnet também. O seguinte é um pedido da amostra que possa ser datilografado após a mensagem “conectada”:

GET http://www.example.com HTTP/1.1
HOST: www.example.com
{Entre}

Note: Certifique-se adicionar a tecla semelhante a tecla ENTER extra na extremidade, se não o server não responderá ao pedido.