Diagnosticando problemas de conexão com o Fortigate - PARTE 1

Autor: Flavio Borup

VISÃO GERAL

Esse artigo visa mostrar as técnicas mais comuns para fazer diagnóstico de problemas complexos usando a plataforma Fortigate da Fortinet. O artigo se refere à versão 5.4, mas como as versões 5.6 e 6.0 estão começando a substituir a 5.4, nem todos as técnicas aqui apresentadas podem ser válidas.

PRÉ-REQUISITOS

Esse artigo tem como público-alvo responsáveis por ambientes com Fortigate com um conhecimento mínimo de administração do FortiOS, bem como conceitos de segurança, modelo OSI e rede. Na imensa maioria das vezes, para o diagnóstico, é necessário um usuário com privilégio de “super_admin” ou “prof_admin”

INTRODUÇÃO

Apesar da Interface Web/HTTPS ser a mais indicada para operação, gerenciamento, manutenção ou administração, existem situações onde a linha de comando do FortiOS, acessível via SSH é a opção mais indicada para resolver problemas complexos. Às vezes é necessária uma combinação dessas interfaces ou até múltiplas sessões SSH simultâneas.

UM PROBLEMA

Existem situações onde “as coisas não funcionam” e “ninguém sabe o motivo”. Não se desespere, você não está sozinho. Mesmo em ambientes simples, configurações erradas, desconhecimento do ambiente ou até “Bugs” podem causar problemas.

As situações mais comuns são de tráfego que não está chegando ao destinatário conforme esperado e esse artigo vai mostrar os meios pelos quais podemos fazer recolhimento de informações para diagnosticar o problema.

O QUE É COMUM A TODOS OS PROBLEMAS

Independente do problema, sempre existe um conjunto mínimo de informações que tem que ser recolhida antes do diagnóstico avançado, como por exemplo, mas não limitado a:

1. IP ou rede de origem
2. IP ou rede de destino
3. Protocolo
4. Porta TCP/IP
5. Interface física ou lógica por onde o tráfego passa
6. ID da Policy envolvida
7. Rotas disponíveis para o destino

EXEMPLO DE PROBLEMA E SOLUÇÃO

Problema: Aplicação não funciona.

Pode parecer bobagem, mas as descrições dos problemas são sempre assim: impossíveis de serem avaliadas sem ter que fazer mais perguntas. Vamos supor que após um breve contato, você tenha conseguido as informações citadas no item “O QUE É COMUM A TODOS OS PROBLEMAS”, vamos dar alguns exemplos.

Apesar do PING/ICMP não ser 100% conclusivo, pois há situações nas quais o PING/ICMP é propositalmente bloqueado, pode-se começar com o bom e velho PING para dar início.

FGT5000F98789786 # execute ping-options source

<string> Auto | <source interface IP>. FGT5000F98789786 # execute ping-options source

10.14.0.99 FGT5000F98789786 #

DICAS, TRUQUES E MACETES: *MESMO QUE VOCÊ USE UM IP QUE NÃO EXISTE, ADIVINHA, NÃO DÁ ERRO... USE UM IP QUE REALMENTE EXISTA, POIS NÃO TEM MENSAGEM DE ERRO. ESSE EXEMPLO ACIMA FOI GERADO EXATAMENTE ASSIM, COM UM IP ABRITRÁRIO*

FGT5000F98789786 # execute ping 8.8.8.8 PING 8.8.8.8 (8.8.8.8): 56 data

bytes

64 bytes from 8.8.8.8: icmp_seq=0 ttl=120 time=43.8 ms

Lembre-se de avaliar se é necessário alterar o IP de origem desse PING, pois as vezes o FortiOS arbitra uma interface inapropriada para fazer a saída do PING, nesse caso, vale determinar de forma clara, qual dos IPs (e, portanto, Interfaces) do FortiOS devem ser usadas para gerar a saída do PING. O default é “auto” e cada vez que carrega o SSH, isso volta para o Default.

Nem todos os comandos tem o parâmetro “source”, outro que tem é o “traceroute”, mas o “telnet”, por exemplo, não tem. Evite pensar no FortiOS como sendo um PC local para fazer os testes, tente ter um PC Windows ou Linux na rede para ajudar na avaliação.

FGT5000F98789786 # execute traceroute-options source

<string> Auto | <source interface IP>.

Indo adiante, sabemos que o PING/ICMP não é conclusivo por motivos diversos ele é apenas o ponto de partida para começar a avaliação.

Outros comandos úteis:
Ver a tabela ARP< para ver os IPs e MACs da rede, isso pelo menos ajuda a observar se camada 2 pelo menos está funcional, entre outras coisas.

FGT5000F98789786 # get sys arp

Address	Age(min)	Hardware Addr	Interface
10.14.0.2	0	01:da:44:a4:0a:c0	internal1
10.14.0.10	0	65:00:fa:81:89:ca	internal1
10.14.0.17	1	01:2b:73:ac:b6:b3	internal1
10.14.0.32	0	01:a1:1f:f0:4e:93	internal1

Ver a tabela de rotas é importante também, para avaliar se há realmente rotas que permitam chegar no destino desejado. No exemplo, abaixo, vemos que temos rotas para dois escritórios diferentes e oq eu não estiver relacionado com isso, será encaminhado para Internet.

FGT5000F98789786 # get router info routing-table all

S* 0.0.0.0/0 [10/0] via 201.224.76.89, wan1
S 10.10.0.0/8 [10/0] is directly connected, VPN_MAINOFFICE S 10.0.128.0/21 is directly connected, VPN_REMOTEOFFICE

Faça uma simulação do tráfego que está sendo avaliado e faça o rastreamento, para saber se o tráfego está realmente passando através do Firewall, as vezes ele pode estar sendo bloqueado em outro ponto da rede.
Como se trata de uma versão modificada do “tcpdump”, é um “sniffer”. No caso a seguir, pode-se observar o tráfego indo e voltando pelas Interfaces “Internal1” e “VPN_MAINOFFICE”

FGT5000F98789786 # diagnose sniffer packet any 'host 10.24.0.10 and port 161' 4 filters=[host 10.24.0.10 and port 161]
0.369322 internal1 in 10.14.0.2.161 -> 10.24.0.10.60709: udp 232

0.369403 VPN_MAINOFFICE out 10.124.0.2.161 -> 10.24.0.109.60709: udp 232