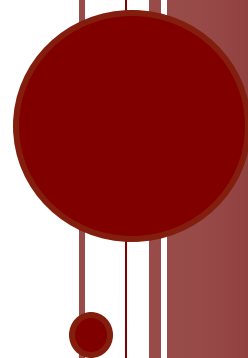




DIAGNOSTICANDO
PROBLEMAS DE CONEXÃO
COM O FORTIGATE –
PARTE 2

Autor: Flavio Borup



Diagnosticando problemas de Fortigate – PARTE 2

VISÃO GERAL

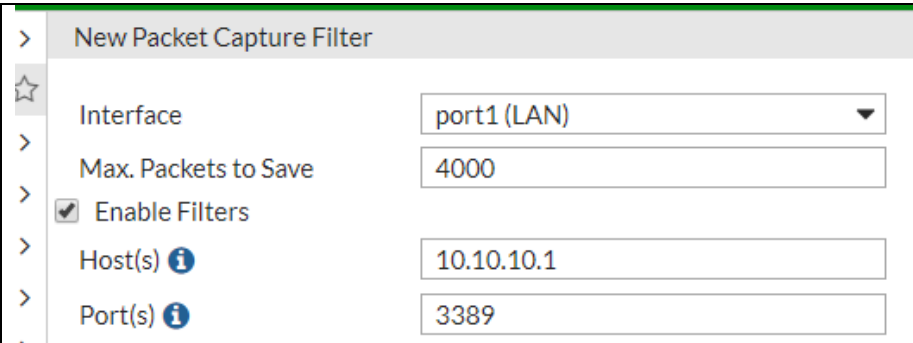
Dando continuidade ao artigo, parte 1, vamos seguir aprendendo mais algumas técnicas de avaliação de problemas usando a linha de comando (CLI).

Problema: Aplicação não funciona - *CONTINUAÇÃO*.

A ferramenta de “sniffer” do FortiOS hoje em dia está integrada na GUI (Interface Web) e apesar de limitada é bem útil. Só tem dois problemas: 1) Não está disponível em todos os equipamentos ou configurações de hardware e 2) em algumas versões ele está disponível, mas não tem “atalho”, só se chega na ferramenta usando um “link direto”. Em certos equipamentos que não tem discos específicos de armazenamento, mesmo digitando o Link direto e vendo a funcionalidade como disponível, não tente usar, não vai dar certo.

Exemplo: usando a URL: [https://\[Host-IP\]/p/firewall/sniffer](https://[Host-IP]/p/firewall/sniffer) é possível ver o Sniffer, mas em certos equipamentos pode-se acabar vendo o erro: “Error 403: Access denied.”

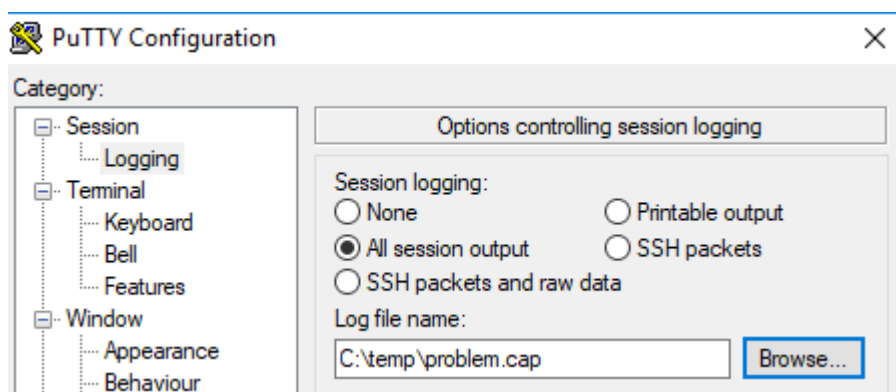
Se a funcionalidade estiver disponível, você veria:

	Isso geraria um arquivo “.cap” que mais tarde pode ser aberto em ferramentas como o antigo EtherReal, hoje WireShark e até o MS Network Monitor 3.4.
---	--

A alternativa é fazer via CLI, usando o comando:

```
diag sniffer packet any 'host 10.10.10.1 and port 3389' 60 a
```

O problema é que isso será enviado para a tela e não vai ajudar muito. O ideal seria enviar todo a saída para um arquivo-texto. Segue exemplo, usando o PUTTY.



Exemplos de como usar o “sniffer” para diagnosticar alguns problemas

Diagnosticando problemas de Fortigate – PARTE 2

Vendo todo o tráfego, relativo á porta 80, apenas na Porta1

```
diagnose sniffer packet port1 'port 80'
```

Vendo todo o tráfego, menos o da porta 22, para tirar o SSH da análise, em todas as interfaces

```
diagnose sniffer packet any 'not port 22'
```

Vendo o tráfego relative a um certo Servidor, mas sem o protocolo RDP, abreviando

```
diag sniff packet any 'host 1.2.3.4 and not port 3389'
```

Versões mais modernas do FortiOS suportam o “grep” para fazer filtros mais precisos, no caso, podemos excluir (-v) a Porta 1 da avaliação preliminar. O parâmetro “4” mostra a porta relativa onde em qual Interface, o tráfego foi detectado.

```
diagnose sniffer packet any 'port 80' 4 | grep -v port1
```

Abaixo, a “ida e volta” de um pacote, observe o número sequencial do ACK

```
VPN-OfficeA in 10.2.1.1.61781 -> 14.2.1.2.80: 1789585242
```

```
VPN-OfficeA out 14.2.1.2.80 -> 10.2.1.1.61781: ack 1789585243
```

Nesse exemplo, vemos que o cliente usou o “socket” de origem 10.2.1.1:61781 para se conectar ao sistema remoto, no “socket” 14.2.1.2:80 de destino.

E também vemos que esse tráfego passou pela Interface de VPN chamada VPN-OfficeA

Isso pelo menos prova que o tráfego passou pelas interfaces e que havia regras (policies) que permitam a passagem desse tráfego em específico.

Se não houve regra (policy) ou se o destino não estiver disponível, pode-ser ver algo como:

```
82.378862 10.1.1.7.62421 -> 100.4.1.1.80: syn 314583005
```

```
85.396138 10.1.1.7.62421 -> 100.4.1.1.80: syn 314583005
```

```
91.415968 10.1.1.7.62421 -> 100.4.1.1.80: syn 314583005
```

Nesse caso acima, houve 3 tentativas, não houve resposta e cada tentativa seguinte, demorou mais que a anterior, comportamento esperado do TCP.

```
4.025219 VPN-WAN1 in 10.1.1.7.62832 -> 100.4.0.1.80: syn 3491618932
```

```
7.030933 VPN-WAN1 in 10.1.1.7.62832 -> 100.4.0.1.80: syn 3491618932
```

```
13.035115 VPN-WAN1 in 10.1.1.7.62832 -> 100.4.0.1.80: syn 3491618932
```

Usando o parâmetro “4” ainda foi possível ver por qual interface o tráfego está passando.

Diagnosticando problemas de Fortigate – PARTE 2

Quer mais detalhes? Que tal o parâmetro “2”? O parâmetro “4” visto antes, se for substituído pelo parâmetro “2”, mostra coisas ainda mais interessantes, particularmente em tráfegos sem nenhuma criptografia, codificação ou proteção.

No exemplo abaixo, observa-se uma conexão HTTP (TCP/80), usando a função “GET”, no WebSite remoto “test.speedycom.net” ao usar um Browser similar ao MSIE7.

```
58.035814 10.122.1.7.61399 -> 10.24.0.105.80: psh 3762803081 ack 2705072207
0x0020 5018 ffff 65c5 0000 4745 5420 2f20 4854 P...e...GET./.HT
0x0030 5450 2f31 2e31 0d0a 4163 6365 7074 3a20 TP/1.1..Accept:.
0x0040 696d 6167 652f 6a70 6567 2c20 6170 706c image/jpeg,.appl
0x0050 6963 6174 696f 6e2f 782d 6d73 2d61 7070 ication/x-ms-app
0x0060 6c69 6361 7469 6f6e 2c20 696d 6167 652f lication,.image/
0x0070 6769 662c 2061 7070 6c69 6361 7469 6f6e gif,.application
0x0080 2f78 616d 6c2b 786d 6c2c 2069 6d61 6765 /xaml+xml,.image
0x0090 2f70 6a70 6567 2c20 6170 706c 6963 6174 /jpeg,.applicat
0x00a0 696f 6e2f 782d 6d73 2d78 6261 702c 202a ion/x-ms-xbap,.*
0x00b0 2f2a 0d0a 4163 6365 7074 2d4c 616e 6775 /*..Accept-Langu
0x00c0 6167 653a 2070 742d 4252 0d0a 5573 6572 age:.pt-BR..User
0x00d0 2d41 6765 6e74 3a20 4d6f 7a69 6c6c 612f -Agent:.Mozilla/
0x00e0 342e 3020 2863 6f6d 7061 7469 626c 653b 4.0.(compatible;
0x00f0 204d 5349 4520 372e 303b 2057 696e 646f .MSIE.7.0;.Windo
0x0100 7773 204e 5420 362e 333b 2057 4f57 3634 ws.NT.6.3;.WOW64
0x0110 3b20 5472 6964 656e 742f 372e 303b 202e ;.Trident/7.0;..
0x0120 4e45 5434 2e30 453b 202e 4e45 5434 2e30 NET4.0E;..NET4.0
0x0130 4329 0d0a 4163 6365 7074 2d45 6e63 6f64 C)..Accept-Encod
0x0140 696e 673a 2067 7a69 702c 2064 6566 6c61 ing:.gzip,.defla
0x0150 7465 0d0a 486f 7374 3a20 7465 7374 652e te..Host:.test.
0x0160 7167 6f67 2e63 6f6d 2e62 720d 0a43 6f6e speedycom.net..Con
0x0170 6e65 6374 696f 6e3a 204b 6565 702d 416c nection:.Keep-Al
0x0180 6976 650d 0a43 6163 6865 2d43 6f6e 7472 iver..Cache-Contr
0x0190 6f6c 3a20 6e6f 2d63 6163 6865 0d0a 0d0a ol:.no-cache....
```

Diagnosticando problemas de Fortigate – PARTE 2

Ou, nesse exemplo, um Web Server baseado em IIS:

```
58.037491 10.24.0.105.80 -> 10.122.1.7.61399: psh 2705072207 ack 3762803457
0x0000 4500 03bc 5f30 4000 8006 820a 0a18 0069      E..._0@.....i
0x0010 0a7a 0107 0050 efd7 a13c 204f e047 d301      .z...P...<.O.G..
0x0020 5018 fb2c d4af 0000 4854 5450 2f31 2e31      P...HTTP/1.1
0x0030 2032 3030 204f 4b0d 0a43 6f6e 7465 6e74      .200.OK..Content
0x0040 2d54 7970 653a 2074 6578 742f 6874 6d6c      -Type:.text/html
0x0050 3b20 6368 6172 7365 743d 5554 462d 380d      ;.charset=UTF-8.
0x0060 0a53 6572 7665 723a 204d 6963 726f 736f      .Server:.Microso
0x0070 6674 2d49 4953 2f37 2e35 0d0a 582d 506f      ft-IIS/7.5..X-Po
0x0080 7765 7265 642d 4279 3a20 4153 502e 4e45      wered-By:ASP.NET
```

É claro que isso é apenas “ Ponta do iceberg”, uma pequena parcela das possibilidades.

Quem sabe esse artigo mereça uma continuação? Só depende dos leitores.
