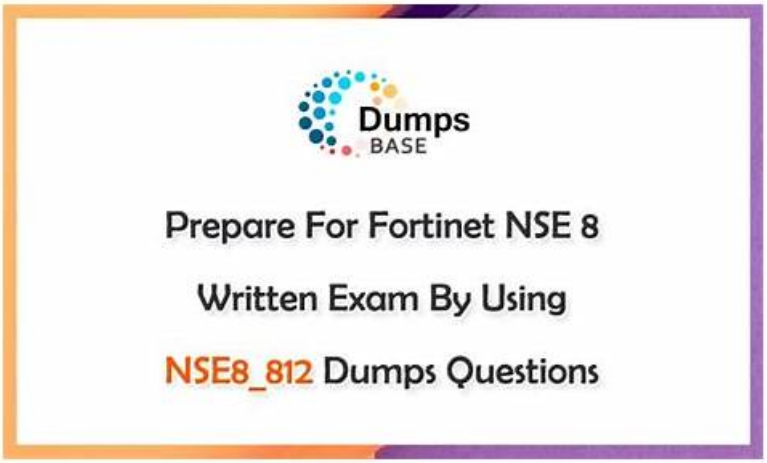
NSE8_812최고품질시험덤프자료 & NSE8_812최신업데이트버전인증덤프



참고: ITDumpsKR에서 Google Drive로 공유하는 무료, 최신 NSE8_812 시험 문제집이 있습니다: https://drive.google.com/open?id=1gZnoj4t1gCiQcX2JPNHNb7QVLDysxJFi

많은 분들이 고난의도인 Fortinet관련인증시험을 응시하고 싶어 하는데 이런 시험은 많은 전문적인 관련지식이 필요합니다. 시험은 당연히 완전히 전문적인 NSE8_812관련지식을 터득하자만이 패스할 가능성이 높습니다. 하지만 지금은 많은 방법들로 여러분의 부족한 면을 보충해드릴 수 있으며 또 힘든 Fortinet시험도 패스하실 수 있습니다. 혹은 여러분은 전문적인 Fortinet NSE 8 - Written Exam (NSE8_812)관련지식을 터득하자들보다 더 간단히 더 빨리 시험을 패스하실 수 있습니다.

NSE8_812 인증 시험을 받으려면 유효한 NSE7 인증과 네트워크 보안에 대한 2 년 이상의 경험이 있어야합니다. 또한 Fortigate, Fortianalyzer, Fortimanager 및 Fortisandbox를 포함한 Fortinet 제품 및 서비스에 대한 광범위한 지식이 있어야합니다.

Fortinet NSE8_812 시험을 통과하려면 응시자는 Fortinet 제품 및 기술에 대한 깊은 이해를 가져야합니다. Fortinet 제품을 사용하여 복잡한 네트워크 보안 솔루션을 설계, 구현 및 관리하는 능력을 보여 주어야합니다. 이 시험은 Fortinet 제품 및 솔루션으로 작업 한 경험이있는 숙련 된 네트워크 보안 전문가를 위해 설계되었습니다.

>> NSE8_812최고품질 시험덤프자료 <<

NSE8_812최고품질 시험덤프자료 최신 덤프로 시험정복하기

아직도Fortinet NSE8_812 인증시험을 어떻게 패스할지 고민하시고 계십니까? ITDumpsKR는 여러분이Fortinet NSE8_812덤프자료로Fortinet NSE8_812 인증시험에 응시하여 안전하게 자격증을 취득할 수 있도록 도와드립니다. Fortinet NSE8_812 시험가이드를 사용해보지 않으실래요? ITDumpsKR는 여러분께Fortinet NSE8_812시험패스의 편리를 드릴 수 있다고 굳게 믿고 있습니다.

Fortinet NSE8_812 시험 준비를 위해 개인은 교육 과정, 학습 안내서 및 모의 시험을 비롯한 다양한 자원을 활용할 수 있습니다. Fortinet은 또한 인증 프로그램의 다양한 범위를 제공하여 개인이 시험을 통과하고 진로를 발전시키는 데 필요한 기술과 지식을 개발할 수 있도록 지원합니다.

최신 Fortinet Network Security Expert NSE8_812 무료샘플문제 (Q77-Q82):

질문 # 77
Refer to the exhibits.
Exhibit A

```
vd: root/0
name: vpn-hub02-1
version: 2
interface: wan1 7
addr: 10.73.255.67:500 -> 10.73.255.82:500
tun_id: 10.73.255.82/::10.73.255.82
remote_location: 0.0.0.0
created: 82236s ago
peer-id: CN = fgtdc01.example.com
peer-id-auth: yes
assigned IPv4 address: 192.168.73.67/255.255.255.224
auto-discovery: 2 receiver
PPK: no
IKE SA: created 1/1  established 1/1  time 50/50/50 ms
IPsec SA: created 1/2  established 1/2  time 0/25/50 ms
  id/spi: 1 e4f6465bbae7490f/2535d26ef1f21557
  direction: initiator
  status: established 82236-82236s ago = 50ms
  proposal: aes256-sha256
  child: no
  PPK: no
  message-id sent/recv: 4/1
  lifetime/rekey: 86400/3863
  DPD sent/recv: 00000000/00000000
  peer-id: CN = fgtdc01.example.com
```

Exhibit B

```
fgt01-branch01 # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=vpn-hub02-1 ver=2 serial=1 10.73.255.67:0->10.73.255.82:0 u..id=10.73.255.82
tun_id6=::10.73.255.82 dst_mtu=1500 dpd-link=on weight=1
bound_if=7 lgwy=static/1 tun=tunnel/255 mode=auto/1 encap=none/536 options[0218]=npu create_dev frag
 accept_traffic=1 overlay_id=0
proxyid_num=1 child_num=0 refcnt=4 ilast=0 olast=0 ad=:/2
stat: rxp=1 txp=1500326 rxb=73 txb=273040631
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=vpn-hub02-1 proto=0 sa=1 ref=27 serial=1 auto-negotiate adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=6 options=1a227 type=00 soft=0 mtu=1438 expire=3844/0B replaywin=2048
       seqno=b1d18 esn=0 replaywin_lastseq=00000000 itn=0 qat=0 hash_search_len=1
  life: type=01 bytes=0/0 timeout=42902/43200
  dec: spi=4da0c1a4 esp=aes key=32 649504000696356 1c4c9b9d91e5e22c454446438480484a81e6bed9f9d3742ef
       ah=sha256 key=32 7fb9fce764431ba10b6da88263cd0484d9f5824cc9d5bd268db2cffca1a1d572
  enc: spi=f80065a7 esp=aes key=32 df2741a4d69cf6a241fe80b7722e1b13045b88457e7bf29ee171779b556c83cf
       ah=sha256 key=32 9e87bf36eca21c4732cf5af4ccdfe7f1dbc19e7e1afe17fe2a77475f2dd2b0fa
  dec:pkts/bytes=0/0, enc:pkts/bytes=1456559/316245764
  npu_flag=03 npu_rgwy=10.73.255.82 npu_lgwy=10.73.255.67 npu_selid=0 dec_npuid=1 enc_npuid=1
```

Exhibit C

```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set interface "wan1"
        set net-device enable
        set mode-cfg enable
        set proposal aes256-sha256
        set add-route disable
        set auto-discovery-receiver enable
        set remote-gw 10.73.255.82
    next
end
```

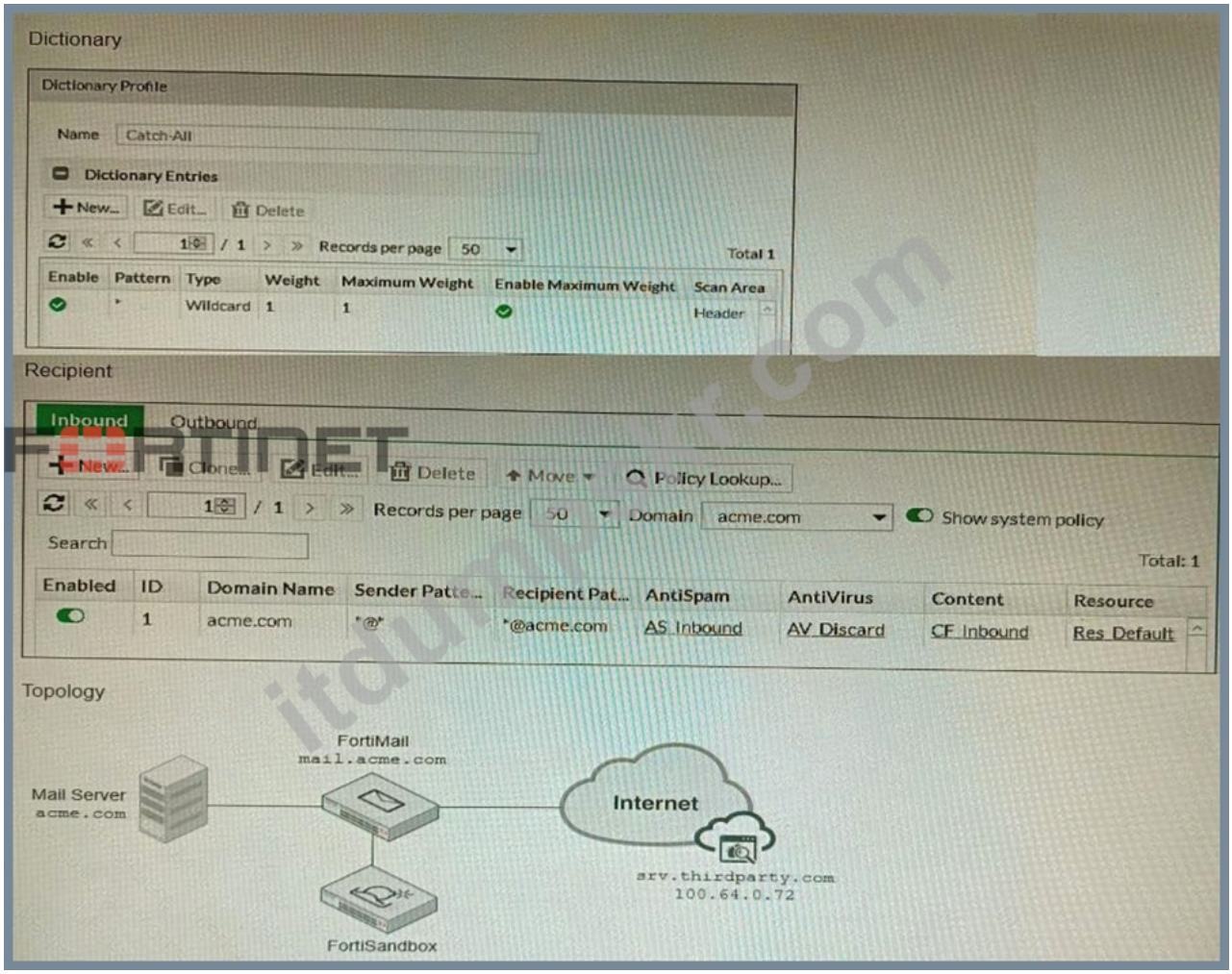
A customer is trying to set up a VPN with a FortiGate, but they do not have a backup of the configuration. Output during a troubleshooting session is shown in the exhibits A and B and a baseline VPN configuration is shown in Exhibit C Referring to the exhibits, which configuration will restore VPN connectivity?

- A.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set net-device enable
        set psksecret fortinet
    next
end
```
- B.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set npu-offload disable
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```
- C.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 1
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```
- D.
```
config vpn ipsec phase1-interface
    edit "vpn-hub02-1"
        set ike-version 2
        set authmethod signature
        set certificate "BR01FGTLOCAL"
        set peer "vpn-hub02-1_peer"
    next
end
```

정답：B

설명:
The output in Exhibit A shows that the VPN tunnel is not established because the peer IP address is incorrect. The output in Exhibit B shows that the peer IP address is 192.168.1.100, but the baseline VPN configuration in Exhibit C shows that the peer IP address should be 192.168.1.101.
To restore VPN connectivity, you need to change the peer IP address in the VPN tunnel configuration to 192.168.1.101. The correct configuration is shown below:
config vpn ipsec phase1-interface
edit "wan"
set peer-ip 192.168.1.101
set peer-id 192.168.1.101
set dhgrp 1
set auth-mode psk
set psk SECRET_PSK
next
end
Option A is incorrect because it does not change the peer IP address. Option B is incorrect because it changes the peer IP address to 192.168.1.100, which is the incorrect IP address. Option D is incorrect because it does not include the necessary configuration for the VPN tunnel.

질문 # 78
Refer to the exhibits.



The exhibits show a FortiMail network topology, Inbound configuration settings, and a Dictionary Profile.
You are required to integrate a third-party's host service (srv.thirdparty.com) into the e-mail processing path.
All inbound e-mails must be processed by FortiMail antispam and antivirus with FortiSandbox integration. If the email is clean, FortiMail must forward it to the third-party service, which will send the email back to FortiMail for final delivery, FortiMail must not scan the e-mail again.
Which three configuration tasks must be performed to meet these requirements? (Choose three.)

- A. Apply the Catch-AII profile to the ASinbound profile and configure an access delivery rule to deliver to the 100.64.0.72 host.
- B. Apply the Catch-Ail profile to the CFInbound profile and configure a content action profile to deliver to the srv. thirdparty. com FQDN
- C. Create an IP policy with a Source value of 100. 64 .0.72/32, enable precedence, and place the policy at the top of the list.
- D. Change the scan order in FML-GW to antispam-sandbox-content.
- E. Create an access receive rule with a Sender value of srv. thirdparcy.com, Recipient value of *@acme. com, and action value of Safe

정답： B,C,D

설명:
* A is correct because the scan order must be changed to antispam-sandbox-content in order for FortiMail to scan the email for spam and viruses before forwarding it to the third-party service.
* B is correct because the Catch-All profile must be applied to the CFInbound profile in order for FortiMail to forward clean emails to the third-party service.
* E is correct because an IP policy must be created with a Source value of 100.64.0.72/32 in order to allow emails from the third-party service to be delivered to FortiMail.
The other options are not necessary to meet the requirements. Option C is not necessary because the access receive rule will already allow emails from the third-party service to be received by FortiMail. Option D is not necessary because the Catch-All profile already allows emails to be delivered to any destination.
Here are some additional details about integrating a third-party service into the FortiMail email processing path:
* The third-party service must be able to receive emails from FortiMail and send them back to FortiMail.
* The third-party service must be able to communicate with FortiMail using the SMTP protocol.
* The third-party service must be able to authenticate with FortiMail using the SMTP AUTH protocol.
Once the third-party service is integrated into the FortiMail email processing path, all inbound emails will be processed by FortiMail as usual. If the email is clean, FortiMail will forward it to the third-party service. The third-party service will then send the email back to FortiMail for final delivery. FortiMail will not scan the email again.

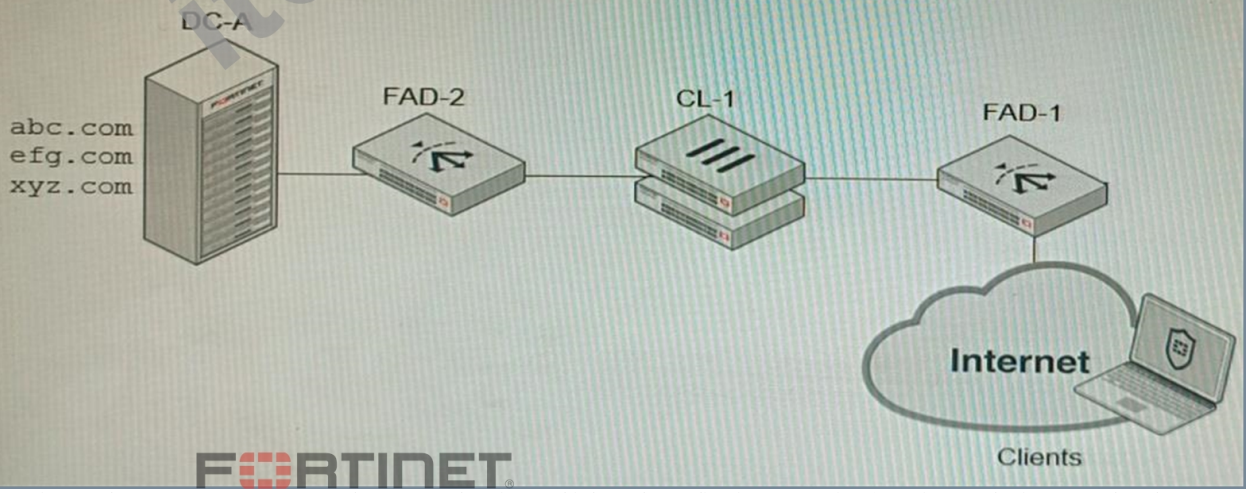
질문 # 79
Refer to the exhibits.

Configuration

```
config firewall profile-protocol-options
    edit "SSL-Offload"
        set comment "For FAD decrypted traffic"
        config http
            set ports 80
            unset options
            unset post-lang
        end
        config ftp
            set ports 21
            set options splice
        end
        config imap
            set ports 143
            set options fragmail
        end
        ...output omitted...
    next
end

config application list
    edit "SSL-Offload-App-Detect"
        set comment "App detect in decrypted traffic"
        config entries
            edit 1
                set action pass
            next
        end
    next
end
```

Topology



A FortiGate cluster (CL-1) protects a data center hosting multiple web applications. A pair of FortiADC devices are already configured for SSL decryption (FAD-1), and re-encryption (FAD-2). CL-1 must accept unencrypted traffic from FAD-1, perform application detection on the plain-text traffic, and forward the inspected traffic to FAD-2.

The SSL-Offload-App-Detect application list and SSL-Offload protocol options profile are applied to the firewall policy handling the web application traffic on CL-1.

Given this scenario, which two configuration tasks must the administrator perform on CL-1? (Choose two.)

A.
```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set ssl-offloaded yes
        end
    next
end
```

B.
```
config firewall profile-protocol-options
    edit SSL-Offload
        config http
            set options splice
        end
    next
end
```

C.
```
config firewall ssl-server
    edit FAD-1
        set ip <FAD-1 IP address>
        set ssl-mode full
    next
end
```

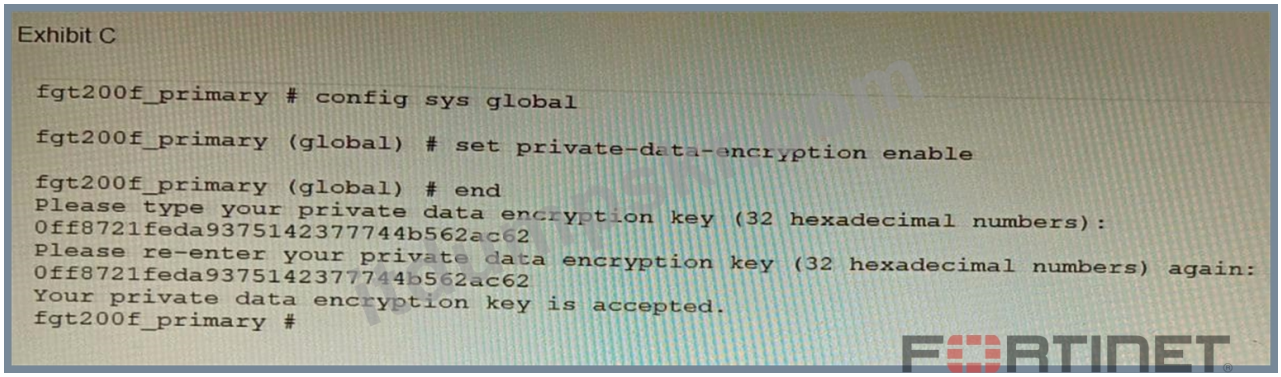
D.
```
config application list
    edit SSL-Offload-App-Detect
        set force-inclusion-ssl-di-sigs enable
    next
end
```

E.
```
config application list
    edit SSL-Offload-App-Detect
        set deep-app-inspection enable
    next
```


- A. Option C
- B. Option B
- C. Option A
- D. Option D

정답：C,D

질문 # 80
Refer to the exhibit.



A customer has deployed a FortiGate 200F high-availability (HA) cluster that contains & TPM chip. The exhibit shows output from the FortiGate CLI session where the administrator enabled TPM.
Following these actions, the administrator immediately notices that both FortiGate high availability (HA) status and FortiManager status for the FortiGate are negatively impacted.
What are the two reasons for this behavior? (Choose two.)

- A. The private-data-encryption key entered on the primary did not match the value that the TPM expected.

- B. TPM functionality is not yet compatible with FortiGate HA.
- C. The FortiGate has not finished the auto-update process to synchronize the new configuration to FortiManager yet.
- D. Configuration for TPM is not synchronized between FortiGate HA cluster members.
- E. The administrator needs to manually enter the hex private data encryption key in FortiManager.

정답：D,E

설명：
https://docs.fortinet.com/document/fortimanager/7.4.2/administration-guide/30332/verifying-devices-with- private-data-encryption-enabled

질문 # 81
You are migrating the branches of a customer to FortiGate devices. They require independent routing tables on the LAN side of the network.
After reviewing the design, you notice the firewall will have many BGP sessions as you have two data centers (DC) and two ISPs per DC while each branch is using at least 10 internal segments.
Based on this scenario, what would you suggest as the more efficient solution, considering that in the future the number of internal segments, DCs or internet links per DC will increase?

- A. Redesign the SD-WAN deployment to only use a single VPN tunnel and segment traffic using VRFs on BGP
- B. Acquire a FortiGate model with more capacity, considering the next 5 years growth.
- C. No change in design is needed as even small FortiGate devices have a large memory capacity.
- D. Implement network-id, neighbor-group and increase the advertisement-interval

정답：A

설명：
https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/810981/sd-wan-segmentation-over-a- single-overlay

질문 # 82
.....

출문제

- 높은 통과율 NSE8_812최고품질 시험덤프자료 공부문제 □ ☀ www.koreadumps.com □☀□웹사이트를 열고 【 NSE8_812 】를 검색하여 무료 다운로드NSE8_812인증덤프공부문제
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, lms.ait.edu.za, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.dssmymdiv.com, csbskillcenter.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, aula.totifernandez.com, Disposable vapes

BONUS!!! ITDumpsKR NSE8_812 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=1gZnoj4t1gCiQcX2JPNHNb7QVLDysxJFi