Incident Report

Ticket ID	IT/2404/0166
Customer Name	Sigma Cipta Utama
Request	Perangkat VPN PHR Bermasalah
Engineer	Richard & Taufiq
PIC Customer	Ahmad Faris
Technology	Network Security

Incident Description

Pada tanggal 29 April 2024 terdapat laporan dari user bahwa VPN akses untuk jaringan PHR tidak dapat digunakan.

Incident Fulfillment

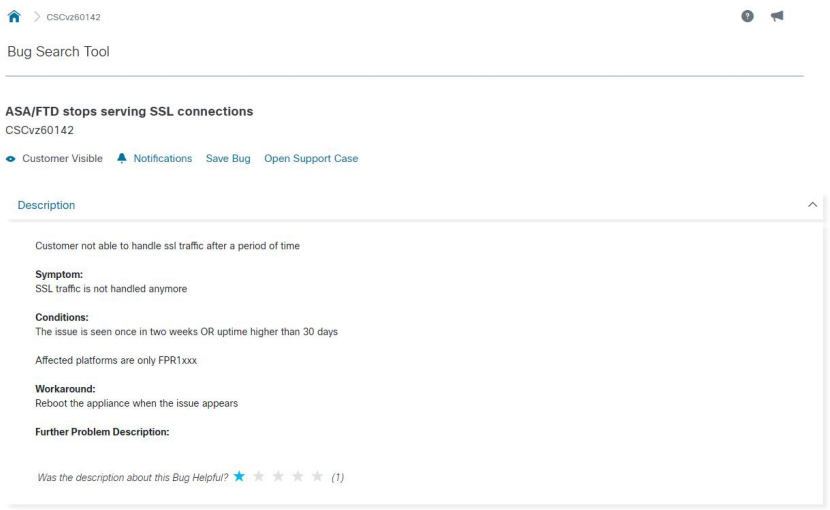
1. Dilakukan pengecekan pada ASA VPN yang bermalasah dengan mengecek jumlah session VPN yang sedang berjalan.
2. Jumlah session yang aktif terbilang rendah.

```
ASAVPN01-PHR/pri/act# show vpn-sessiondb summary
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                                  Active : Cumulative : Peak Concur : Inactive
                                 ------------------------------------------------
AnyConnect Client                :     33 :         45 :          44 :        7
  SSL/TLS/DTLS                   :     33 :         45 :          44 :        7
----------------------------------------------------------------------------
Total Active and Inactive    :     40             Total Cumulative :     45
Device Total VPN Capacity    :    800
Device Load                  :     5%
----------------------------------------------------------------------------
```

3. Dilakukan swing traffic atau failover dari ASA VPN 1 ke ASA VPN 2.
4. Traffic Sudah berjalan normal kembali setelah di swing ke ASA VPN 2.
5. Dilakukan pengecekan lebih lanjut dengan mengambil output show tech support pada ASA VPN 1.

```
ASAVPN01-PHR/pri/act# Terminal Pager 0
ASAVPN01-PHR/pri/act# show tech

Cisco Adaptive Security Appliance Software Version 9.14(2)15
SSP Operating System Version 2.8(1.148)
Device Manager Version 7.14(1)

Compiled on Fri 16-Apr-21 04:55 GMT by builders
System image file is "disk0:/installables/switch/fxos-k8-fp1k-lfbff.2.8.1.148.SPA"
Config file at boot was "startup-config"

ASAVPN01-PHR up 61 days 4 hours
failover cluster up 2 years 206 days

Hardware:   FPR-1150, 28251 MB RAM, CPU Atom C3000 series 2000 MHz, 1 CPU (16 cores)

Encryption hardware device : Cisco FP Crypto on-board accelerator (revision 0x11)
                             Driver version        : 4.1.0
                             Number of accelerators: 6

 1: Int: Internal-Data0/0    : address is 00a0.c900.0002, irq 10
 3: Int: Not licensed        : irq 0
 4: Ext: Management1/1       : address is 74ad.9842.9c81, irq 0
 5: Int: Internal-Data1/1    : address is 0000.0100.0001, irq 0

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 2
Carrier                           : Disabled
AnyConnect Premium Peers          : 800
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 800
Total VPN Peers                   : 800
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
```

6. Beberapa hari setelah di cek, ASA VPN 1 terkena bug version oleh karena itu perlu dilakukan upgrade software menuju golden version yang direkomendasikan oleh Cisco.



7. Pada tanggal 03 Mei 2024, ASA VPN 1 dan ASA VPN 2 dilakukan upgrade secara bergantian.

```
ASAVPN01-PHR/pri/act# show version | in Ver
Cisco Adaptive Security Appliance Software Version 9.18(4)24
SSP Operating System Version 2.12(1.74)
Device Manager Version 7.20(2)
```

```
ASAVPN01-PHR/sec/stby# Show version | in Ver
Cisco Adaptive Security Appliance Software Version 9.18(4)24
SSP Operating System Version 2.12(1.74)
Device Manager Version 7.20(2)
```

8. Setelah di upgrade software version, dilakukan monitoring selama beberapa hari.
9. Setelah satu minggu termonitor, software version yang telah diupgrade cukup stabil untuk network PHR.

Last Status

Akses VPN sudah dapat digunakan kembali.

```
ASAVPN01-PHR/pri/act# show vpn-sessiondb
--------------------------------------------------------------------------
VPN Session Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concur : Inactive
                           ----------------------------------------------
AnyConnect Client           :     98 :       3770 :         198 :        8
  SSL/TLS/DTLS              :     98 :       3770 :         198 :        8
--------------------------------------------------------------------------
Total Active and Inactive   :    106            Total Cumulative :   3770
Device Total VPN Capacity   :    800
Device Load                 :    13%
--------------------------------------------------------------------------


--------------------------------------------------------------------------
Tunnels Summary
--------------------------------------------------------------------------
                            Active : Cumulative : Peak Concurrent
                           ----------------------------------------------
AnyConnect-Parent           :    106 :       3770 :             198
SSL-Tunnel                  :     93 :      21875 :             179
--------------------------------------------------------------------------
Totals                      :    199 :      25645
--------------------------------------------------------------------------
```

Recommended Action