How: Sesje

12 listopada 2020
10:08

azagrobelny@PFI-000B01(active-primary)> **show system statistics session**
System Statistics: ('q' to quit, 'h' for help)

Device is up : 1 day 10 hours 2 mins 8 sec
Packet rate : 210136/s
Throughput : 897290 Kbps
Total active sessions : 263963
Active TCP sessions : 195865
Active UDP sessions : 56704
Active ICMP sessions : 886

azagrobelny@PFI-000B01(active-primary)> **show counter global**

azagrobelny@PFI-000B01(active-primary)> **show session all filter source 10.1.16.100 destination 193.111.166.206**

ID Application State Type Flag Src[Sport]/Zone/Proto (translated IP[Port])
Vsys Dst[Dport]/Zone (translated IP[Port])

605974 SSL-Tabletbanking ACTIVE FLOW 10.1.16.100[17691]/DMZI-INSIDE/6 (10.1.16.100[17691])
vsys1 193.111.166.206[9615]/DMZI-OUTSIDE (193.111.166.206[9615])

azagrobelny@PFI-000B01(active-primary)> **show session id 605974**

Session 605974
c2s flow:
source: 10.1.16.100 [DMZI-INSIDE]
dst: 193.111.166.206
proto: 6
sport: 34194 dport: 9600
state: INIT type: FLOW
src user: unknown
dst user: unknown

s2c flow:
source: 193.111.166.206 [DMZI-OUTSIDE]
dst: 10.1.16.100
proto: 6
sport: 9600 dport: 34194
state: INIT type: FLOW
src user: unknown
dst user: unknown
qos node: ethernet1/13.10, qos member N/A Qid 0
ecmp id: 8000

Slot : 1
DP : 0
index(local): : 605974
start time : Tue Nov 10 14:23:13 2020
timeout : 15 sec
total byte count(c2s) : 805
...

How: PFI Check

12 listopada 2020
11:24

Polkomtel-topup
(addr in 10.1.16.100) and (addr.dst in 212.2.96.132) and ((port.dst eq 8080) or (port.dst eq
(port.dst eq 4343))

APN-Tmobile -> Connex
(addr.src in 172.22.128.0/18) and (addr.dst in 10.143.216.84)

APN-Polkomtel -> Connex
((addr.src in 7.8.0.0/18) or (addr.src in 7.8.64.0/18)) and (addr.dst in 10.143.216.84)

APN-Orange -> Connex
(addr.src in 7.7.0.0/18) and (addr.dst in 10.143.216.84)

Biedronka -> Connex
(addr.src in 10.0.5.57) and (addr.dst in 10.143.216.84)

Blik
(addr.src in 172.31.2.30) and (addr.dst in 200.0.110.45/32)

Blumedia
(addr.dst in 195.182.23.220)

Tesco
(addr in 10.92.0.0/15) or (addr.src in 10.93.99.74) or (addr.src in 10.88.0.0/14) or (addr.src in 10.92.0.0/15) and (addr.src in 106.0.0.0/8)

Westernunion
(rule eq OUT_WESTERNUNION)

SWIFT
(addr in 200.0.110.250) or (addr in 200.0.110.49) and (addr.src in 200.0.110.188)

Bondspot
(rule eq OUT_BONDSPOT-app)

KDPW
(addr.src in 195.136.21.0/26)

PZU -> Unisales
(addr.src in 10.6.27.250) and (port.dst eq 443) and (addr.dst in 10.249.4.134)

PZU -> ADFS
(addr.src in 10.6.27.250) and (addr.dst in 10.143.133.128) and (port.dst eq 443)

ProxyX
(addr.dst in 172.20.17.210) and (port.dst eq 8080)

ProxyV

(addr.dst in 10.143.139.76) and (port.dst eq 80)

PR-VPN
(addr.src in 172.24.32.0/20) or (addr.src in 172.24.0.0/20)

FZ-VPN
(addr.src in 172.20.14.0/24) or (addr.src in 172.24.48.0/20)

How: Offloaded trafic

13 listopada 2020
09:01

Which Traffic Can Be Offloaded?

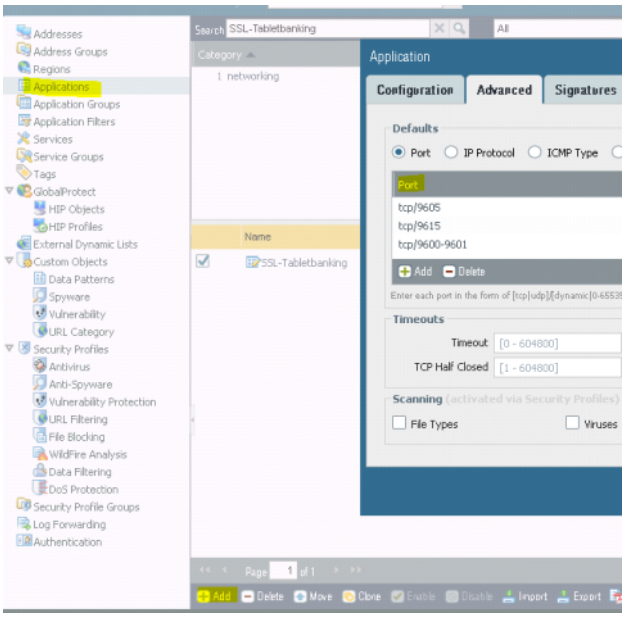
Commonly offloaded packets includes:

- SSL and SSH sessions that are not subject to decryption
- Sessions to which an Application Override rule is applied with a custom application
- Dynamic routing protocols such as OSPF, BGP, or RIP
- Sessions based on protocols for which no known exploits exist, such that additional inspection is not applicable

This traffic *never* will be offloaded:

- Security-Profile matched
- Web browsing
- Decrypted SSL
- Firewall-bound sessions
- VPN sessions
- IPsec
- Inter-vsys sessions
- PBF, if no next hop
- Non-TCP/UDP (including ping)
- ARP (all non-IP traffic)
- NAT64
- TCP SYN, FIN, and RST

Tworzenie custom application



19 listopada 2021
14:47

admin@PFI-000A01(active-primary)> **show system state filter-pretty sys.s1.p9.phy**

```
sys.s1.p9.phy: {
  link-partner: { },
  media: SFP-CAT5,
  sfp: {
    connector: Reserved,
    encoding: 8B10B,
    identifier: SFP,
    transceiver: 1000B-T,
    vendor-name: FINISAR CORP.   ,
    vendor-part-number: FCLF8522P2BTL   ,
    vendor-part-rev: A   ,
  },
  type: Ethernet,
}
```

azagrobelny@PFI-000A01(active-secondary)> **show system state filter-pretty ha.net.s0.hsci.hwcfg**

```
ha.net.s0.hsci.hwcfg: {
  farloop: False,
  link: Down,
  mode: PowerDown,
  mru: 10048,
  nearloop: False,
  pause-frames: True,
  setting: 100Gb/s-full,
  type: QSFP28,
}
```

azagrobelny@PFI-000A01(active-secondary)> **show system state filter-pretty ha.net.s0.hsci.stats**

```
ha.net.s0.hsci.stats: {
  rx-broadcast: 0,
  rx-bytes: 0,
  rx-multicast: 0,
  rx-unicast: 0,
  tx-broadcast: 0,
  tx-bytes: 0,
  tx-multicast: 0,
  tx-unicast: 0,
}
```

How: C2L

12 listopada 2020
12:35

PVO-000P02/sec/actNoFailover# **show ip local pool POOL-VPN-PR-Devel**

Begin	End	Mask	Free	Held	In use
172.20.8.161	172.20.8.190	255.255.255.224	30	0	0

Available Addresses:
172.20.8.161
172.20.8.162
172.20.8.163
172.20.8.164
172.20.8.165
…

ASA: *vpn-idle-timeout*

18 listopada 2022
11:52

vpn-idle-timeout 30 = the amount of time the vpn connection is idle ie. no activity seen on the tunnel, before it is disconnected
vpn-session-timeout 900 = the amount of time the VPN tunnel is allowed to stay up regardless of whether there is activity or not

Z <https://community.cisco.com/t5/network-security/what-is-the-difference-between-vpn-idle-timeout-and-vpn-session/td-p/1095487>

ASA: The default value of 'vpn idle timeout' is set to 30 minutes.
If the idle timeout is set to 30 minutes (default), it means that it drops the tunnel after 30 minutes of traffic passes through it. The VPN client gets disconnected after 30 minutes regardless of the setting idle timeout and encounters the PEER_DELETE-IKE_DELETE_UNSPECIFIED error.

Z <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/81824-common-ipsec-trouble.html#solution13>

How: Wykresy portów

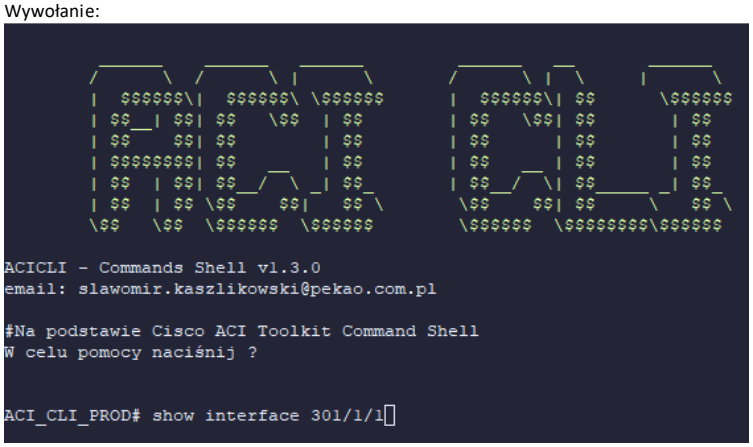
17 listopada 2020
12:17

Cześć,

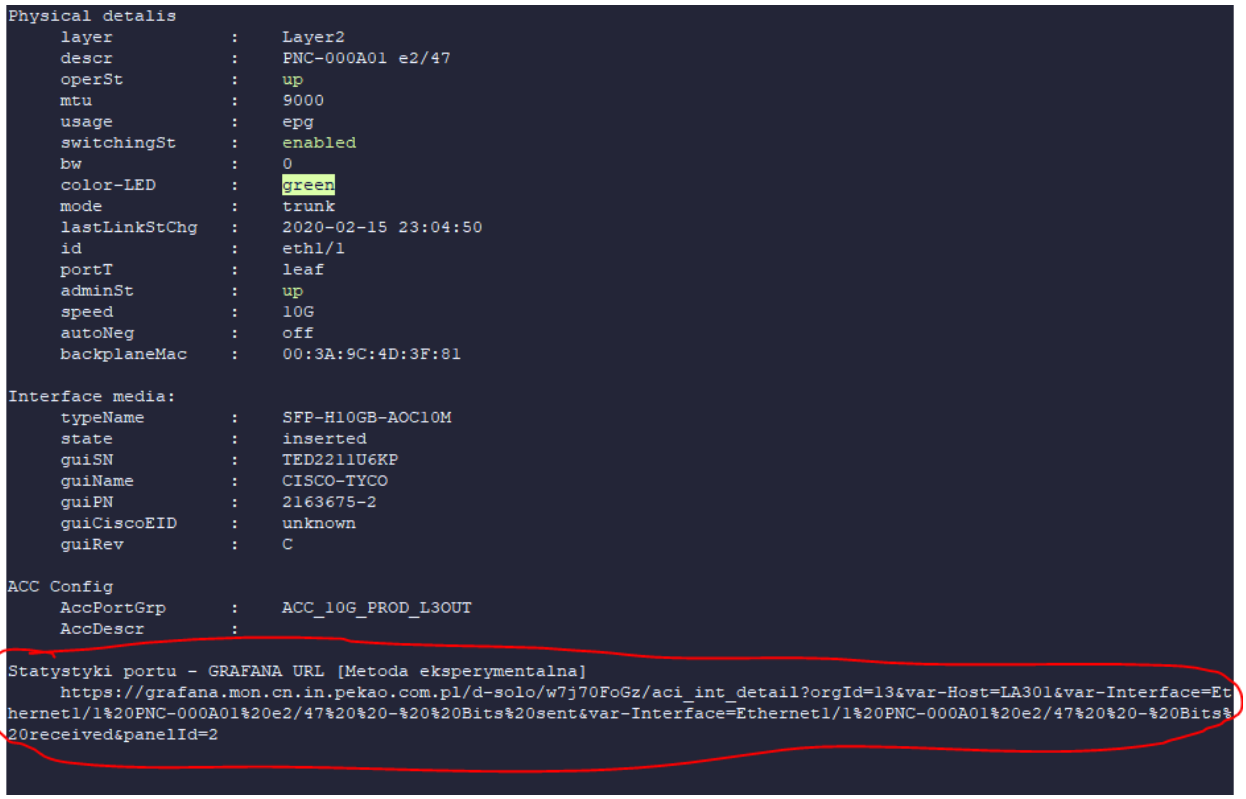
Dla korzystających bądź chcących skorzystać, dorzuciłem eksperymentalną metodę (więc może mieć problemy) generowania URL dla wykresy statystyk portu. Dodatkowo zmieniłem metodę zapytań zamiast
show interface eth 301/1/1 na show interface 301/1/1

Ważne info dla kolegów z T-SEC, dzisiaj wyślę do was zaproszenia z grafany, należy kliknąć link, przez formularz. Dopiero po tym kroku będę mógł was dodać do grafany. W razie problemów z prośba o kontakt ze mną bądź Kamilem Raczyńskim

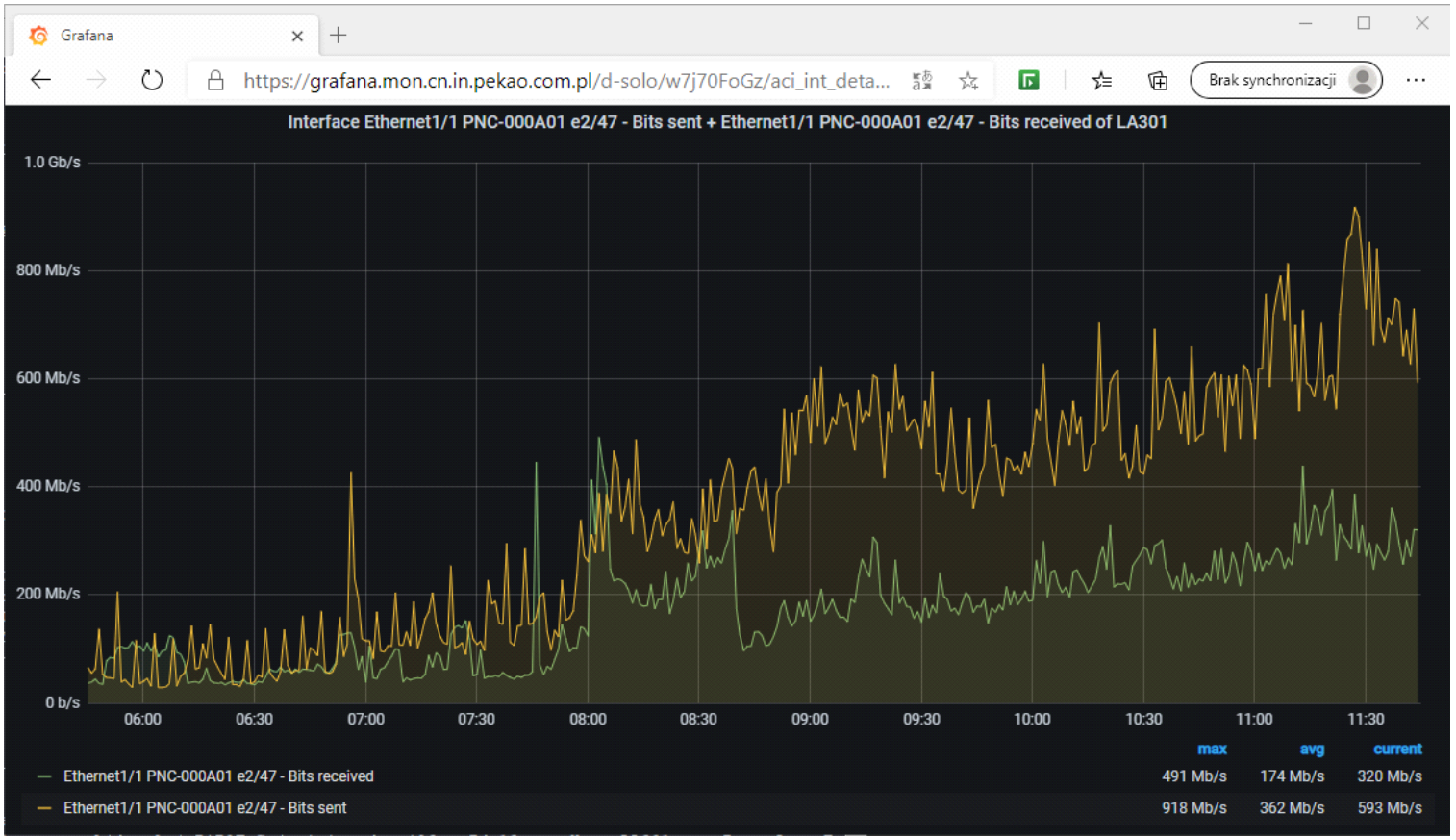
Wywołanie:



Wynik:



Skopiować wygenerowany URL i wkleić w okno przeglądarki:



Na dzień dzisiejszy opcja działa dla leafów:

- LA301
- LA302
- LA303
- LA304
- LP109
- LP110

Kolejne będą sukcesywnie dodawane.

Show interface

23 marca 2022
15:18

APIC1-BDC# fabric 193 show interface eth1/5

How: Manual Shutdown node

16 grudnia 2020
19:02

The correct way to shut down an ISE node CLI is:
1. Application stop ise
2. Halt

<https://community.cisco.com/t5/network-access-control/shutdown-ise/td-p/3396126>

How: Manual Failover PAN

17 grudnia 2020
09:04

What to do next

After the promotion of Secondary PAN to the Primary PAN, do the following:

- Manually sync the old Primary PAN to bring it back into the deployment.
- Manually sync any other secondary node that is out-of sync, to bring it back into the deployment.

Manually Promote Secondary PAN To Primary

If the Primary PAN fails and you have not configured PAN auto-failover, you must manually the Secondary PAN to become the new Primary PAN.

Before you begin

Ensure that you have a second Cisco ISE node configured with the Administration persona to promote as your Primary PAN.

Procedure

Step 1 Log in to the user interface of the Secondary PAN.

Step 2 Choose Administration > System > Deployment.

Step 3 In the Edit Node page, click Promote to Primary.
You can only promote a Secondary PAN to become the Primary PAN. Cisco ISE nodes assume only the Policy Service or Monitoring persona, or both, cannot be promoted to become the Primary PAN.

Step 4 Click Save.

Z <https://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20/b_ise_admin_guide_20_chapter_010.html#ID590>

HOW: FTP copy

2 grudnia 2021
10:45

COPY FROM FTP TO ISE

isepan2001/admin# copy ftp://10.143.135.33/ISE/ISEnew/ise-urtbundle-3.0.0.458-1.0.0.SPA.x86_64.tar.gz disk:/
Username: uploadisenew
Password:

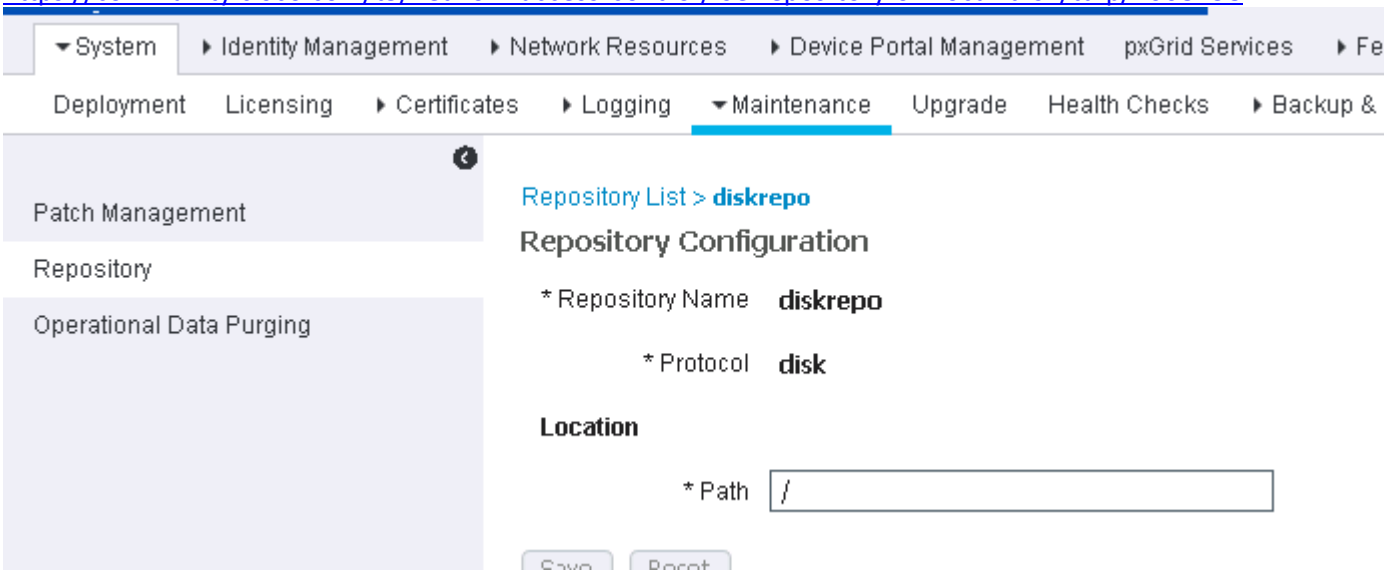
COPY FROM ISE TO FTP

isepsn1002/admin# copy disk:/tech_isepsn1002_17-11-2021-12-20.tar.gz ftp://10.143.135.33/ISE
Username: uploadisenew
Password:

HOW: URT check

2 grudnia 2021
11:32

Krok1: Stworzenie repozytorium lokalne
https://community.cisco.com/t5/network-access-control/ise-repository-on-local-disk/td-p/4068458



Krok2: Skopiowanie pliku do ISE na disk:/

Krok3: instalacja ISE
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215528-upgrade-identity-services-engine-ise.html

isepan2001/admin# application install ise-urtbundle-3.0.0.458-1.0.0.SPA.x86_64.tar.gz diskrepo
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Generating configuration...
Saved the ADE-OS running configuration to startup successfully

Getting bundle to local machine...
Unbundling Application Package...
Verifying Application Signature...

Uinstall URT:
isepan2001/admin#
isepan2001/admin# application remove urt

HOW: Trabelshoot ISE

22 grudnia 2021
18:22

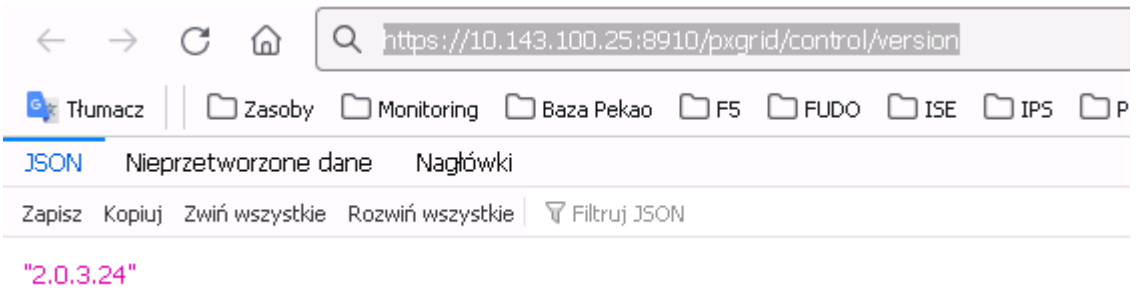
isemnt2001/admin# **application configure ise**

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[26]Recreate undotablespace
[27]Configure TCP params
[28]Fetch SGA/PGA Memory usage
[0]Exit

HOW: Pxgrid check version

22 grudnia 2021
20:12

https://10.143.100.25:8910/pxgrid/control/version



Configure Local Repository

12 kwietnia 2023
12:55

CLI

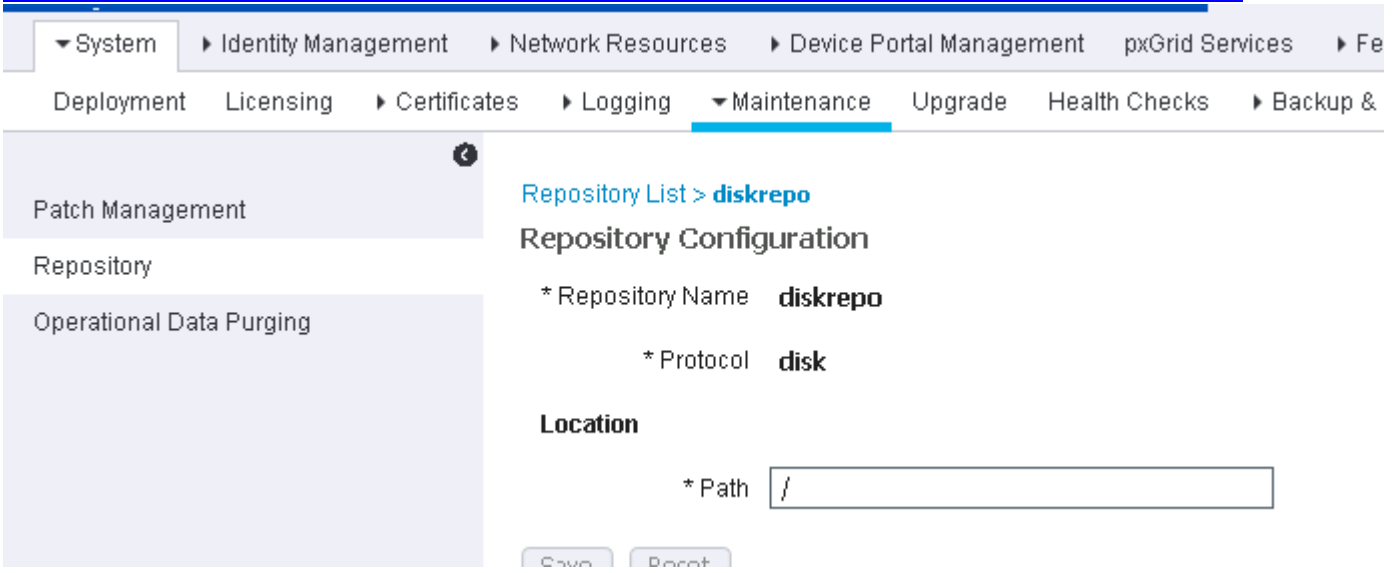
Log in to the CLI of the ISE node via SSH and run these commands:

```
ise/admin#
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# repository Local-Repo
ise/admin(config-Repository)# url disk:/
ise/admin(config-Repository)# exit
ise/admin(config)# exit
ise/admin#
```

Z <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/215348-how-to-configure-repository-on-identity.html#anc17>

GUI

https://community.cisco.com/t5/network-access-control/ise-repository-on-local-disk/td-p/4068458



Rollback

13 kwietnia 2023
13:01

Roll Back to the Previous Version

In rare cases, you might have to reimage the Cisco ISE-PIC appliance by using the previous version of ISO image and restoring the data from the backup file. After restoring the data, you can register with the deployment. Hence, we recommend that you back up the Cisco ISE-PIC configuration data before you start the upgrade process.
Sometimes, upgrade failures that occur because of issues in the configuration database are not rolled back automatically. When this occurs, you get a notification stating that the database is not rolled back with an upgrade failure message. In such scenarios, you should manually reimage your system, install Cisco ISE, and restore the configuration data.
Before you attempt to rollback or recovery, generate a support bundle by using the backup-logs command, and place the support bundle in a remote repository.

Z <https://www.cisco.com/c/en/us/td/docs/security/ise/3-1/upgrade_guide/HTML/b_upgrade_method_3_1.html>

DNA interation check

13 kwietnia 2023
14:06

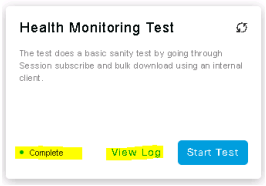
ISE site

1. Adminisraion - > pxGrid Service -> Client Managment -> Summary
2. Adminisraion - > pxGrid Service -> Client Managment -> Clients
https://10.143.100.11/admin/#administration/administration_messageservice/pxgrid_clientmanagement/pxgrid_clientmanagement_cli ents

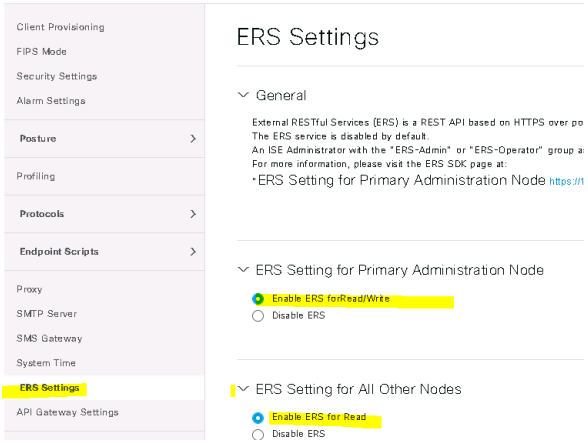
Name	Description	Client Groups	Status
ise-bridge-isepxg1001			Deleted
pxgrid_client_1613835436_dnac...			Enabled
livenx			Enabled
ise-mnt-isepan2001			Enabled
pxgrid_client_1613835436	Cisco DNA Center ise-bridge servi...		Enabled

3. Adminisraion - > pxGrid Service -> Diagnostics -> Tests

Tests



4. ERS enable
Adminisraion - >System -> Settings
https://10.143.100.11/admin/#administration/administration_system/administration_system_settings/ers_Settings



DNA Site

DEEPER INTO DNA'S IDENTITY SERVICE

The process of DNA connecting to ISE ERS API are in a docker container on DNA called *identity-manager-pxgrid-service*. Here's how to kick start DNA and tail some logs of what's going on. Let's restart it, and tail it's logs to follow as it makes ERS queries, and tries to connect to PXGrid.

```
$ magctl service restart identity-manager-pxgrid-service
```

Now, let's tail the logs as it restarts

```
$ magctl service logs -rf identity-manager-pxgrid-service
```

After about 10 minutes... wait for it... it will start downloading from the ERS API and connecting to PXGrid. Here's where it's connecting to ERS, this is your policy data download.

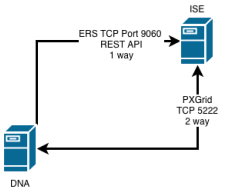
```
2018-12-04 17:30:07,346 |   INFO | Thread-58                | identity-manager-px
2018-12-04 17:30:07,690 |   INFO | Thread-58                | identity-manager-px
```

You might see something like this - It's downloading the ISE Policy SGT Matrix to sync with the DNA Policy module.

```
INFO | SimpleAsyncTaskExecutor-2 | identity-manager-pxgrid-service | c.c.e.i.p.i.u
```

DNAC TO ISE DIAGRAM.

ERS gets the policies and updates them as needed when you make policy changes on DNA. PXGrid is the push, it pushes changes to DNAC related to SGTs. Making policy changes in ISE will not push to DNAC.



module.

```
INFO | SimpleAsyncTaskExecutor-2 | identity-manager-pxgrid-service | c.c.e.i.p.i.u
```

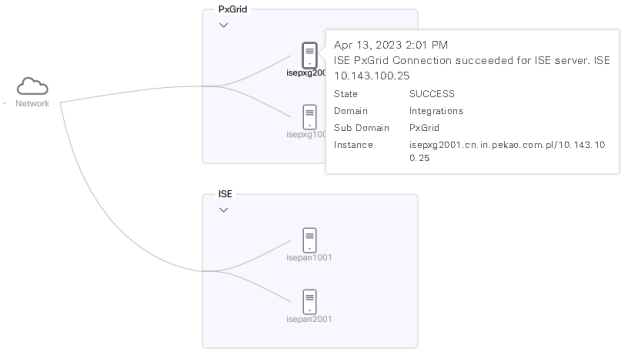
Or PXGrid trying to connect and getting refused.

```
2018-12-18 21:04:22,218 |   INFO | Thread-89                | identity-manager-px
2018-12-18 21:05:22,218 |   INFO | Thread-89                | identity-manager-px
2018-12-18 21:05:22,218 |   INFO | Thread-89                | identity-manager-px
2018-12-18 21:05:22,231 |   INFO | Thread-89                | identity-manager-px
```

These can give you the right direction to continue troubleshooting in, or may resolve your issue.

DNA Site

System -> Settings -> System Health
https://10.143.100.202/dna/systemSettings/systemHealth



Basic

7 lutego 2021
17:39

ASN

Number	Bits	Description
0	16	Reserved for RPKI unallocated space invalidation[11]
1 - 23455	16	Public ASNs
23456	16	Reserved for AS Pool Transition
23457 - 64495	16	Public ASNs
64496 - 64511	16	Reserved for use in documentation/sample code
64512 - 65534	16	Reserved for private use
65535	16	Reserved
65536 - 65551	32	Reserved for use in documentation and sample code
65552 - 131071	32	Reserved
131072 - 4199999999	32	Public 32-bit ASNs
4200000000 - 4294967294	32	Reserved for private use
4294967295	32	Reserved

PORT

TCP-179

Route Selection Process

7 lutego 2021
18:18

Cisco BGP Route Selection Process

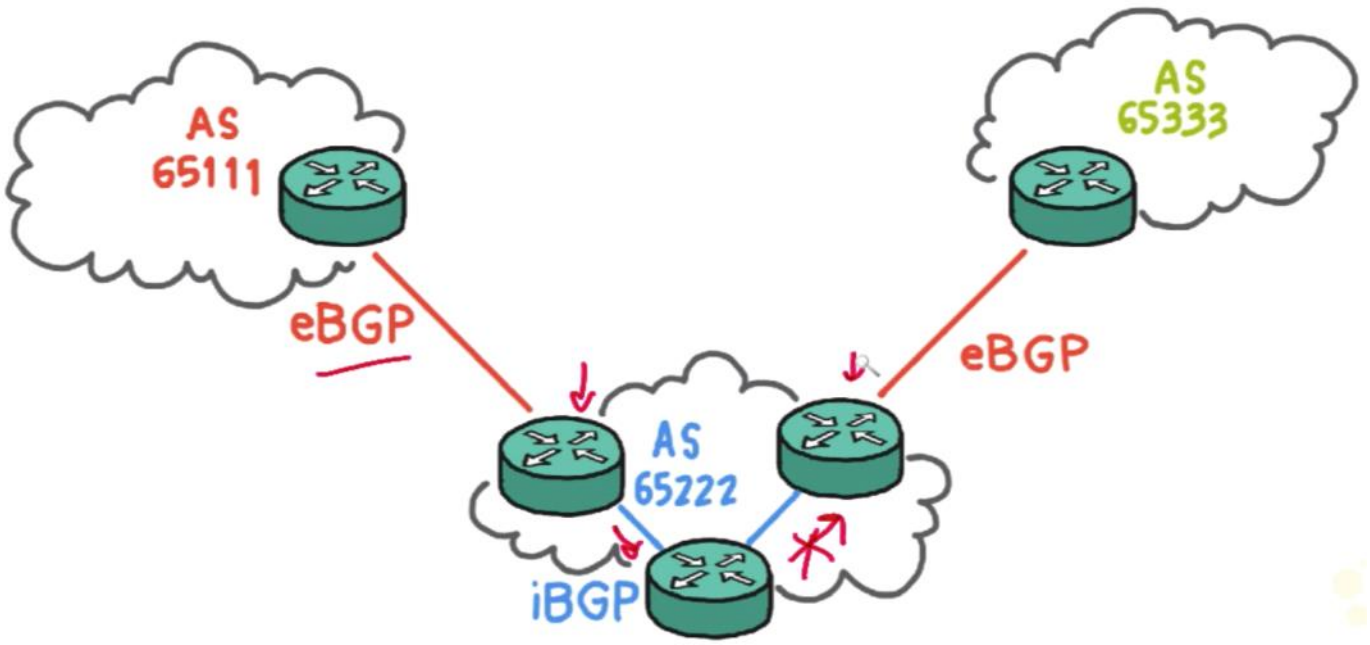
- Step 1: Prefer highest weight (local to router)
- Step 2: Prefer highest local preference (global within AS)
- Step 3: Prefer route originated by the local router
- Step 4: Prefer shortest AS path
- Step 5: Prefer lowest origin code (IGP < EGP < incomplete)
- Step 6: Prefer lowest MED (from other AS)
- Step 7: Prefer EBGP path over IBGP path
- Step 8: Prefer the path through the closest IGP neighbor
- Step 9: Prefer oldest route for EBGP paths
- Step 10: Prefer the path with the lowest neighbor BGP router ID

iBGP

14 marca 2021
17:45

iBGP Split Horizon

- Domyślnie gdy ruter otrzyma prefix z sesji eBGP to w ramach sesji iBGP reklamuje go tylko do swojego pierwszwgo sąsiada
- Rozwiązaniem może być np.. Route reflection



Troubleshooting

18 marca 2021
20:57

Weryfikacja sąsiectwa
R2#show ip bgp summary

Weryfikacja prefixów:

HOW: TCPdump

19 lutego 2021
10:21

azagrobelny@(bdlb1113)(cfg-sync Standalone)(Active)(/Common)(tmos)# **tcpdump -A -s0 -vv -i VLAN270 host 10.10.0.20**
azagrobelny@(bdlb1113)(cfg-sync Standalone)(Active)(/Common)(tmos)# **tcpdump -A -s0 -vv -i VLAN270 src host 10.151.136.60 and dst host 10.143.217.116 and dst port 4000**

Przełączniki

-n	To disable name resolution, use the **-**n flag as in the following examples: tcpdump -n
-**r**	Reading tcpdump binary file output
-w	Zapis snifowanego ruchu do pliku binarnego
-i	Wskazanie interfajsu,vlany na któym ma być snifowany ruch. Domyślnie bez tego linux nasłuchuje na pierwszym interfejsie jaki znajdzie.
-l	Wyłączenie standardowego buforowania na wyjściu na konsole. Oznacza to, że od razu wyrzuci na wyjście snifowany ruch
-**v** **-vv** **-vvv**	Służą do coraz dokładniejszego analizowania zawartości pakietu
-t	*Don't* print a timestamp on each dump line.
-tt	Print the timestamp, as seconds since January 1, 1970, 00:00:00, UTC, and fractions of second since that time, on each dump line.
-ttt	Print a delta (microsecond or nanosecond resolution depending on the **--time-stamp-precision** option) between current and previous line on each dump line. The default is microsecond resolution.
-A	Print each packet (minus its link level header) in ASCII. Handy for capturing web pages
-c	Exit after receiving *count* packets.
-0 n	Nie powoduje zamiany oid na MIB. Wyświetla pełne ciągi

Składnie:

\ and tcp\[tcpflags\]\=tcp- \ and tcp\[tcpflags\]\=tcp-	Snifowanie tylko pakitów z flagą SYN lub

Saving tcpdump output to a file

Binary file:
tcpdump > dump1.txt

Text file
tcpdump -w dump1.bin

Reading tcpdump binary file output
tcpdump -r <filename>

Filtering on a host address

- To view all packets that are traveling to or from a specific IP address, type the following **tcpdump host 10.90.100.1**
- To view all packets that are traveling from a specific IP address, type the following command: **tcpdump src host 10.90.100.**1
- To view all packets that are traveling to a particular IP address, type the following command: **tcpdump dst host 10.90.100.1**

Filtering on a port

- To view all packets that are traveling through the BIG-IP system and are either sourced from or destined to a specific port, type the following command: **tcpdump port 80**
- To view all packets that are traveling through the BIG-IP system and sourced from a specific type the following command: **tcpdump src port 80**
- To view all packets that are traveling through the BIG-IP system and destined to a specific port, type the following command: **tcpdump dst port 80**

History delete line

12 kwietnia 2023
12:59

history -d 1234

Z <https://unix.stackexchange.com/questions/49214/how-to-remove-a-single-line-from-history>

How: Clear IPsec

8 września 2021
14:06

If **peer**, **map**, **entry**, or **counters** keywords are not used, all IPSec security associations will be deleted.
•The **peer** keyword deletes any IPSec security associations for the specified peer.
•The **map** keyword deletes any IPSec security associations for the named crypto map set.
•The **entry** keyword deletes the IPSec security association with the specified address, protocol, and SPI.

#show crypto ipsec sa peer 193.26.25.30
local crypto endpt.: 193.111.166.10/500, remote crypto endpt.: 193.26.25.30/500
path mtu 1500, ipsec overhead 78(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: **DC36A41C**
current inbound spi : **128AB362**

clear crypto ipsec sa entry 10.244.40.12 esp DC36A41C

Z <https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/srfipsec.html>

HOW: delete persistence

16 września 2021
13:59

delete ltm persistence persist-records virtual TRANSPARENT_proxyx.cn.in.pekao.com.pl-80

HOW: LTM connection

16 września 2021
13:59

show ltm traffic-matching-criteria source-address-list 172.24.1.1

show sys connection cs-client-addr 172.24.163.166 virtual-server TRANSPARENT_proxyx.cn.in.pekao.com.pl

Health Monitor: 200

30 grudnia 2021
08:14

General Properties

Name	GET-SMS-NAPS-HTTPS
Partition / Path	Common
Description	
Type	HTTPS
Parent Monitor	https

Configuration: Basic

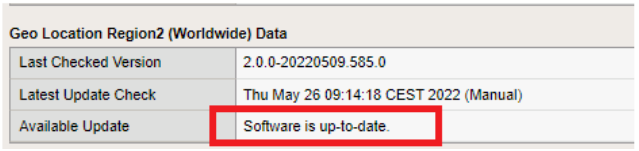
Interval	5 seconds
Timeout	16 seconds
Send String	GET / HTTP/1.1\r\nHost: sms.naps.pekao.com.pl\r\nAccept: */*\r\n
Receive String	200

Aktualizacja bazy GeoIP na F5 DMZ

19 kwietnia 2023
12:02

UWAGA, procedura nieaktualna do momentu podniesienia wersji do 15.1.8.
Aktualizacja bazy GeoIP na F5.
Należy wykonać na wszystkich F5 DMZ-owych (4 sztuki: 2x DMZ Bankowe + 2x DMZ Apiusowe). Nie konieczności wykonywania aktualizacji w okienku serwisowym, gdyż obecnie nie korzystamy z geolokacyjnej na F5. Aktualizacja nie ma wpływu na działanie systemu. Bez znaczenia kolejność wykonywania aktualizacji (active / standby).
Uwaga: W 2023 roku zmieniła się lokalizacja update'ów na stronie F5. Obecnie jest przekierowanie na https://my.f5.com/manage/s/downloads Tam wybieramy platformę i wersję. Są do wyboru dwa pliki:
GeoLocationUpdates_Edge
GeoLocationUpdates_Pulse
Wybieramy PULSE.
Plik z updatem + plik md5 ściągamy i wrzucamy do /shared/tmp i przechodzimy do punktu 3)

1) Sprawdzenie aktualności bazy GeoIP
a) z GUI:
Przejść do: System → Software Management: Update Check



Geo Location Region2 (Worldwide) Data	
Last Checked Version	2.0.0-20220509.585.0
Latest Update Check	Thu May 26 09:14:18 CEST 2022 (Manual)
Available Update	Software is up-to-date.

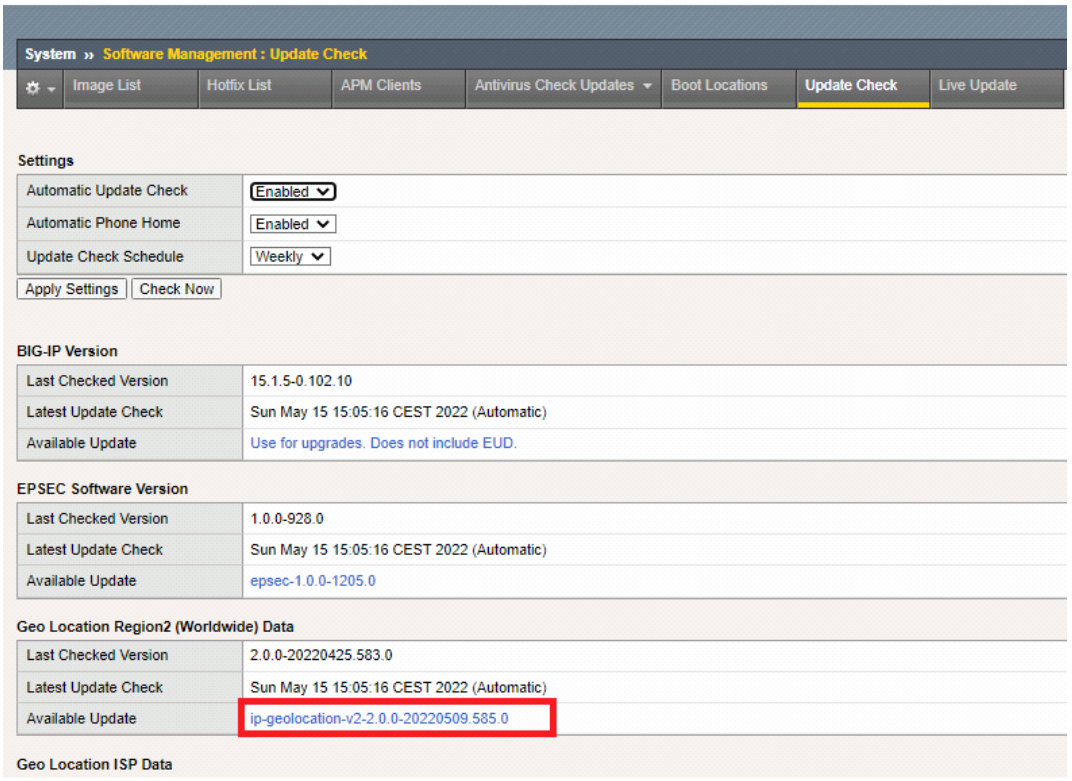
Na powyższym screenie mamy informację, że baza GeoIP jest aktualna i nie trzeba aktualizować. W przypadku nieaktualnej bazy będzie dostępny link (na screenie w punkcie 2).
Informacja z jakiego dnia mamy bieżącą bazę znajduje się w wierszu *Last Checked Version.*
Available Update - nie sugerujemy się tym. Jest tu pokazana data wersji dla EDGE (którą F5 chce niebawem porzucić).

b) z linii komend (powłoka bash):
#ls -ltr /shared/GeoIP/v2

```
[admin@pli-000a21:Active:In Sync] ~ # ls -ltr /shared/GeoIP/v2
total 232096
-rw-r--r--. 1 root root      24620311 Apr 25 17:17 F5GeoIPRegion2v2.dat
-rw-r--r--. 1 root root     207915652 Apr 25 17:17 F5GeoIPOrgv2.dat
-rw-r--r--. 1 root root       4876252 Apr 25 17:17 F5GeoIPISPv2.dat
lrwxrwxrwx. 1 root webusers        33 May 12 14:53 F5GeoIPISP.dat -> /shared/GeoIP/v2/F5GeoIPISPv2.dat
lrwxrwxrwx. 1 root webusers        33 May 12 14:54 F5GeoIPOrg.dat -> /shared/GeoIP/v2/F5GeoIPOrgv2.dat
lrwxrwxrwx. 1 root webusers        37 May 12 14:54 F5GeoIPv6.dat -> /shared/GeoIP/v2/F5GeoIPRegion2v2.dat
lrwxrwxrwx. 1 root webusers        37 May 12 14:54 F5GeoIP.dat -> /shared/GeoIP/v2/F5GeoIPRegion2v2.dat
[admin@pli-000a21:Active:In Sync] ~ #
[admin@pli-000a21:Active:In Sync] ~ #
```

Interesuje nas data zaznaczonych plików.

2) Ściągnąć ze strony f5 nową bazę. Wchodzimy bezpośrednio z naszej f5: System ›› Software Management : Update Check i klikamy na link np. z tabeli "Geo Location Region2 (Worldwide) Link w wierszu "Available Update". Zalogować się na stronie F5, ściągnąć plik ZIP + plik MD5 i na każdą f5-tkę do /shared/tmp – należy zalogować się na użytkownika z powłoką bash (np. admin).



3) Wykonać backup obecnych plików GeoIP:
#cp -R /shared/GeoIP/* /shared/GeoIP_backup/ (nadpisać pliki o ile trzeba)

4) przejść do katalogu /shared/tmp/ i sprawdzić sumę kontrolną ściągniętego pliku, powinien być status OK:
#cd /shared/tmp
#md5sum -c *.md5
ip-geolocation-v2-2.0.0-20220509.585.0.zip: OK

5) rozpakować plik ZIP:
[admin@pli-000a21:Active:In Sync] tmp # unzip ip-geolocation-v2-2.0.0-20220509.585.0.zip
Archive: ip-geolocation-v2-2.0.0-20220509.585.0.zip
inflating: geoip-data-v2-Region2-2.0.0-20220509.585.0.i686.rpm
inflating: geoip-data-v2-ISP-2.0.0-20220509.585.0.i686.rpm
inflating: geoip-data-v2-Org-2.0.0-20220509.585.0.i686.rpm

6) dla każdego rozpakowanego pliku (3 sztuki) użyć komendy:
geoip_update_data -f </path/to/rpm> , np:
[admin@pli-000a21:Active:In Sync] tmp # geoip_update_data -f geoip-data-v2-Region2-2.0.0-20220509.585.0.i686.rpm
[admin@pli-000a21:Active:In Sync] tmp # geoip_update_data -f geoip-data-v2-ISP-2.0.0-20220509.585.0.i686.rpm
[admin@pli-000a21:Active:In Sync] tmp # geoip_update_data -f geoip-data-v2-Org-2.0.0-20220509.585.0.i686.rpm

7) zweryfikować poprawną instalację bazy:
geoip_lookup -f /shared/GeoIP/v2/F5GeoIPOrg.dat 193.111.166.166

```
[admin@pli-000a21:Active:In Sync] tmp # geoip_lookup -f /shared/GeoIP/v2/F5GeoIPOrg.dat 193.111.166.166
Will attempt to lookup ip '193.111.166.166'
opening database in /shared/GeoIP/v2/F5GeoIPOrg.dat
size of geoip database = 207894904, segments = 14049688, version = Copyright (c) F5 Networks Inc, All Rights Reserved GEOIP2 v1, 20220509
geoip_seek = 0004739a
geoip record ip = 193.111.166.166
name = bank polska kasa opieki s.a.
scope = 24
[admin@pli-000a21:Active:In Sync] tmp #
```

8) usunąć z /shared/tmp zip-a, plik md5, rozpakowane 3 pliki rpm i README.txt
rm -f ip-geo*
rm -f *.rpm
rm -f README.txt

Z <https://wiki/display/TSEC/Aktualizacja+bazy+GeoIP+na+F5+DMZ>

WAF

25 kwietnia 2023
11:58

RDP check

9 marca 2023
09:55

```
C:\Users\azagrobelny>query session
 NAZWA SESJI       NAZWA UŻYTKOWNIKA       ID  STAN    TYP        URZĄDZENIE
                                            0  Disc
 console                                    1  Conn
>rdp-tcp#0         azagrobelny             2  Aktywna  rdpwd
 rdp-tcp                                65536  Nasłuchuj

C:\Users\azagrobelny>
```

PowerSehll - generator haseł

7 kwietnia 2023
15:34

```
# Funkcja do generowania hasła
function Generate-Password {
   # Długość hasła
   $Length = 20

   # Zbiór znaków, z których może składać się hasło
   $Chars = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%
^&*()_+-=[]{};:,.<>?"

   # Generowanie losowego hasła
   $Password = ""
   1..$Length | ForEach-Object {
      $Password += $Chars[(Get-Random -Minimum 0 -Maximum $Chars.Length)]
   }

   # Zwrócenie hasła
   return $Password
}

# Wywołanie funkcji i wyświetlenie hasła
Generate-Password
```

PowerShell - suma konktrolna

21 kwietnia 2023
13:48

```
PS H:\> Get-FileHash .\Kosztorys.xls

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          D9F597AA32DBB7A59D3759558366EBFAB4112AB3A730831B7E70AA41F6E9A137       H:
\Kosztorys.xls
```

CMD - komendy

24 kwietnia 2023
16:10

Grepowanie

```
C:\Users\azagrobelny>ipconfig /all | findstr "fizyczny"
   Adres fizyczny. . . . . . . . . . : A0-8C-FD-F3-09-1E
```

Upgrade

9 marca 2022
11:54

IOS-XE firmware have a filename extension of “bin”.
ROMMON files have an extension of “pkg”.

Weryfikacja zeminnej boot:

```
PRO-ISAA1#show bootvar
        BOOT variable does not exist
        CONFIG_FILE variable does not exist
        BOOTLDR variable does not exist
        Configuration register is 0x2102

Standby not ready to show bootvar
```

ISR: Software upgrade

9 marca 2022
11:40

How to Install and Upgrade the Software

To install or upgrade the software, use one of the following methods to use the software from a consolidated package or an individual package. Also see the overview section.

a. Managing and Configuring a Router to Run Using a Consolidated Package
b. Managing and Configuring a Router to Run Using Individual Packages
c. Managing and Configuring a Router to Run Using a Consolidated Package
d. Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example

Z <https://www.cisco.com/c/en/us/td/docs/routers/access/isr4400/software/configuration/xe-17/isr4400-sw-config-xe-17/install.html#concept_0EDA6D6296B74D3B9743A77302187643>

A') Managing and Configuring a Consolidated Package Using copy and boot Commands

To upgrade a consolidated package, copy the consolidated package to the bootflash: directory on the router using the copy command. After making this copy of the consolidated package, configure the router to boot using the consolidated package file.

The following example shows the consolidated package file being copied to the bootflash: file system TFTP. The config register is then set to boot using boot system commands, and the boot system commands instruct the router to boot using the consolidated package stored in the bootflash: file system. The new configuration is then saved using the copy running-config startup-config command, and the system is then reloaded to complete the process.

```
Router# copy tftp:<ścieżka source> bootflash:
Router# configure terminal
Router(config)# boot system flash bootflash:isr4400-universalk9.17.03.04a.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# copy run start
Router# reload
```

ASR: show tx power

5 listopada 2021
00:47

RP/0/RSP0/CPU0:PRO-INTA1# show controllers Te0/0/2/2 phy
…

```
      Thresholds:                Alarm High       Warning High       Warning Low        Alarm Low
          Temperature:           +75.000 C        +70.000 C          +0.000 C           -5.000 C
              Voltage:           3.630 Volt       3.465 Volt         3.135 Volt         2.970 Volt
                Bias:            80.000 mAmps     75.000 mAmps       10.000 mAmps       8.000 mAmps
        Transmit Power:  2.23870 mW (3.49996 dBm)   1.12200 mW (0.49993 dBm)   0.15140 mW
(-8.19874 dBm)   0.06030 mW (-12.19683 dBm)
         Receive Power:  2.23870 mW (3.49996 dBm)   1.12200 mW (0.49993 dBm)   0.03630 mW
(-14.40093 dBm)   0.01450 mW (-18.38632 dBm)
      Temperature: 26.590
      Voltage: 3.253 Volt
      Tx Bias: 26.916 mAmps
      Tx Power:  0.66970 mW (-1.74120 dBm)
      Rx Power:  0.25260 mW (-5.97567 dBm)
```

NSM Upgrade (mlos)

18 lutego 2022
08:49

1. Zalogowanie się do NSM po CLI

1. Wykonać **watchdog stop** command.

```
Manager@PID-000VM1> watchdog stop

We trust you have received the usual lecture from the local
System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for admin:
```

3. Wykonać **manager stop** command.

Manager@PID-000VM1> manager stop

4. You must download the Manager upgrade file (setup.bin) from the Download Server (https://www.mcafee.com/ENTERPRISE/EN-US/DOWNLOADS/MY-PRODUCTS.html) and save it in the Linux machine, when using scp setup from remote machine and install
5. Przekopiować plik instalacyjny przez SCP (Bitvise) do /opt/scpfiles

6. Wylkonać **upgrade** command

Manager@PID-000VM1> upgrade
Choose one of the below options

1: scp setup from remote machine and install
2: install the setup present on local machine
Input [1] or [2] : **2**

Enter the path to the setup.bin file: **/opt/scpfiles/NSM_1017502_setup.bin**
Installing : NSM_1017502_setup.bin
Decrypting and verifying /opt/scpfiles/NSM_1017502_setup.bin, this may take couple of minutes to complete
Preparing to install
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

==========
Manager (created with InstallAnywhere)

Preparing CONSOLE Mode Installation...
==========
Introduction

Welcome to the McAfee Installation Wizard.

This Wizard can be used to install either of the following applications:

- McAfee Network Security Manager v10.1.7.50.2

- McAfee Network Security Central Manager v10.1.7.50.2

It is strongly recommended that you quit all programs before continuing with this installation.

Respond to each prompt to proceed to the next step in the installation.

You may cancel this installation at any time by typing 'quit'.

PRESS <**ENTER**> TO CONTINUE:

==========
Manager Upgrade

Your current McAfee Network Security Manager Version 10.1.7.50 will be upgraded to 10.1.7.50.2.

PRESS <**ENTER**> TO CONTINUE:

==========
Enter Database Root password

Please enter Database Root password :

```
================================================================================
====
Choose Link Location
--------------------

Where would you like to create links?

 ->1- Default: /root
   2- In your home folder
   3- Choose another location...

   4- Don't create links

ENTER THE NUMBER OF AN OPTION ABOVE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
     : 1



================================================================================
====
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
   Manager

Manager Type:
   Network Security Manager

Install folder:
   /opt/NetworkSecurityManager/App

Database folder:
   /opt/NetworkSecurityManager/MariaDB

Solr folder:
   /opt/NetworkSecurityManager/Solr

Link folder:
   /root

Disk Space Information (for Installation Target):
   Required:   2,534,251,169 Bytes
   Available: 81,222,930,432 Bytes

PRESS <ENTER> TO CONTINUE:



================================================================================
====
```

Ready To Install

Ready to install Network Security Manager onto your system at the following location:

/opt/NetworkSecurityManager/App

PRESS <**ENTER**> TO INSTALL:

==========
====
Installing...

[==========|==========|==========|==========]
[==========|==========|==========|==========]
]

Please Wait

Please Wait

----------pub rsa2048/9365EB6F3B62B36E 2018-11-05 McAfee NSM (nsm key)

pub rsa2048/9365EB6F3B62B36E 2018-11-05 McAfee NSM (nsm key)

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: unknown validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: unknown validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately

m = back to the main menu

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: ultimate validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)
Please note that the shown key validity is not necessarily correct
unless you restart the program.

Key not changed so no update needed.

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: unknown validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: unknown validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

1 = I don't know or won't say
2 = I do NOT trust
3 = I trust marginally
4 = I trust fully
5 = I trust ultimately
m = back to the main menu

pub rsa2048/9365EB6F3B62B36E
created: 2018-11-05 expires: never usage: SC
trust: ultimate validity: unknown
sub rsa2048/077845F659B6ED14
created: 2018-11-05 expires: never usage: E
[unknown] (1). McAfee NSM (nsm key)
Please note that the shown key validity is not necessarily correct
unless you restart the program.

Key not changed so no update needed.
5
-|-----------------|-----------------|---------

==========
====

Please Wait

Installation Complete

Congratulations. Manager has been successfully installed to:

/opt/NetworkSecurityManager/App

Auto Reboot of the server will be initiated to complete the upgrade process
after exiting the installer.

PRESS <**ENTER**> TO EXIT THE INSTALLER:

Please Wait

Connection closing...Socket close.

1. Wykona się automatyczny reload. Po uruchomieniu NSM ma nowy soft

NSM: DB query

28 grudnia 2022
11:42

1. SSH to Manager IP address.
2. Login with admin credentials.
3. Type the CLI command 'dbShell' and press ENTER.
4. When prompted, provide your database username and password and press ENTER.
   Default admin/admin123
5. Run the query - SELECT COUNT(*) FROM iv_alert WHERE sensorAlertUUID <= 0;
6. Copy and save the output to a text file.
7. Upload file to supportm.trellix.com/upload.

NSM: IPS Sensor Trace

28 lutego 2023
12:09

https://kcm.trellix.com/corporate/index?page=content&id=KB55549

Environment

Trellix Intrusion Prevention System (Trellix IPS)

Summary

If the Sensor is trusted to a Manager, collect the diagnostic trace on the Manager:

1. Navigate to the **Devices** tab, and select the Sensor from the drop-down list.
2. Click the **Troubleshooting** tab and select **Diagnostic Trace**.
3. Verify that the Sensor is selected under the **Diagnostic trace** table and then click **Upload**. Close the window when you see the **Download Complete** message.
4. Refresh the window and view the trace listed in the bottom section.
5. Select the trace and click **Export**.
6. Save the file to your local client and send it to Technical Support. Or, collect the trace file directly from the Manager.

   NOTE: The trace files are uploaded to the following directory on the Manager:

   \<Installation Directory>\App\temp\tftpin\<sensor name>\trace

If the Sensor isn't trusted to a Manager, collect the Diagnostic Trace from the Sensor using TFTP:

1. Set up a TFTP server.
2. Log on to the Sensor via a console connection or SSH.
3. Type the following commands:

   Set sensor ip xxx.xxx.xxx.xxx 255.xxx.xxx.xxx (to set IP address and mask if the Sensor doesn't have them)
   Set tftpserver ip xxxx (to set to TFTP server IP address)
   logstat all
   traceupload <TraceFileName>.enc
   The Sensor now uploads the trace file to the TFTP server.

   NOTE: The **logstat** command injects the current Sensor status to the log files.

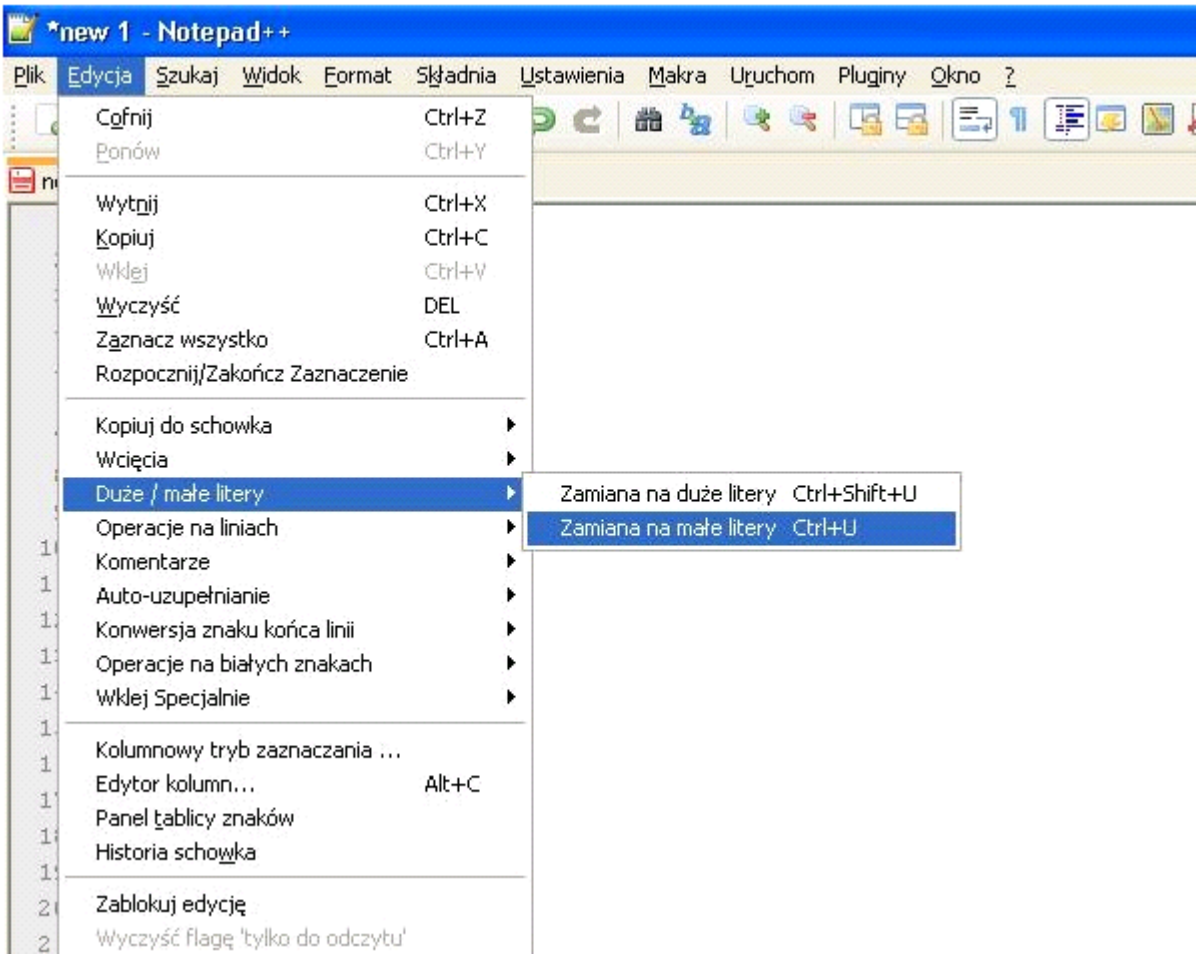
Notepad: Tekst w jednej linijce

4 marca 2022
12:41

Ctrl + J – tekst w jednej linijce

Notepas: Zamiana liter

27 października 2022
12:12



Planowane Prace

1 lutego 2023
14:28

Topic: Bank Pekao S.A - Prace w obszarze Extranet

Szanowni Państwo,

Z ramienia Banku Pekao S.A. informujemy, iż w związku z planowanymi pracami w obszarze Extranet okresie 2023-02-02 22:00 - 2023-02-03 01:00 prowadzone będą działania skutkujące czasową niedostępnością łącza podstawowego ID: SOZ66604.
Z uwagi na obecność łącza zapasowego nie przewidujemy przerwy w działaniu usług produkcyjnych.

Pozdrawiam

Key Tag

6 marca 2023
13:47

```
[azagrobelny@ipsmipc-poc ~]$ delv @8.8.8.8 peopay.pl +nocrypto DNSKEY
; unsigned answer
peopay.pl.              6879    IN      DNSKEY256 3 13 [key id = 38446]  ; ZSK; alg = ECDSAP256SHA256 ; key id = 38446
peopay.pl.              6879    IN      DNSKEY256 3 13 [key id = 28541]  ; ZSK; alg = ECDSAP256SHA256 ; key id = 28541
peopay.pl.              6879    IN      DNSKEY257 3 13 [key id = 21276]  ; KSK; alg = ECDSAP256SHA256 ; key id = 21276
peopay.pl.              6879    IN      RRSIG   DNSKEY 13 2 7200 20230309102414 20230306092414 21276 peopay.pl. [omitted
```

```
$ dig +multi isc.org DNSKEY
; <<>> DiG 9.8.2 <<>> +multi isc.org DNSKEY
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54063
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;isc.org.       IN DNSKEY
;; ANSWER SECTION:
isc.org.       2249 IN    DNSKEY 256 3 5 (
            BEAAAAO6L6BadeFzvt6J63GDGrFANfJAitCd9Njcj49y
            6PE1Bv6t33sEyxSVi4KWbjQgViMCxAArxP0IhDLhYFGb
            sU2ugkQ4UMFCPgYIVxC1yvBw1Gt7p+SBQU9qX+Il/cqY
            TJWQkWRdDPHJoaMT1+f7e6YLlntxpl+M7yw3aOEbCByP
            zw==
            ) ; key id = 21693
isc.org.       2249 IN    DNSKEY 257 3 5 (
            BEAAAAOhHQDBrhQbtphgq2wQUpEQ5t4DtUHxoMVFu2hW
            LDMvoOMRXjGrhhCeFvAZih7yJHf8ZGfW6hd38hXG/xyl
            YCO6Krpbdojwx8YMXLA5/kA+u50WIL8ZR1R6KTbsYVMf
            /Qx5RiNbPClw+vT+U8eXEJmO20jIS1ULgqy347cBB1zM
            nnz/4LJpA0da9CbKj3A254T515sNIMcwsB8/2+2E63/z
            ZrQzBkj0BrN/9Bexjpiks3jRhZatEsXn3dTy47R09Uix
            5WcJt+xzqZ7+ysyLKOOedS39Z7SDmsn2eA0FKtQpwA6L
            XeG2w+jxmw3oA8lVUgEf/rzeC/bByBNsO70aEFTd
            ) ; key id = 12892
;; Query time: 35 msec
;; SERVER: 194.74.65.69#53(194.74.65.69)
;; WHEN: Thu Jan 26 12:43:36 2012
;; MSG SIZE  rcvd: 451
```

Z <https://kb.isc.org/docs/aa-00610>

DS Rekord

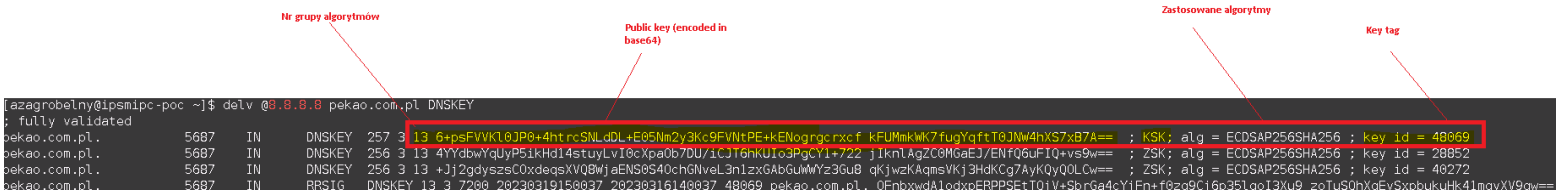
14 marca 2023
22:28

DS. Record (Delegation Signer) – wskazuje klucz KSK (Key Signing Key), podpisujący klucz ZSK (Zone Signing Key) strefy podrzędnej. W celu zbudowania pełnego łańcucha zaufania dla DNSSEC, należy przekazać do registrara rekord DS. W tym celu należy podać takie pola jak te poniżej.

General information | DNS zone | DNS servers | Redirection | DynHost | GLUE | DS records | Recent tasks | Emails and mailin

Key tag	Flag	Algorithm	Public key (encoded in base64)
48069	257 - Key Signing Key (KSK)	13 - ECDSAP256SHA256	6+psFVVKl0JP0+4htrcSNLdDL+E05Nm2y3Kc9FVNtPE+kENogrgcrxcfkFUMmkWK7fugYqftT0JNW4hXS7xB7A==

Te dane możemy odszukać poleceniem **delv @8.8.8.8 pekao.com.pl DNSKEY**




```
[azagrobelny@ipsmipc-poc ~]$ delv @8.8.8.8 pekao.com.pl DNSKEY
; fully validated
pekao.com.pl.           5687    IN      DNSKEY  257 3 13 6+psFVVKl0JP0+4htrcSNLdDL+E05Nm2y3Kc9FVNtPE+kENogrgcrxcf kFUMmkWK7fugYqftT0JNW4hXS7xB7A== ; KSK; alg = ECDSAP256SHA256 ; key id = 48069
pekao.com.pl.           5687    IN      DNSKEY  256 3 13 4YYdbwYqUyP5ikHd14stuyLvI0cXpaOb7DU/iCJT6hKUIo3PgCY1+722 jIknlAgZC0MGaEJ/ENfQ6uFIQ+vs9w==  ; ZSK; alg = ECDSAP256SHA256 ; key id = 28052
pekao.com.pl.           5687    IN      DNSKEY  256 3 13 +Jj2gdyszsC0xdeqsXVQ8WjaENS0S4OchGNveL3nlzxGAbGuWWYz3Gu8 qKjwzKAqmsVKjJHdKCg7AyKQyQOLCw==  ; ZSK; alg = ECDSAP256SHA256 ; key id = 40272
pekao.com.pl.           5687    IN      RRSIG   DNSKEY 13 3 7200 20230319150037 20230316140037 48069 pekao.com.pl. QEnbxwdAlodxpERPPSEtTOiV+SbrGa4cYiEn+f9zo9Ci6p35lqoI3Xu9 zoIuSOhXqEvSxpbukuHk4lmqvXV9qw==
```

Weryfikacja czy rekord DS. jest:

[azagrobelny@ipsmipc-poc ~]$ **delv @8.8.8.8 pekao.com.pl DS**
; fully validated
pekao.com.pl. 20967 IN DS 48069 13 2
E5B3D696AE13415C2CC2471F5E2A7D3D20A880EDC612B649AE02914E 8768FAEB

Weryfikacja czy DNSSEC jest poprawnie podpisany:

azagrobelny@ipsmipc-poc ~]$ **delv @8.8.8.8 pekaopartner.pl DNSSEC**
;; validating pekaopartner.pl/A: no valid signature found
; unsigned answer
pekaopartner.pl. 21600 IN A 193.111.166.220
pekaopartner.pl. 21600 IN RRSIG A 13 2 21600 20230317100405 20230314090405
pekaopartner.pl. 9z/B3sTFdASwpNl/gg0braxSzQcj0uGihKbFwV1VONbSoUaqg/+iMtr9
/AlH6nbIOSh5hiA7TNAfWPlQCCxJ1w==

Or

; fully validated
pekaopartner.pl. 21600 IN A 193.111.166.220
pekaopartner.pl. 21600 IN RRSIG A 13 2 21600 20230318220405 20230315210405
pekaopartner.pl. 7W8jLoKx9uFx6XnLCBRN1HaesfwrA4RwOjXOsrSlW5DHV2h1NQk+uqkg
f6ZfFWs711imltngw4thrHY9UPpqBA==

Powershell: Operacje na grupie

2 marca 2023
10:06

https://learn.microsoft.com/en-us/powershell/module/activedirectory/get-adgroup?view=windowsserver2022-ps

Wyświetlenie właściwości danej grupy

PS H:\> Get-ADGroup -Identity "Biuro Telekomunikacji-Zespół Rozwoju i Bezpieczeństwa Sieci"

Filtry

20 kwietnia 2023
14:04

Basic Network

ip.addr = = 10.1.0.52	Szukanie adresu stricte 10.1.0.52 w obu kierunkach
ip.src == 192.168.1.1/16	#Filtruj komunikację IP z SIECI 192.168.1.1 jako ADRES
ip.dst == 192.168.1.1	#Filtruj komunikację z IP 192.168.1.1 jako ADRES DOCELOWY
tcp/udp/icmp/dns/http/ssl/smb/nbt/nbns/ftp/ssh/	#Filtruj komunikację konkretnego protokołu
ether host 00:ff:11:22:33:ff	#Filtruj ruch tylko z konkretnego adresu MAC

Advance Network

Eth.src[1-2] = = !00:83	Szukanie wszystkich mac addresów kart, które nie zaczynają się od
Udp contains "DNS" && dns.qry.name = =	Filtruj zapytania dns dla konkrtnej doomeny
Tcp.flags.syn = = 1	Pokaż tylko flagi SYN
Tcp[13] = = 0x12	Filtruj pakiety SYN-ACK
radius.access-request	#Filtruj pakiety REQUEST serwera RADIUS
radius.access-reject	#Filtruj pakiety REJECT serwera RADIUS
ip.id == 0 && tcp.analysis.retransmission	#Filtruj retransmisjie TCP z zerowym ID IP
arp.duplicate-address-detected	#Filtruj duplikaty pakietów ARP

Time

frame.time >= "2023-04-19	#Pokaż pakiety od określonego czasu
frame.time_delta >= 0.1	#Pokaż pakiety których różnica czasu DELTA jest większa lub równa 0.1
frame.len < 100	#Pokaż pakiety z długością ramki mniej niż 100 bajtów

Application

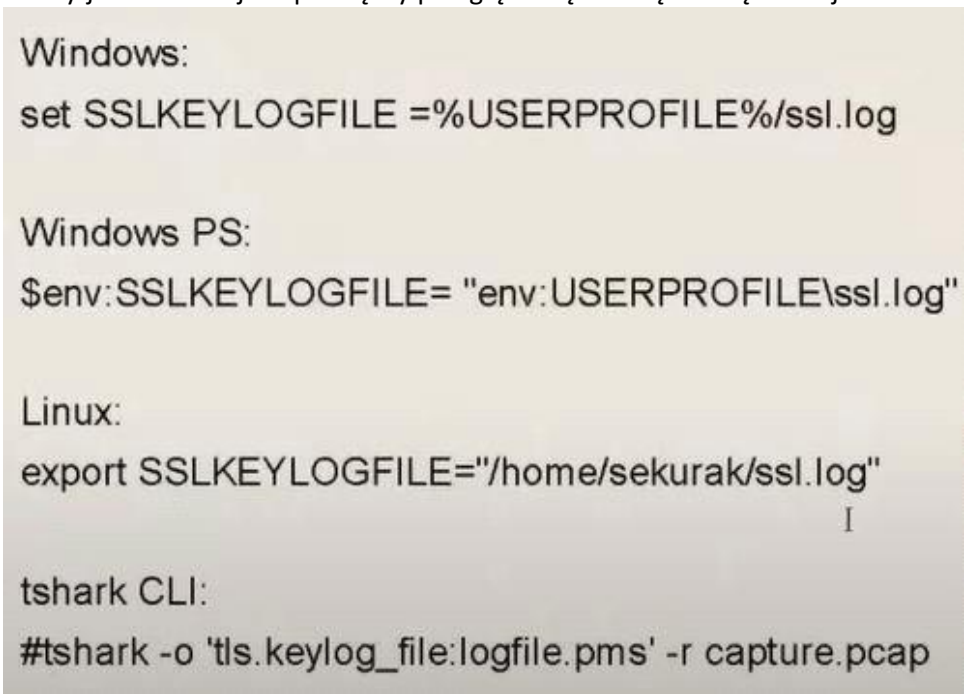
Data-txt-lines = = "POST"	Filtruje pakiety zawierające tekst "POST" w poli danych
Http.cookie contains "SESSIONID="	Filtruje pakiety ze specyficznym ciasteczkiem
Tcp contains "GET" && http.host = =	Filtruje metody GET do konkretnego hosta
Http.responce.status_code = = 200	Filtruj tylko odpowiedzi HTTP = 200
http.request.uri matches ".*(\.jpg|\.png|\.gif)$"	#Filtruj ruch HTTP z obrazkami
frame contains "passw0rd"	#Pakiety zawierające łańcuch "passw0rd" w dowolnym
tcp contains "GET"	#Pakiety TCP zawierające łańcuch "GET" w dowolnym polu
udp contains "DNS"	#Pakiety UDP zawierające łańcuch "DNS" w dowolnym
http.request	#Filtruj pakiety zawierające HTTP REQUEST
http.response	#Filtruj pakiety zawierające HTTP RESPONSE

Deszyfracja ruchu

24 kwietnia 2023
15:12

Scenariusz: Łapiemy ruch na jednym z końców komunikacji.

Krok 1. Zdefinioawanie zmiennej środowiskoej SSLKEYLOGFILE. Zmienna ta loguje do pliku całą kluczy jaka ma miejsće pomiędzy przeglądarką a daną stroną która jest odwiedzana.

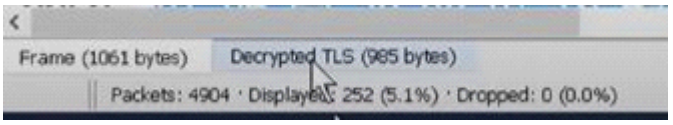


Lub na WINDOWS Cmd-> stystempropertiesadvanced.exe

Krok2.
Zebrać ruch wiresharkiem i go otworzyć

Krok3.
Z menu wybieramy edycja -> preference ->protokoły -> tls -> i w polu (PRE)-Master-Secret log filname wskzaujemy plik z kroku 1

Krok4.
Wybierając pakiet TLS, pokazuje się nam nowa zakładka Decrypted TLS



Weryfikacja Fingerprint

24 kwietnia 2023
12:19

Krok1. Złapać pcap i znaleść pakiet z Server Hello

```
Frame 393: 116 bytes on wire (928 bits), 116 bytes captured (928 bits) on interface \Device\NPF_{7389A04E-2E27-4408-8E62-1F23887CF974}, id 0
Ethernet II, Src: Cisco_9f:f4:69 (00:00:0c:9f:f4:69), Dst: HewlettP_f3:09:1e (a0:8c:fd:f3:09:1e)
Internet Protocol Version 4, Src: proxyx.cn.in.pekao.com.pl (172.20.17.210), Dst: P0C13004.cn.in.pekao.com.pl (10.151.136.49)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 102
    Identification: 0x5442 (21570)
  010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 249
    Protocol: TCP (6)
    Header Checksum: 0xdca0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: proxyx.cn.in.pekao.com.pl (172.20.17.210)
    Destination Address: P0C13004.cn.in.pekao.com.pl (10.151.136.49)
Transmission Control Protocol, Src Port: 8080, Dst Port: 27510, Seq: 131, Ack: 730, Len: 62
Hypertext Transfer Protocol
Transport Layer Security
  TLSv1.2 Record Layer: Handshake Protocol: Server Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 57
    Handshake Protocol: Server Hello
        Handshake Type: Server Hello (2)
        Length: 53
        Version: TLS 1.2 (0x0303)
      Random: 5c94223f8af6ab2fda477f8e7cbba0c51106dea62cefdab63f62fb7257a131e5
          GMT Unix Time: Mar 22, 2019 00:46:07.000000000 rodkowoeuropejski czas stand.
          Random Bytes: 8af6ab2fda477f8e7cbba0c51106dea62cefdab63f62fb7257a131e5
        Session ID Length: 0
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 13
      Extension: renegotiation_info (len=1)
      Extension: ec_point_formats (len=4)
        [JA3S Fullstring: 771,49199,65281-11]
        [JA3S: 303951d4c50efb2e991652225a6f02b1]
```

Krok 2.w Nagłówku Transport Layer Securty w polu Handshake Protocol szukamy pozycji JA3 - który stnowi odcisk palca

Krok 3. Kopiujemy na stronę poniżej i sprawdzamy

Baza do weryfikacji:
https://sslbl.abuse.ch/ja3-fingerprints/

JA3 Fingerprints

Here you can browse a list of malicious JA3 fingerprints identified by SSLBL. JA3 is an open source tool used to fingerprint SSL/TLS client applications. In the best case, you can use JA3 to identify malware traffic that is leveraging SSL/TLS.

Caution!

The JA3 fingerprints below have been collected by analysing more than 25,000,000 PCAPs generated by malware samples. These fingerprints have **not been tested against known good traffic yet and may cause a significant amount of FPs!**

Show 50 entries

Search:

Listing Date (UTC)	JA3 Fingerprint	Listing Reason	Malware Samples

Analizatory

21 kwietnia 2023
13:56

https://packettotal.com/
https://www.virustotal.com
https://any.run/

Nauka security

24 kwietnia 2023
10:59

Https://malware-traffic-analysys.net

CSR Generate

Generate CSR
##########################
openssl req -out apcon.cn.in.pekao.com.pl.csr -newkey rsa:2048 -nodes -keyout apcon.cn.in.pekao.com.pl.key -config apcon.txt

default_bits = 2048
default_md = sha256
prompt = no
distinguished_name = req_distinguished_name
req_extensions = req_ext
[req_distinguished_name]
countryName = PL
stateOrProvinceName = Mazowieckie
localityName = Warszawa
organizationName = Bank Polska Kasa Opieki S.A.
commonName = apcon2.cn.in.pekao.com.pl
[req_ext]
subjectAltName = @alt_names
[alt_names]
DNS.1 = apcon2.cn.in.pekao.com.pl
DNS.2 = apcon2
IP.1 = 10.143.135.109

PKCS12

4 stycznia 2022
13:19

Odczyt pliku:

#openssl pkcs12 -info -in INFILE.p12 -nodes
You will then be prompted for the PKCS#12 file's password:
#Enter Import Password:
Type the password entered when creating the PKCS#12 file and press enter. OpenSSL will output any certificates and private keys in the file to the screen

Export PKCS12 - tylko cert
root@Ubuntu:/home/lab/Pulpit/Fime_V5# openssl pkcs12 -info -in keystore.p12 -nokeys

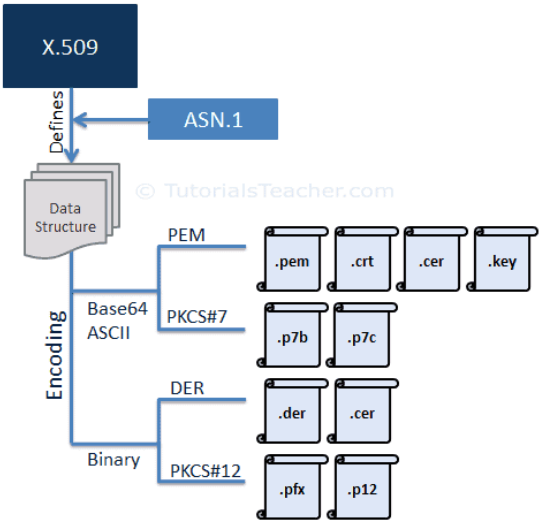
Certificate Convert

4 marca 2022
11:59

PEM Format

The certificate file types can be .pem, .crt, .cer, or .key. The .pem file can include the server certificate, the certificate and the private key in a single file. The server certificate and intermediate certificate can also be in a separate .crt or .cer file. The private key can be in a .key file.

PEM files use ASCII encoding, so you can open them in any text editor such as notepad, MS word etc. Each certificate the PEM file is contained between the ---- BEGIN CERTIFICATE---- and ----END CERTIFICATE---- statements. The private key is contained between the ---- BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY----- statements. The CSR is contained between the -----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST----- statements.



Convert PEM to PFX
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile more.crt

Convert PEM to PKCS#12
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt

Convert PEM to DER
openssl x509 -outform der -in certificate.pem -out certificate.der

Convert PEM to CER
openssl x509 -outform der -in certificate.pem -out certificate.crt

Convert PEM to P7B
openssl crl2pkcs7 -nocrl -certfile certificate.cer -out certificate.p7b -certfile CACert.cer

Convert CRT to DER
openssl x509 -outform der -in rootCA.crt -out rootCA.der

PKCS#7 Format

The PKCS#7 format is a Cryptographic Message Syntax Standard. The PKCS#7 certificate uses Base64 ASCII encoding file extension .p7b or .p7c. Only certificates can be stored in this format, not private keys. The P7B certificates are contained between the "-----BEGIN PKCS7-----" and "-----END PKCS7-----" statements.

Convert P7B to PEM
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer

Convert P7B to PFX
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out certificate.pfx -certfile CACert.cer

DER Format

The DER certificates are in binary form, contained in .der or .cer files. These certificates are mainly used in Java-web servers.

Convert DER to PEM
openssl x509 -inform der -in certificate.cer -out certificate.pem

PKCS#12 Format

The PKCS#12 certificates are in binary form, contained in .pfx or .p12 files.
The PKCS#12 can store the server certificate, the intermediate certificate and the private key in a single .pfx file with password protection. These certificates are mainly used on the Windows platform.
CAs provide certificates in any of the above formats. Learn how to install a certificate on different web servers in the next chapter.

Convert PFX to PEM
openssl pkcs12 -in certificate.pfx -out cert.pem
or
openssl pkcs12 -in yourfile.pfx -out nowa_nazwa_certa.cer
openssl pkcs12 -in yourfile.pfx -nocerts -out nowa_nazwa_klucza.key