

HÁLÓZATI ISMERETEK

4. forduló



Lufthansa Systems

A kategória támogatója: Lufthansa Systems

Hungária Kft.

Ismertető a feladatlaphoz

Közeleg az 5. forduló, figyelj az időpontokra!

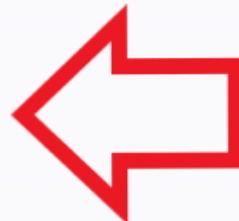
Használd a naptárat:

KATEGÓRIÁIM

Összesen 10 kategóriára jelentkezted



Versenynaptár letöltése



Vagy figyeld kategóriánként az időpontokat (íme egy MINTA, hol találsz):




● 3. FORDULÓ

A lezárt fordulókban eddig megszerzett pontok:

0/105 pont

**BOSCH**
Invented for life

Fordulók

Forduló	Pontok, időtartam	Feladat megoldható	Státusz
7. forduló	23 pont 25:00	 2023.11.28. 20:00-tól 2023.11.28. 20:35-ig	Feladatlap
6. forduló	23 pont 30:00	 2023.11.21. 20:00-tól 2023.11.21. 20:40-ig	Feladatlap
5. forduló	28 pont 25:00	 2023.11.14. 20:00-tól 2023.11.14. 20:35-ig	Feladatlap

Amennyiben olyan kategóriában játszol, ahol van csatolmány, de hibába ütközel a letöltésnél, ott valószínűleg a vírusirtó korlátoz, annak ideiglenes kikapcsolása megoldhatja a problémát. (Körülbelül minden 3000. letöltésnél fordul ez elő.)

Jó versenyzést kívánunk!

Tűzfalas kollégád egész hónapban szabadságon van, így téged kértek meg a tűzfalas jegyek, problémák és az üzemeltetési feladatok ellátására.

1. feladat 4 pont

Melyek az igaz állítások az újgenerációs tűzfalakra (NGFW) nézve?

Válaszok

- ☐ Stateful módon viselkednek, azaz a válaszcsoomagok automatikusan engedélyezettek.
- ☐ Alkalmazás szintjén (Layer 7) képesek a hálózati forgalom engedélyezésére, vagy tiltására.
- ☐ Képesek az aszimmetrikus hálózati topológiából eredő forgalom kezelésére is.
- ☐ A maximális védelem érdekében az engedélyezett TCP SYN csomagra érkező TCP SYN-ACK-ot is engedélyezni szükséges.

- ☐ Integrált IDS/IPS képességekkel rendelkeznek.
- ☐ Titkosított SSL/TLS forgalom bontására is képesek.
- ☐ URL szűrési funkciók is elérhetők.

2. feladat 4 pont

Sajnos megérkezett az első hibajegy, amit szerveres kollégád adott fel. Elpanaszolja a jegyben, hogy a kérésük az volt, hogy csak SSH protokollal lehessen elérni a szervert, de neki telnet-en is sikerült csatlakoznia. Milyen magyarázatot tudsz adni neki a szabályrendszer átnézése után?

```
user@host:~$ telnet 192.168.9.250 22
```

```
Trying 192.168.9.250...
```

```
Connected to 192.168.9.250.
```

```
Escape character is '^['.
```

```
SSH-2.0-Cisco-1.25
```

```
telnet> quit
```

```
Connection closed.
```

Tűzfal szabályok:

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	ZONE	ADDRESS				
52	allow_ssh-to-ssh-server	OITM	intrazone	zone_l2-lan	any	any	(intrazone)	ip_ssh-server	ssh	application-default	any	Allow
53	deny_else-to-ssh-server	OITM	intrazone	zone_l2-lan	any	any	(intrazone)	ip_ssh-server	any	any	any	Deny
		deny										

Válasz

- ☐ A tűzfal szoftver verziója bugos, upgrade szükséges.
- ☐ A tűzfal hardverrel van a gond, RMA-zni kell.
- ☐ Ez az elvárt működés, szóban elmagyarázod neki.
- ☐ Elrontottad a config-ot, módosítani kell az application-default-ot TCP 22-re.
- ☐ Elrontottad a config-ot, specifikusan blokkolni kellett volna a telnet alkalmazást.

3. feladat 4 pont

Kollégád előkészítette a konfigurációját annak a tűzfalnak, amit ma reggel vittek ki egy új ügyfelekhez, ahonnan csak annyi visszajelzés érkezett, hogy "nincs Internet!". Egy Teamviewer session keretében eléred a tűzfalat, a következő szabályrendszerrel találkozol:

	NAME	TAGS	TYPE	Source		Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
				ZONE	ADDRESS	ZONE	ADDRESS						
35	allow_internet-web	OITM	universal	any	any	SecZ_WAN	any	ssl web-browsing	application-default	any	Allow	none	
36	allow_users-dns	OITM dns	universal	any	any	any	ip_dns-server-local	dns	application-default	any	Allow	none	
37	allow_users-mail	OITM mail	universal	any	any	any	ip_mail-server	imap smtp	application-default	any	Allow	none	
38	deny_else	OITM deny	universal	any	any	any	any	any	any	any	Deny	none	

Melyik szabályra van szükség, hogy az internet elérés megjavuljon?

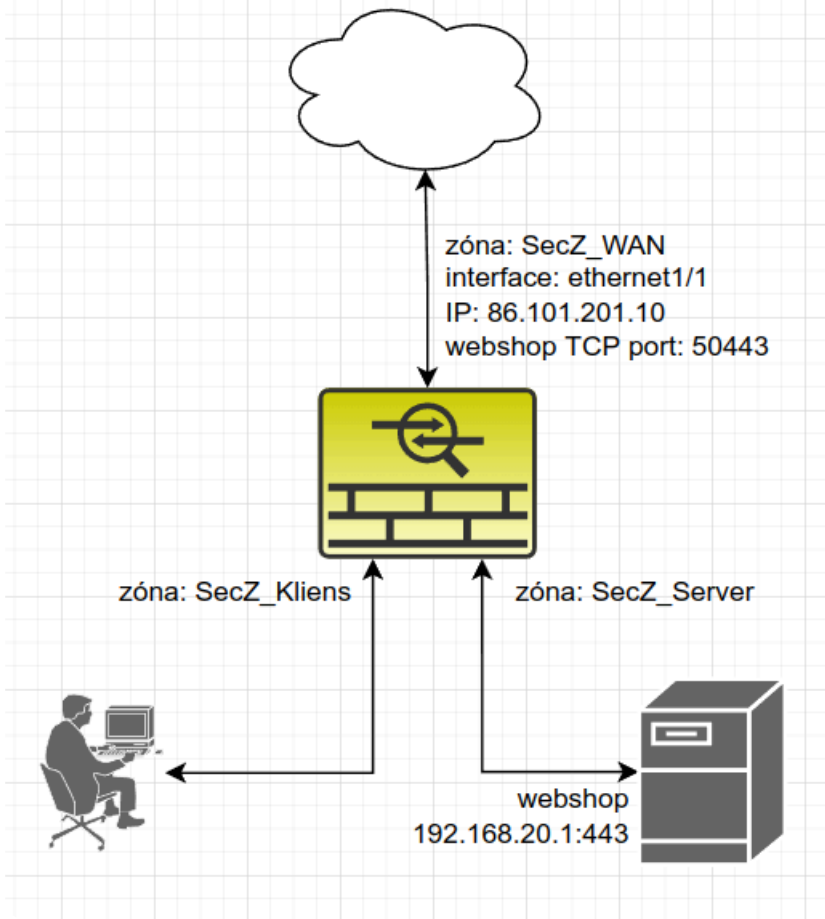
NAME	TAGS	TYPE	Source		Destination		APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	ZONE	ADDRESS						
rule_OPTION1	OITM dns	universal	any	ip_dns-server-local	any	any	ssl web-browsing	application-default	any	Allow	none	
rule_OPTION2	OITM	universal	any	any	any	any	ntp	application-default	any	Allow	none	
rule_OPTION3	OITM	universal	any	any	SecZ_WAN	any	facebook	application-default	any	Allow	none	
rule_OPTION4	OITM dns	universal	any	ip_dns-server-local	any	ip_dns-public	dns	application-default	any	Allow	none	
rule_OPTION5	OITM	universal	any	any	any	any	ping	application-default	any	Allow	none	
rule_OPTION6	OITM	universal	any	any	SecZ_WAN	any	quic	application-default	any	Allow	none	
rule_OPTION7	OITM	universal	any	any	SecZ_WAN	any	any	application-default	url_google.com	Allow	none	

Válasz

- ☐ rule_OPTION1
- ☐ rule_OPTION2
- ☐ rule_OPTION3
- ☐ rule_OPTION4
- ☐ rule_OPTION5
- ☐ rule_OPTION5
- ☐ rule_OPTION6
- ☐ rule_OPTION7

4. feladat 4 pont

A következő sürgős kérés érkezett a menedzsentől: "Kérem, hogy tegyék elérhetővé a webshop alkalmazást a TCP 50443-as porton az internetes felhasználók számára, amely a 192.168.20.1-es szerveren fut a TCP 443-as porton!" Hálózati topológia átnézése után bejelentkezel a tűzfalokba, ahol látod, hogy több NAT szabály is szerepel előkészítve. Melyik opciót kell aktiválnod, hogy a menedzsment kérését teljesítsd?



	NAME	TAGS	Original Packet						Translated Packet	
			SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
8	nat_OPTION1	OITM	any	SecZ_WAN	ethernet1/1	any	any	tcp-50443	none	destination-translation address: 192.168.20.1 port: 443
9	nat_OPTION2	OITM	any	SecZ_Server	ethernet1/1	any	86.101.201.10	tcp-50443	none	destination-translation address: 192.168.20.1 port: 443
10	nat_OPTION3	OITM	any	SecZ_WAN	ethernet1/1	any	192.168.20.1	tcp-443	none	destination-translation address: 86.101.201.10 port: 50443
11	nat_OPTION4	OITM	any	SecZ_WAN	ethernet1/1	192.168.20.1	any	tcp-443	dynamic-ip-and-port 86.101.201.10	none
12	nat_OPTION5	OITM	any	SecZ_Server	ethernet1/1	any	86.101.201.10	tcp-443	none	destination-translation address: 192.168.20.1 port: 50443

Válasz

- ☐ nat_OPTION1
- ☐ nat_OPTION2
- ☐ nat_OPTION3
- ☐ nat_OPTION4
- ☐ nat_OPTION5

Megoldások beküldése