

# Bezpečnostní audit firewallu

Číslo auditu:.....

Datum:.....

Adresa:.....

.....

.....

Kontaktní osoba:.....

Telefon:.....

---

## Doporučení:

- Zapnutí automatických aktualizací nebo zavedení pravidelných ručních aktualizací se zápisem do záznamu.
- Zabezpečit GRUB heslem.
- Zakázat automatické přihlašování.
- Vypnout nepotřebné služby systému.
- Zakázat přihlašování pro uživatele root přes ssh.
- Zvážit povolení všech služeb pro lan, dmz a firewallu při připojení do externí sítě,
- Vytvořit překlad adres pro servery v dmz pro všechny porty.
- Povolit vyžadovaný ping na servery dmz.
- Odstranit kolizní a nadbytečná pravidla.

# 1 Řízení bezpečnosti a personální bezpečnost

## 1.1 Řízení bezpečnosti - bezpečnostní politiky

1.1.1 Jsou dokumentované bezpečnostní politiky schválené managementem?

není dostupné

1.1.2 Obsahují bezpečnostní politiky jména, kdo navrhl bezpečnostní dokument a kdo jej schválil?

není dostupné

1.1.3 Jsou zavedeny prokazatelné seznámení zaměstnanců s bezpečnostními politikami?

není dostupné

1.1.4 Jsou bezpečnostní politiky a nařízení společnosti dostupné zaměstnancům?

není dostupné

1.1.5 Jsou zavedeny nařízení ukládající bezpečnostní kontroly a audity?

není dostupné

1.1.6 Jsou zavedeny nařízení stanovující pravidelné bezpečnostní reporty? (zprávy o bezpečnostních incidentech, risk management)

není dostupné

## 1.2 Personální bezpečnost

1.2.1 Je zodpovědnost o bezpečnosti pro jednotlivé pracovní funkce definována v popisu práce a v bezpečnostních politikách?

není dostupné

1.2.2 Jsou zaměstnanci prokazatelně proškoleni a trénováni?

není dostupné

1.2.3 Jsou definovány disciplinární zaměstnanců porušující bezpečnostní nařízení?

není dostupné

# 2 Kontrola firewallu - Fyzická bezpečnost, logický přístup

## 2.1 Fyzická bezpečnost

2.2.1 Je firewall umístěn v oddělené uzamykatelné místnosti? (např. serverovna)

není dostupné

2.2.2 Je zavedena forma autentifikace při přístupu k firewallu?

není dostupné

2.2.3 Je firewall umístěn v uzamykatelné skříni? (racková skříň)

není dostupné

2.2.4 Je zabezpečena kabeláž proti přímému přístupu? (volně dostupná x chráněná )

není dostupné

2.2.5 Je zavedena forma dohledu nad zařízením? (kamerový systém apod.)

není dostupné

2.2.6 Je využívána záloha napájení? (UPS, generátory)

není dostupné

2.2.7 Je prostředí klimatizováno?

není dostupné

2.2.8 Je veden prokazatelný záznam přístupů k zařízením?

není dostupné

2.2.9 Je přístup k veškeré dokumentaci o firewallu zabezpečen? (uzamykatelná skříň, trezor)

není dostupné

## **2.2 Logický přístup**

2.2.1 Je zavedena politika řízení oprávnění pro definování přístupu ke specifickým zařízením a službám?

není dostupné

2.2.2 Je zavedena politika vytváření a mazání uživatelských účtů?

není dostupné

2.2.3 Je zavedena politika hesel? (změna hesel, síla hesel apod.)

není dostupné

2.2.4 Jsou zavedeny automatické aktualizace?

pouze upozornění na aktualizace

2.2.5 Je zaheslován přístup do BIOSu?

není dostupné

2.2.6 Je zakázáno startování systému z vyměnitelných médií?

Bios – nelze dostupné detekovat, Grub – zapnuta volba bootování z diskety, možnost upravit bootování

2.2.7 Je zaheslován přístup do operačního systému?

ano

2.2.8 Jsou zakázány nezaheslované účty, Guest apod.?

ne, ale nelze přihlásit k systému

2.2.9 Je zakázáno automatické přihlášení?

ne

2.2.10 Je při nečinnosti po časovém limitu vyžadováno heslo pro přístup do systému?

ano

2.2.11 Jsou datové soubory s hesly zabezpečeny, šifrovány?

ano

2.2.12 Jsou spuštěny jen vyžadované služby?

*netstat -an*

ne, doporučuje se vypnout nebo zablokovat porty  
tcp 111 (0.0.0.0), tcp 25(0.0.0.0), udp 5353(0.0.0.0),udp 631(0.0.0.0), udp 731(0.0.0.0)  
doporučuje se specifikovat naslouchající rozhraní  
tcp ssh(0.0.0.0)

2.2.13 Pokud je spuštěna vzdálená správa, je použito šifrování? (ssh, HTTPS atd.)

ano

2.2.14 Je při vzdáleném přístupu zakázáno přímé přihlašování administratorského účtu?

ne, root povolen

2.2.15 Je vyžadována autentizace pro vzdálenou správu?

ano

2.2.16 Nejsou využívána defaultní hesla zařízení?

ano

### 3 Kontrola pravidel filtrování

**Doporučení auditu:** Audit pro jeden stavový paketový firewall filtrující provoz pro lokální sítě a DMZ využívající IPv4.

3.1 Jaký firewall je použit? (HW X SW)

SW

3.2 Na jakém operačním systému firewall běží?

OpenSuse 11.2 x64

3.3 Jaké rozsahy IP adres firewall používá a jak jsou přiděleny síťovým rozhraním a do zón?

192.168.10.10/24 - DMZ – eth1  
192.168.20.10/24 - LAN – eth2  
192.168.30.10/24 - WAN - eth0

3.4 Jaké servery poskytují služby vnější síti? (IP adresy, služby)

veřejná ip – privátní ip - služby

192.168.30.20/24 - 192.168.10.20/24 - HTTP, HTTPS  
192.168.30.30/24 - 192.168.10.30/24 - HTTP, HTTPS, POP3, POP3S, SMTP, SMTPS, IMAP, IMAPS

3.5 Jsou veškeré veřejně dostupné servery v DMZ síti?

ano

3.6 Jsou ostatní PC řádně přiděleny do LAN sítě (síti)?

ano – 1 LAN – 192.168.20.0/24

3.7 Je spouštění firewallu automatické?

ano

3.8 Je zavedeno správné pořadí pravidel?

- *Anti-spoofing filtr (blokování privátní adresy, interní adresy z vnější sítě),*
- *logování a blokování útoků,*
- *zakazující pravidla,*
- *povolovací pravidla – uživatelská (např. veřejný web server),*
- *povolovací pravidla – správa (např. SNMP),*
- *logování (odladění filtrování, informace o filtrované komunikaci na síti).*

ne, ale neovlivňuje funkčnost

3.9 Je zakázán tzv. source routing?

ano

3.10 Je logování dostatečně omezováno? (počet záznamů za jednotku času)

*-m --limit \$Nr/\$TIME -j LOG*

ano

3.11 Jsou defaultní politiky nastaveny na zahazování paketů?

*iptables -P INPUT DROP*

*iptables -P FORWARD DROP*

*iptables -P OUTPUT DROP*

ne - OUTPUT ACCEPT

3.12 Jsou zakázány příchozí pakety z vnější sítě se zdrojovou adresou vnějšího rozhraní?

ano

3.13 Jsou zakázány příchozí pakety z vnější sítě s privátní zdrojovou adresou (RFC 1918), neroutovatelnou adresou nebo adresou APIPA?

rp\_filter zapnut, paketový filtr pravidla neobsahuje

3.14 Je zakázáno broadcast vysílání na jednotlivých rozhraních? Je-li vyžadováno, je blokováno alespoň icmp broadcast vysílání (RFC 2644)?

*iptables -A INPUT -i \$ANY\_IF -m pkttype --pkt-type broadcast -j drop*

*iptables -A FORWARD -i \$ANY\_IF -m pkttype --pkt-type broadcast -j drop*

ano

3.15 Je zakázáno multicastové vysílání?

*iptables -A INPUT -i \$ANY\_IF -m pkttype --pkt-type multicast -j drop*

*iptables -A FORWARD -i \$ANY\_IF -m pkttype --pkt-type multicast -j drop*

ano

3.16 Je logován a blokován tzv. SYN-flood na všech rozhraních na vstupu a v tabulce FORWARD? Je zapnut SYN-cookies?

logování ano, blokování ne, SYN-cookies zapnut

3.17 Jsou logovány a blokovány tzv. Bogus (falešné) pakety na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags SYN, FIN SYN, FIN*

logování ano, blokování na nevyužitých portech

3.18 Je logováno a blokováno FIN/URG/PSH skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags ALL FIN, URG, PSH*

logování ano, blokování na nevyužitých portech

3.19 Je logováno a blokováno SYN/RST skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags SYN, RST SYN, RST*

logování ano, blokování na nevyužitých portech

3.20 Je logováno a blokováno FIN skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags FIN, ACK FIN*

logování ano, blokování na nevyužitých portech

3.21 Je logováno a blokováno FIN Stealth skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags ALL FIN*

logování ano, blokování na nevyužitých portech

3.22 Je logováno a blokováno Null skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags ALL NONE*

logování ano, blokování na nevyužitých portech

3.23 Je logováno a blokováno XMAS skenování na všech rozhraních na vstupu a v tabulce FORWARD?

*--tcp-flags FIN, URG, PSH*

logování ano, blokování na nevyužitých portech

3.24 Je blokováno UDP skenování na všech rozhraních na vstupu a v tabulce FORWARD?

logování ano, blokování na nevyužitých portech

3.25 Je povolena komunikace na rozhraní loopback?

*iptables -A INPUT -i lo -j ACCEPT*

*iptables -A OUTPUT -i lo -j ACCEPT*

ano

3.26 a) V případě veřejných adres v DMZ je prováděn NAT pro LAN na externím rozhraní firewallu i na rozhraní DMZ?

*iptables -t nat -s \$LAN -o \$EXT\_IF -A POSTROUTING -j MASQUERADE*

*iptables -t nat -s \$LAN -o \$DMZ\_IF -A POSTROUTING -j MASQUERADE*

není dostupné

3.26 b) V případě privátních adres v DMZ je prováděn NAT na externím rozhraní firewallu pro obě sítě ?

*iptables -t nat -o \$EXT\_IF -A POSTROUTING -j MASQUERADE*

ano

3.27 Je povolena zpětná komunikace, tj. povolení navázaných spojení?

*iptables -A FORWARD -i \$EXT\_IF -o \$LAN\_IF -m state --state ESTABLISHED, RELATED*

*iptables -A FORWARD -i \$DMZ\_IF -o \$LAN\_IF -m state --state ESTABLISHED, RELATED*

*iptables -A INPUT -m state --state ESTABLISHED, RELATED*

ano

3.28 Které služby jsou při přístupu na firewall blokovány?

*iptables -A INPUT -i \$ANY\_IF -p \$PACKET\_TYPE --dport \$PORT -j DROP*

*iptables -A INPUT -p icmp -m icmp --icmp-type \$Nr -j DROP*

nejsou vyžadovány přímo zakazující pravidla

3.29 Na vstupu jednotlivých rozhraní je povolena komunikace pouze pro požadované služby poskytované firewalllem?

*iptables -A INPUT -i \$ANY\_IF -p \$PACKET\_TYPE --dport \$PORT -j ACCEPT*

*iptables -A INPUT -p icmp -m icmp --icmp-type \$Nr -j ACCEPT*

ne, ale je možné ponechat

LAN, DMZ, WAN: SSH(tcp 22), ping(icmp echo), ping(Source quench)

3.30 Které služby jsou zakázány z Lan do vnější sítě?

*iptables -A FORWARD -i \$LAN\_IF -o \$EXT\_IF -p \$PACKET\_TYPE --dport \$port -j DROP*

*iptables -A FORWARD -i \$LAN\_IF -o \$EXT\_IF -p icmp -m icmp --icmp-type \$Nr -j DROP*

nejsou vyžadovány přímo zakazující pravidla

3.31 Jsou povoleny pouze specifické služby (porty) vnější sítě pro LAN? (připojení na internet)

*iptables -A FORWARD -i \$LAN\_IF -o \$EXT\_IF -p \$PACKET\_TYPE --dport \$port -j ACCEPT*

*iptables -A FORWARD -i \$LAN\_IF -o \$EXT\_IF -p icmp -m icmp --icmp-type \$Nr -j ACCEPT*

ne – povoleny všechny porty

3.32 Které služby jsou zakázány z Lan do DMZ?

```
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE --dport $port -j DROP
```

```
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j DROP
```

nejsou vyžadovány přímo zakazující pravidla

3.33 Jsou povoleny pouze požadované služby (porty) poskytované servery v DMZ síti pro LAN?

```
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p $PACKET_TYPE --dport $port -j ACCEPT
```

```
iptables -A FORWARD -i $LAN_IF -o $DMZ_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT
```

ano – omezení na cílový dmz server a cílový port

dmz\_server – povolené služby

192.168.10.20 - HTTP(tcp 80),HTTPS(tcp 443)

192.168.10.30 - HTTP(tcp 80), HTTPS(tcp 443), SMTP(tcp 25), SMTPS(tcp 465),POP3(tcp 110), POP3S (tcp 993), IMAP (tcp 143), IMAPS(tcp 995)

dmz síť - ping(icmp echo)

3.34 Které služby jsou zakázány z DMZ do Wan?

```
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE --dport $port -j DROP
```

```
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j DROP
```

nejsou vyžadovány přímo zakazující pravidla

3.35 Jsou povoleny pouze požadované služby (porty) vnější síť pro DMZ? (připojení na internet)

```
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p $PACKET_TYPE --dport $port -j ACCEPT
```

```
iptables -A FORWARD -i $DMZ_IF -o $WAN_IF -p icmp -m icmp --icmp-type $Nr -j ACCEPT
```

ne, povoleny všechny porty

3.36 a) V případě veřejných adres v DMZ je prováděn forward pro poskytované služby.

```
iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p $PACKET_TYPE --dport $PORT -j ACCEPT
```

```
iptables -A FORWARD -i $EXT_IF -d $IP_SERVER -p icmp -m icmp --icmp-type $Nr -j ACCEPT
```

není dostupné

3.36 b) V případě privátních adres v DMZ je prováděn překlad adres a forward pro poskytované služby?

```
iptables -A PREROUTING -d $PUBLIC_IP_DMZSERVER -i $EXT_IF -j DNAT --to-destination $PRIVATE_IP_DMZSERVER
```



```
iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p $PACKET_TYPE --  
dport $PORT -j ACCEPT
```

```
iptables -A FORWARD -i $EXT_IF -d $PRIVATE_IP_DMZSERVER -p icmp -m icmp --  
icmp-type $Nr -j ACCEPT
```

překlad adres pouze pro dané služby (nemapované porty jsou vyřízeny firewallem), forward omezení na cílový server a cílový port, icmp není poskytován (neprovádí překlad adres, odezva je vyřízena firewallem)

dmz\_server – povolené služby

192.168.30.20 - HTTP(tcp 80),HTTPS(tcp 443)

192.168.30.30 - HTTP(tcp 80), HTTPS(tcp 443), SMTP(tcp 25), SMTPS(tcp 465),POP3 (tcp 110), POP3S (tcp 993), IMAP (tcp 143), IMAPS(tcp 995)

3.37 Je povolena zpětná komunikace pro daný server v DMZ poskytující služby?

```
iptables -A FORWARD -s $IP_SERVER -p $PACKET_TYPE -m state --state ESTABLISHED,  
RELATED -j ACCEPT
```

ano z konkrétního IP daného serveru

3.38 Je prováděno logování paketů před konečným zahozením v INPUT, OUTPUT i FORWARD tabulce?

ano

3.39 Dochází ke vzájemné kolizi pravidel?

ano

```
-A FORWARD -i eth1 -j forward_dmz
```

```
-A forward_dmz -i eth2 -o eth0 -m state --state NEW,RELATED,ESTABLISHED -j  
ACCEPT
```

poznámka: pravidlo obsahuje pokaždé jiný vstupní interface – kolize existuje i pro další zóny

3.40 Jsou některá pravidla nadbytečná?

```
-A forward_dmz -d 192.168.10.20/32 -p tcp -m tcp --dport 80 -j ACCEPT
```

poznámka: uvedená IP je v zóně – existuje i pro další cílové IP adresy z rozsahu 192.168.10.0/24

```
-A forward_ext -s 192.168.10.20/32 -p tcp -m state --state RELATED,ESTABLISHED -j  
ACCEPT
```

poznámka: uvedená IP je v jiné zóně – existuje i pro další zdrojové IP adresu z rozsahu 192.168.10.0/24

```
-A forward_int -s 192.168.10.30/32 -p tcp -m state --state RELATED,ESTABLISHED -j  
ACCEPT
```

poznámka: uvedená IP je v jiné zóně – existuje i pro další zdrojové IP adresu z rozsahu 192.168.10.0/24

```
-A forward_dmz -p icmp -m state --state ESTABLISHED -m icmp --icmp-type 0 -j ACCEPT
```

poznámka: existuje pravidlo povolující related i established

```
-A forward_dmz -p icmp -m state --state RELATED,ESTABLISHED -m icmp --icmp-type 3  
-j ACCEPT
```

poznámka: pravidlo povoluje zpětné navázané spojení, pro která neexistují pravidla umožňující spojení navázat – existuje i pro ostatní ICMP typy (kromě icmp 0) a pro zónu forward\_int ( včetně icmp 0)

## **4 Kontrola údržby a monitorování**

### **4.1 Kontrola údržby - záznamy, procedury**

4.1.1 Jsou vedeny záznamy o haváriích HW a výpadcích firewallu?

není dostupné

4.1.2 Jsou vedeny záznamy o reinstalacích, restartech a obnovách ze záloh?

není dostupné

4.1.3 Jsou vedeny záznamy o provedených zálohách?

není dostupné

4.1.4 Jsou zálohy správně vytvořeny? (zda jsou skutečně vytvořeny při automatických zálohách)

není dostupné

4.1.5 Jsou zálohy pravidelně kontrolovány?

není dostupné

4.1.6 Jsou vytvořeny procedury schvalování pro změny konfigurací firewallu?

není dostupné

4.1.7 Jsou vedeny záznamy změn konfigurací firewallu?

není dostupné

4.1.8 Jsou vedeny záznamy o bezpečnostních incidentech?

není dostupné

4.1.9 Jsou vytvořeny procedury reakcí na bezpečnostní incidenty?

není dostupné

### **4.2 Monitorování, logování**

4.2.1 Je zavedeno monitorování firewallu? (status, bezpečnostní incidenty, zasílání upozornění apod.)

ne

4.2.2 Je prováděno logování firewallu?

ano

4.2.3 Jsou logovány veškeré útoky a užitečné informace firewallu?

ano

4.2.4 Je míra logování přiměřená?

ano

4.2.5 Jsou logovací soubory zálohovány?

není dostupné

4.2.6 Je prováděna pravidelná kontrola logů?

není dostupné

Jméno auditora:.....

Datum:.....

Převzal:.....

Datum:.....