Fortinet / FortiGate – převod poznámek z Juniper ScreenOS a Junos SRX do FortiOS

Table of Contents

Fortinet / FortiGate – převod poznámek z Juniper ScreenOS a Junos SRX do FortiOS....1
1. Základní orientace: ScreenOS / Junos / FortiOS....2
2. HA – obdoba Junos Chassis Cluster / JSRP....3
2.1 Architektura a základní konfigurace....3
2.2 Ověření stavu clusteru....3
2.3 Správa jednotlivých uzlů....4
2.4 Failover a troubleshooting....4
2.5 Přehled tvých HA KB a jejich náhrad....5
3. NAT – obdoba SRX NAT a ScreenOS MIP/VIP/DIP....5
3.1 Převod ScreenOS a SRX NAT....6
3.2 Běžný Source NAT....6
3.3 Destination NAT – publikování serveru....6
3.4 Central SNAT....7
3.5 Persistent NAT, port preservation, full cone....8
3.6 Hairpin NAT – přístup na vlastní veřejnou IP zevnitř....8
3.7 Jak ověřit NAT na živém provozu....8
3.8 Nejvýznamnější náhrada Junos flow traceoptions....9
3.9 Převod zbývajících NAT KB....9
4. Logování – náhrada Juniper syslog, security log a NSM logů....10
4.1 Syslog server....10
4.2 Traffic logging....10
4.3 Prohlížení logů v CLI....11
4.4 FortiAnalyzer....11
4.5 Převod KB....11
5. SNMP – odpovídající nastavení FortiGate....12
5.1 Zapnutí SNMP agenta....12
5.2 SNMPv3....12
5.3 SNMP u HA clusteru....12
5.4 Čím nahradit původní SNMP KB....13
6. NSM – náhrada v prostředí Fortinet....13
6.1 Připojení FortiGate k FortiManageru....13
6.2 FortiManager – interní diagnostika....13
6.3 Backup databáze FortiManageru....14
6.4 FortiAnalyzer – logy a databáze....14
6.5 Převod historických NSM KB....15
7. Praktické CLI – převod tvých ScreenOS příkazů....16
7.1 Konfigurace, informace o systému a soubory....16
7.2 SCP přímo z Linuxu....16
7.3 Systémový stav a hardware....17
7.4 Administrace, SSH, bezpečnost managementu....17
7.5 Interface management....18
7.6 Routing....18
7.7 Address objekty a firewall policies....19
7.8 NTP a systémový čas....19
7.9 DNS a DHCP....20

7.10 IPsec VPN....20
7.11 Packet capture a debug....21
7.12 Co ze ScreenOS nemá smysl převádět doslova....21
8. Bonus: FortiOS CLI, které se vyplatí znát....21
Praktický diagnostický tahák....22
9. Co bych používal jako náhradu za tvou sbírku Juniper KB....22

Aktualizováno k 31. 10. 2026. Jako referenční základ používám především FortiOS 7.6.x, včetně dokumentace 7.6.6. Některé příkazy fungují i na starších verzích 7.2/7.4, ale syntaxe, dostupné parametry a chování se mohou lišit podle modelu, verze a konfigurace VDOM.

Tvoje poznámky pokrývají prakticky celý životní cyklus firewallu: od HA přes NAT a troubleshooting až po centralizovanou správu. Proto zachovám jejich tematické rozdělení a doplním konkrétní příkazy, příklady, diagnostiku i odkazy na dokumentaci.

1. Základní orientace: ScreenOS / Junos / FortiOS

Nejdříve několik důležitých rozdílů.

Juniper / NetScreen	**Fortinet / FortiGate**
`ScreenOS get config`	`show`
`Junos show configuration`	`show`
`Junos show configuration ... | display set`	`show a hierarchické config`
`get system`	`get system status`
`ScreenOS get session`	`diagnose sys session list`
`SRX show security flow session`	`diagnose sys session list`
`SRX show chassis cluster status`	`get system ha status`
`SRX show security nat ...`	`show firewall vip, show firewall ippool, diagnostika sessions`
`ScreenOS get route`	`get router info routing-table all`
`SRX show route`	`get router info routing-table all`
`SRX monitor traffic`	`diagnose sniffer packet`
`SRX traceoptions`	`diagnose debug flow`
`Juniper NSM`	`FortiManager + FortiAnalyzer`
`SRX logical systems / ScreenOS VSYS`	`FortiOS VDOM`
`Junos commit confirmed`	`FortiOS cfg-save revert + execute cfg save`

FortiOS má tři hlavní skupiny příkazů:

- `get` – informace o provozním stavu a vybraných nastaveních.
- `show` – výpis konfigurace, zpravidla bez výchozích hodnot.
- `diagnose` – detailní diagnostika, tabulky sessions, HA, debug a interní stav.

Důležitá odlišnost: FortiOS standardně ukládá změny automaticky. Není tu běžný mechanismus `commit` jako v Junos. Režim ukládání je ale možné změnit:

```
config system global
    set cfg-save automatic
end
```

Případně nastavit `manual` nebo `revert`, kdy se neuložené změny po uplynutí časového limitu vrátí zpět. Potvrzení se provádí `execute cfg save`. zdroj

2. HA – obdoba Junos Chassis Cluster / JSRP

2.1 Architektura a základní konfigurace

U FortiGate se nejčastěji používá FGCP (FortiGate Clustering Protocol).

Juniper SRX	FortiGate
Chassis Cluster	FGCP HA cluster
Node 0 / Node 1	Primary / Secondary
Redundancy group 0	Částečně odpovídá primární řídicí roli HA
Redundancy group 1+	Neexistuje přímý ekvivalent v běžném FGCP A-P
Control link	Heartbeat links
Fabric link	Heartbeat + session synchronization
reth interface	Sdílené clusterové rozhraní
fxp0	Management / HA reserved management interface
Node priority	HA priority
Interface monitoring	HA monitored interfaces

Pozor na odlišnost od SRX: standardní FortiGate A-P cluster není tvořen samostatnými redundancy groups pro jednotlivá rozhraní. V běžném FGCP A-P se přepíná primární jednotka clusteru. Existují také režimy A-A a virtual clustering.

Základní HA konfigurace může vypadat takto:

```
config system ha
    set group-name "FGT-CLUSTER"
    set mode a-p
    set group-id 10
    set password <ha-secret>
    set hbdev "port3" 100 "port4" 50
    set priority 200
    set override disable
    set monitor "port1" "port2"
    set session-pickup enable
end
```

Na druhém zařízení se používá odpovídající konfigurace, ale typicky jiná priorita, například `100`.

`hbdev` určuje heartbeat rozhraní a jejich relativní preference. `monitor` nastavuje sledovaná produkční rozhraní. `session-pickup` umožňuje synchronizaci podporovaných provozních sessions; není standardně zapnuté a má omezení například pro proxy-based inspekci. HA selection Failover

2.2 Ověření stavu clusteru

Tohle je přímá obdoba tvých KB15439, KB20672, KB20673 a souvisejících troubleshooting článků.

```
get system ha status
diagnose sys ha status
diagnose sys ha checksum cluster
diagnose sys ha history read
```

Jednotlivé příkazy odpovídají na různé otázky:

Otázka	**Příkaz**
Kdo je Primary a Secondary?	get system ha status
Je cluster zdravý?	diagnose sys ha status
Jsou konfigurace	diagnose sys ha checksum cluster

synchronizované?	
Co se historicky přepínalo?	diagnose sys ha history read
Jaká je HA konfigurace?	show system ha
Jaký je detail heartbeat?	diagnose sys ha status

V `get system ha status` je zvlášť užitečná část `Primary selected using`, která vysvětluje, proč byla zvolena konkrétní primární jednotka. Synchronizační stav najdeš v `Configuration Status`. HA selection HA status

2.3 Správa jednotlivých uzlů

Ekvivalent přístupu na konkrétní node:

```
execute ha manage 1 admin
```

Index uzlu si ověř ve výpisu HA statusu. Přístup takto funguje i bez individuální IP adresy každého uzlu.

Pro samostatnou správu přes síť slouží HA reserved management interfaces, tedy nejbližší analogie SRX `fxp0`.

```
config system ha
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "mgmt"
            set dst 192.0.2.0/24
            set gateway 192.0.2.1
        next
    end
    set ha-direct enable
end
```

`dst` a `gateway` zde řeší směrování managementu, nikoli přidělení IP adresy rozhraní. IP samotného management interface se nastavuje samostatně na jednotlivých uzlech; jeho konfigurace se mezi uzly nesynchronizuje.

`ha-direct` dovoluje vybraným službám, například logování a SNMP, komunikovat přes individuální management interface. To je důležité zejména u samostatného management VLAN.

2.4 Failover a troubleshooting

```
# Historie clusteru
diagnose sys ha history read

# Porovnání konfigurací
diagnose sys ha checksum cluster

# Diagnostika HA komunikace
diagnose debug reset
diagnose debug application hatalk -1
diagnose debug application hasync -1
diagnose debug enable

# Ukončení diagnostiky
diagnose debug disable
diagnose debug reset
```

Ruční přepnutí primárního uzlu:

```
execute ha failover set
```

Kontrola vynuceného stavu:

```
execute ha failover status
```

Odstranění vynuceného stavu:

```
execute ha failover unset
```

Upozornění: `set` provádí failover a `unset` může vyvolat další přepnutí, protože vrací rozhodování na standardní HA kritéria. Jsou to provozně rizikové příkazy. CLI cheat sheet execute HA

2.5 Přehled tvých HA KB a jejich náhrad

Původní KB	Fortinet – kde hledat
KB13428, KB16141 – podpora a požadavky clusteru	FGCP HA requirements, HA compatibility
KB15356, KB15504 – přiřazení portů a nastavení	FGCP HA configuration, heartbeat interfaces
KB15439 – kontrola clusteru	get system ha status
KB17161, KB21113, KB22431 – management konkrétních uzlů	HA reserved management interfaces
KB17410 – kopírování mezi uzly	Synchronizace HA; pro nezávislé soubory záloha/obnova
KB19938, KB20554, KB22679 – upgrade, obraz systému	HA firmware upgrade, secondary image, backup/restore
KB20641, KB20672, KB20697 – cluster nenaběhne	HA status, history, hatalk/hasync debug
KB20673 – správná priorita	HA primary selection criteria
KB20687, KB23862 – fabric monitoring	Heartbeat monitoring, session synchronization
KB20861, KB20987 – failover redundancy groups	FGCP failover a interface monitoring
KB21050 – logy clusteru	FortiAnalyzer/syslog + HA direct
KB21647 – fronty RETH	QoS, traffic shaping, platformové limity

Odkazy, které mají pro HA největší praktickou hodnotu:

- Fortinet – HA reserved management interfaces
- Fortinet – HA primary selection criteria
- Fortinet – execute ha CLI reference
- Fortinet – HA checksum troubleshooting

3. NAT – obdoba SRX NAT a ScreenOS MIP/VIP/DIP

Tady je důležité pochopit, že FortiOS má dva způsoby organizace NAT:

1. Policy NAT – SNAT je součástí firewall policy, DNAT se typicky řeší objektem VIP.
2. Central NAT – SNAT je spravován samostatnou tabulkou `central-snat-map`; DNAT pomocí VIP objektů oddělených od firewall policy.

Central NAT není standardně zapnutý. Fortinet potvrzuje, že po jeho aktivaci se SNAT už nekonfiguruje běžným přepínačem NAT ve firewall policy.

3.1 Převod ScreenOS a SRX NAT

Juniper / ScreenOS	FortiOS
Source NAT interface	set nat enable ve firewall policy
Source NAT pool	config firewall ippool
Source NAT rule-set	config firewall central-snat-map
Destination NAT	config firewall vip
ScreenOS VIP	FortiGate VIP
ScreenOS MIP / statický 1:1 NAT	VIP + vhodně nastavený SNAT
ScreenOS DIP	IP Pool
Source NAT bez PAT	IP Pool typu One-to-One nebo Fixed Port Range dle účelu
Source port preservation	set port-preserve enable
Proxy ARP pro překládanou IP	set arp-reply enable u VIP/IP Pool
NAT loopback	Hairpin NAT
Persistent / cone NAT	Full cone NAT / endpoint-independent filtering v podporovaných režimech

3.2 Běžný Source NAT

Nejjednodušší příklad firewall policy, která povolí komunikaci z LAN do internetu a zároveň provádí SNAT na adresu odchozího rozhraní:

```
config firewall policy
    edit 10
        set name "LAN-to-WAN"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
        set logtraffic all
    next
end
```

Pokud místo IP rozhraní potřebuješ konkrétní veřejnou IP, vytvoříš IP Pool:

```
config firewall ippool
    edit "PUBLIC-NAT"
        set type overload
        set startip 203.0.113.10
        set endip 203.0.113.10
    next
end
```

A ve firewall policy:

```
config firewall policy
    edit 10
        set ippool enable
        set poolname "PUBLIC-NAT"
    next
end
```

3.3 Destination NAT – publikování serveru

Například veřejná adresa `203.0.113.20:443` na interní server `10.0.1.20:443`.

```
config firewall vip
    edit "WEB-HTTPS"
        set extintf "wan1"
        set extip 203.0.113.20
        set mappedip "10.0.1.20"
        set portforward enable
        set protocol tcp
        set extport 443
        set mappedport 443
        set arp-reply enable
    next
end
```

Firewall policy:

```
config firewall policy
    edit 20
        set name "WAN-to-WEB"
        set srcintf "wan1"
        set dstintf "lan"
        set srcaddr "all"
        set dstaddr "WEB-HTTPS"
        set action accept
        set schedule "always"
        set service "HTTPS"
        set logtraffic all
    next
end
```

Důležitý rozdíl proti běžným address objektům: VIP obsahuje externí a interní adresu a při standardním policy NAT režimu se používá jako destination objekt firewall policy.

`set arp-reply enable` pomůže, pokud má firewall na příslušné L2 síti odpovídat na ARP pro externí IP. Není to ale univerzální náhrada správného routingu veřejného prefixu. config VIPs 2

3.4 Central SNAT

Příklad pravidla:

```
config system settings
    set central-nat enable
end
```

```
config firewall central-snat-map
    edit 1
        set srcintf "lan"
        set dstintf "wan1"
        set orig-addr "all"
        set dst-addr "all"
        set nat enable
        set nat-ippool "PUBLIC-NAT"
    next
end
```

Tato varianta bude pro někoho zvyklého na samostatné NAT rule-sety v Junos možná přirozenější než NAT v jednotlivých bezpečnostních policies.

Pozor: přepnutí existujícího produkčního firewallu mezi policy NAT a central NAT vyžaduje pečlivé ověření konfigurace.

3.5 Persistent NAT, port preservation, full cone

Ve tvých poznámkách jsou zejména KB19459, KB20711, KB21296 a KB22059.

FortiOS rozlišuje:

- `port-preserve` – zachování původního zdrojového portu, pokud je dostupný.
- `fixedport` – striktnější zachování původního portu ve vhodném policy NAT scénáři.
- Fixed Port Range IP Pool – řízené přidělování překládaných portů.
- Full cone NAT – umožní v podporovaném režimu přístup z dalších externích adres na již existující UDP mapování.

Ve FortiOS 7.6.6 je zdokumentováno:

```
config firewall ippool
    edit "FPR-POOL"
        set type fixed-port-range
        set permit-any-host enable
    next
end
```

Jde pouze o ukázku relevantních voleb, nikoli kompletní konfiguraci IP Poolu.

Full cone prostřednictvím `permit-any-host` je zde podporováno pro UDP, nikoli obecně pro všechny protokoly. Přesná náhrada SRX Persistent NAT tedy závisí na požadovaném chování mapování a filtrování. SNAT cone nat

3.6 Hairpin NAT – přístup na vlastní veřejnou IP zevnitř

Obdoba tvých KB17448 a KB19400.

Typický případ: klient `10.0.1.50` chce otevřít `203.0.113.20`, které DNATem vede na server `10.0.1.20`.

FortiGate podporuje Hairpin NAT. Obvykle potřebuješ VIP, odpovídající LAN-to-LAN policy, případně také SNAT, jestliže klient a server jsou ve stejné podsíti a odpověď by jinak obešla firewall.

Pozor také na `extintf` VIP objektu: pokud je omezeno na `wan1`, nemusí VIP odpovídat interně příchozím paketům tak, jak očekáváš. Fortinet má pro různé scénáře samostatné konfigurace.

Fortinet – Hairpin NAT

3.7 Jak ověřit NAT na živém provozu

Toto je náhrada především KB10139, KB16252, KB21611, KB21719, KB21757 a KB21839.

```
# NAT konfigurace
show firewall vip
show firewall ippool
show firewall central-snat-map
show firewall policy

# Stav session tabulky
diagnose sys session stat

# Filtr podle klienta
diagnose sys session filter clear
diagnose sys session filter src 10.0.1.50
diagnose sys session list
```

Filtr podle přeložené source IP:

```
diagnose sys session filter clear
diagnose sys session filter nsrc 203.0.113.10
diagnose sys session list
```

Výpis session umožňuje zjistit původní i překládané adresy a porty, policy ID, stav TCP a další interní informace.

Mazání sessions vyžaduje opatrnost:

```
diagnose sys session filter clear
diagnose sys session filter src 10.0.1.50
diagnose sys session clear
diagnose sys session filter clear
```

Příkaz `session clear` maže sessions odpovídající aktuálnímu filtru. Pokud žádný filtr nezůstane aktivní, můžeš přerušit mnohem více provozu, než zamýšlíš. using sess diag sys

3.8 Nejvýznamnější náhrada Junos flow traceoptions

FortiGate `diagnose debug flow`.

```
diagnose debug disable
diagnose debug reset
diagnose debug flow filter clear

diagnose debug flow filter saddr 10.0.1.50
diagnose debug flow filter daddr 8.8.8.8
diagnose debug flow filter proto 6

diagnose debug flow show function-name enable
diagnose debug flow trace start 100
diagnose debug enable
```

Po dokončení:

```
diagnose debug flow trace stop
diagnose debug disable
diagnose debug reset
```

Uvidíš například přijetí paketu, routing lookup, policy match, výběr NAT a drop reason.

Je ale potřeba počítat s tím, že provoz offloadovaný přes NP6/NP7 nemusí být v běžném flow debug viditelný. Při diagnostice je vhodné rozlišovat CPU processing a hardware offload.

Fortinet Document Library

Pro rychlý test konkrétního policy match:

```
diagnose firewall iprope lookup \
  10.0.1.50 12345 8.8.8.8 443 6 lan
```

Zpětné lomítko je tu pouze pro přehlednost; ve FortiOS CLI zadej příkaz na jeden řádek.

Tento nástroj vrací odpovídající policy ID, ale skutečný provoz a jeho případné další kontroly je vhodné ověřit pomocí flow debug. policy lookup

3.9 Převod zbývajících NAT KB

Původní KB	Fortinet – odpovídající téma
TN81, TN25, KB15758	Source NAT, Destination NAT, VIP, IP Pools
KB13427, KB14194	Maximum Values Table, počet sessions, NAT port

	allocation
KB16710, KB21872	Firewall policy, local-in policy, policy counters
KB17525	NAT v IPsec policies / route-based IPsec
KB17855	NAT při HA failover, session pickup
KB19459	DNS helper/ALG a NAT chování
KB20711, KB21296	Port preservation, Full Cone NAT
KB21547, KB21697	Transparent/NAT mode, packet processing
KB21709, KB21783	Pořadí firewall policies a Central SNAT
KB21785, KB24709	VIP/IP Pool arp-reply
KB21886, KB21918	DNAT VIP, session a debug flow
KB22059, KB22178	Security profiles, ALG, IPsec NAT-T

Limity NAT pravidel a sessions nejsou jedno univerzální číslo. Závisí na platformě, typu IP Poolu a způsobu alokace portů.

U IPsec je nutné odlišovat dvě věci: NAT provozu přenášeného tunelem a NAT Traversal samotného IPsecu, tj. UDP zapouzdření ESP. FortiOS pro NAT-T používá `set nattraversal enable` v Phase 1. [phase 1]

Hlavní dokumenty:

- Fortinet – Source NAT
- Fortinet – Destination NAT
- Fortinet – Central SNAT
- Fortinet – Full Cone NAT
- Fortinet – Debugging packet flow

4. Logování – náhrada Juniper syslog, security log a NSM logů

Tvoje KB16224, KB16448, KB16502, KB16509 a KB16643 odpovídají především nastavení syslogu, traffic loggingu a FortiAnalyzeru.

4.1 Syslog server

Příklad odesílání syslogu do vlastního Linux serveru na `192.0.2.100`:

```
config log syslogd setting
    set status enable
    set server "192.0.2.100"
    set port 514
    set mode udp
    set format rfc5424
end
```

FortiOS umožňuje také TCP transport (`reliable`) a různé formáty včetně CEF a JSON. Je potřeba odlišit spolehlivý transport od garantovaného doručení a dlouhodobého uložení logů.

Na samostatných zařízeních můžeš využít více syslog destinací (`syslogd`, `syslogd2` atd.). [log]

4.2 Traffic logging

U jednotlivých pravidel:

```
config firewall policy
    edit 10
        set logtraffic all
    next
end
```

Pro logování provozu směřujícího přímo na FortiGate (management, DNS, NTP apod.) existují samostatná nastavení local-in traffic logging.

V novějších FortiOS 7.6 lze logovat také jednotlivé local-in policies:

```
config log setting
    set local-in-policy-log enable
end
```

A v příslušné local-in policy `set logtraffic enable`. local traffic

4.3 Prohlížení logů v CLI

Velice praktická náhrada ScreenOS `get log event`:

```
execute log filter device disk
execute log filter category event
execute log filter field action login
execute log display
```

Tohle konkrétně filtruje přihlášení administrátorů z lokálních event logů na disku.

Podle hardwaru a konfigurace může být dostupné jiné úložiště logů, případně jen vzdálený FortiAnalyzer/syslog. log commands

4.4 FortiAnalyzer

```
config log fortianalyzer setting
    set status enable
    set server "192.0.2.110"
    set upload-option realtime
end
```

FortiAnalyzer slouží zejména ke sběru, archivaci, vyhledávání, reportování a analýze logů.

Pokud používáš HA, ověř také, zda chceš logy posílat pod identitou clusteru, nebo každého jednotlivého uzlu. K tomu slouží mimo jiné `ha-direct`, individuální management IP a odpovídající nastavení logovací služby.

4.5 Převod KB

Juniper KB	Odpovídající Fortinet funkce
KB16224 – syslog do STRM	FortiGate syslog → SIEM
KB16448, KB16643 – logy do NSM	FortiAnalyzer logging
KB16502 – system logging	config log ...
KB16509 – traffic logging	set logtraffic all
KB21450 – duplicates	Log filters, deduplikace na příjemci
KB21501 – hostname v HA logu	Identita HA uzlu, SN a source IP
KB22193 – chybný timestamp	NTP, timezone, zdrojový a přijímací timestamp
KB22281 – log rotation	Disk logging, retention, log rolling

Dokumentace: Fortinet – Log settings and targets

5. SNMP – odpovídající nastavení FortiGate

5.1 Zapnutí SNMP agenta

```
config system snmp sysinfo
    set status enable
    set description "FortiGate firewall"
    set location "DC Praha"
    set contact-info "noc@example.net"
end
```

SNMP musí být zároveň povoleno na management rozhraní.

```
config system interface
    edit "mgmt"
        append allowaccess snmp
    next
end
```

Používám `append`, protože nechci nechtěně zrušit existující povolené protokoly, například SSH a HTTPS.

5.2 SNMPv3

Doporučený výchozí režim je `auth-priv`.

```
config system snmp user
    edit "monitoring"
        set status enable
        set security-level auth-priv
        set auth-proto sha256
        set auth-pwd <auth-password>
        set priv-proto aes
        set priv-pwd <privacy-password>
        set queries enable
    next
end
```

Zde je dobré ověřit kompatibilitu zvolených algoritmů se SNMP managerem. FortiOS podporuje několik SHA variant a několik privacy algoritmů. snmp basic config snmp

5.3 SNMP u HA clusteru

Tohle je zajímavý ekvivalent KB12142.

Pokud chceš v Zabbixu sledovat každou fyzickou jednotku samostatně, používej raději její individuální HA management IP.

Pro SNMPv3 u konkrétního uživatele:

```
config system snmp user
    edit "monitoring"
        set ha-direct enable
    next
end
```

A samozřejmě odpovídající HA management nastavení.

Fortinet upozorňuje, že samostatný přístup přes reserved management interfaces a společná identita clusteru nejsou totéž. oob ha

5.4 Čím nahradit původní SNMP KB

Původní KB	Fortinet
KB12142 – CPU v HA	SNMP MIB + individuální HA management
KB16545 – SNMP Agent	config system snmp sysinfo
KB20788 – změna ifDescr	SNMP interface index, snmp-index, MIB
KB22048 – SNMPv3	config system snmp user

Kromě standardních interface counterů je vhodné využívat vlastní Fortinet MIB, která pokrývá také HA, stav VPN, sessions, CPU, paměť a další provozní parametry.

FortiGate SNMP implementace je určena pro čtení a traps, nikoli pro konfiguraci pomocí SNMP SET.

Dokumentace: Fortinet – SNMP Administration Guide snmp sum

6. NSM – náhrada v prostředí Fortinet

Tvoje rozsáhlá sekce NSM se týká nejen konfigurace zařízení, ale také správy celé infrastruktury, databáze, procesů, logování a řešení chyb centralizovaného managementu.

Tady je zásadní rozdíl: místo jednoho historického NSM má Fortinet dvě hlavní samostatné komponenty:

FortiManager

Správa konfigurací, zařízení, firewall policies, policy packages, ADOM, revizí, skriptů a firmware.

FortiAnalyzer

Sběr logů, ukládání dat, vyhledávání, analýza událostí, reporty a audit.

FortiManager může poskytovat také některé analytické a logovací funkce, ale pro rozsáhlejší centralizované logování je vhodné samostatné FortiAnalyzer prostředí.

6.1 Připojení FortiGate k FortiManageru

Na FortiGate:

```
config system central-management
    set type fortimanager
    set fmg 192.0.2.120
end
```

Následně ověřit registraci a schválení zařízení na FortiManageru.

```
get system central-management
diagnose fdsm central-mgmt-status
```

Podstatné je, že FortiManager používá pro komunikaci s FortiGate protokol FGFM, typicky TCP/541.

Diagnostika dostupnosti:

```
execute ping 192.0.2.120
execute telnet 192.0.2.120 541
get router info routing-table details 192.0.2.120
```

Dokumentace rozlišuje stavy, kdy je spojení navázané, ale zařízení dosud není schválené, a kdy už je plně registrované. config central mgmt

6.2 FortiManager – interní diagnostika

Teď se dostáváme k období NSM backendu.

Přímo na FortiManageru:

```
get system status
diagnose sys top
diagnose dvm dbstatus
diagnose dvm device list
```

Pro ladění procesů managementu:

```
diagnose debug application fgfmsd -1
diagnose debug enable
```

A po dokončení:

```
diagnose debug disable
diagnose debug reset
```

Další příkazy FortiManageru:

Co zjišťovat	FortiManager
Stav databáze spravovaných zařízení	diagnose dvm dbstatus
Seznam zařízení	diagnose dvm device list
Informace o uzamčení konfigurace	diagnose dvm device lockinfo
Informace o ADOM	diagnose dvm adom ...
Debug komunikace se zařízením	diagnose debug application fgfmsd
Debug DVM	diagnose dvm debug
Interní servisní diagnostika	diagnose debug service
Kompletní servisní report	execute tac report

Parametry jednotlivých diagnostických příkazů je vhodné ověřovat pomocí `?`, protože se liší podle konkrétní verze FortiManageru. Help 7.6.5 help 7.6.6

6.3 Backup databáze FortiManageru

Ekvivalent NSM KB10375, KB11476, KB12285 a dalších.

```
execute backup all-settings sftp ...
```

Aktuální syntaxe podporuje zálohování konfigurace a databáze na FTP, SCP nebo SFTP.

FortiManager má samostatné příkazy pro další typy dat, například:

```
execute backup all-settings
execute backup fmg-logs
execute backup task
```

Tyto příkazy vyžadují odpovídající argumenty, tedy cíl, název souboru, autentizaci a případné heslo zálohy. Nejsou to samostatně spustitelné příklady. Backup backup config

Fortinet doporučuje zálohovat konfiguraci a databázi před upgrade a kontrolovat integritu zálohy.

6.4 FortiAnalyzer – logy a databáze

Na FortiAnalyzeru:

```
diagnose log device
diagnose fortilogd lograte-adom root
diagnose fortilogd logvol-adom root
```

Poslední dva příkazy jsou určeny pro zjištění rychlosti a objemu logování v ADOM; název `root` je potřeba nahradit správným ADOM.

Jde o obdobu NSM KB11257 – zjištění logging rate.

FortiAnalyzer pracuje s logovými soubory a SQL databází pro vyhledávání a analýzu. Nesnažil bych se jeho interní databázi spravovat ručně jako běžnou PostgreSQL/MySQL instalaci. K těmto účelům poskytuje vlastní administrativní a diagnostické rozhraní. Logs examples

6.5 Převod historických NSM KB

Tady bych tvé původní KB uspořádal do následujících funkčních skupin.

Původní NSM KB	Fortinet – náhrada
KB4394, KB9851 – error logs	FortiManager diagnostics, event logs
KB4503, KB12707 – log management	FortiAnalyzer Log Management
KB4514, KB11731 – migrace databáze	FortiManager system backup/restore
KB4548, KB12367, KB13121 – device connection	FGFM, device authorization, DVM
KB4594 – non-root processes	FortiManager appliance/VM service architecture
KB4649 – email queue	Alert mail settings / diagnostika
KB5096 – verze NSM	get system status
KB7115 – core dump	TAC report, crash diagnostics
KB8580 – SNMP trap při odpojení	SNMP traps, event automation
KB9002, KB14938 – timeout/retry	FGFM diagnostics, management deployment
KB9313, KB11714 – procesy Device Serveru	FortiManager DVM/FGFM process diagnostics
KB9692 – změna IP NSM	System interfaces + FGFM reconnect
KB9840 – debug backendu	diagnose debug application
KB9844 – Java exception	FortiManager task log / application debug
KB10375, KB11476, KB12285 – zálohy	execute backup all-settings
KB11015, KB15196 – automatické zálohy	FortiManager backup, scheduler
KB11016 – GUI/Device Server	FortiManager GUI a backend diagnostics
KB11263 – start/stop procesů	FortiManager process management
KB11267 – interní adresáře	FortiManager internal filesystem/diagnostics
KB11598 – standalone → distributed	FortiManager HA a architektura nasazení
KB11829, KB11830 – procesy a logy	FortiManager process/debug reference
KB12173 – upgrade komponent	FortiManager firmware upgrade
KB12891 – blokované IP	Admin lockout / trusted hosts
KB13523 – upgrade history	Firmware and system event history
KB14868 – export logů	FortiAnalyzer log export
KB15643 – restore z tech-support	Backup/restore, TAC-assisted recovery
KB16166 – packet captures	FortiGate sniffer / FortiAnalyzer data
KB16655, KB17268 – backend errors	Task monitor, application debug
KB17358 – přesun logů	FortiAnalyzer storage and retention
KB21050 – HA cluster logging	HA-direct logging, FortiAnalyzer
KB22703 – doporučené verze	Supported Releases / Upgrade Path / RN

Nejde vždy o funkční ekvivalenty 1:1. Zvláště staré NSM příkazy pracující se soubory Device Serveru nebo přímo s jeho databází nemají obdobu v běžném CLI FortiGate.

Doporučené rozcestníky:

- FortiManager – Debug CLI
- FortiManager – DVM diagnostics
- FortiManager – Backup CLI
- FortiAnalyzer – Log and file storage

7. Praktické CLI – převod tvých ScreenOS příkazů

Tohle je podle mě nejcennější část pro každodenní administraci. Některé staré příkazy nemají přímou obdobu, ale FortiOS má zpravidla jinou cestu ke stejným informacím.

7.1 Konfigurace, informace o systému a soubory

ScreenOS	FortiOS
get config	show
get sys-cfg	show full-configuration a příslušné diagnostické příkazy
get system	get system status
get mem	get system performance status
get db info	diagnose sys session stat a příslušné procesní diagnostiky
get file	execute disk list, dostupné filesystem příkazy
get envar	Bez přímé obecné obdoby
save config to tftp	execute backup config tftp
save software from flash to tftp	Firmware backup/upgrade nástroje; ne obecná kopie firmware z flash
set scp enable	set admin-scp enable
get scp	show full-configuration system global
save config to last-known good	Configuration revisions / záloha
exec config rollback enable	cfg-save revert
reset	execute reboot
get log event	execute log filter, execute log display

Příkazy k zálohování:

```
execute backup config tftp fgt.cfg 192.0.2.100
execute backup full-config tftp full.cfg 192.0.2.100
```

Pro SFTP:

```
execute backup config sftp backup.cfg 192.0.2.100 admin
```

U SFTP je potřeba doplnit autentizační argumenty dle dané verze a serveru.

Rozdíl mezi `backup config` a `backup full-config`: druhá varianta zahrnuje také výchozí konfigurační hodnoty.

A pozor – výstup `show full-configuration` není totéž co obnovitelná záloha obsahující vše potřebné pro úplnou obnovu zařízení. [config mgmt]

7.2 SCP přímo z Linuxu

Na FortiGate:

```
config system global
    set admin-scp enable
end
```

Na příslušném rozhraní musí být povolené SSH.

Z Linuxu potom:

```
scp -O admin@192.0.2.1:sys_config ./fortigate.conf
```

Tady je `-O` důležité: moderní OpenSSH používá pro `scp` standardně SFTP transport, ale FortiGate podporuje pro tento způsob zálohování tradiční SCP protokol.

U obnovení konfigurace existuje cílový název `fgt-restore-config`, ale nahrání na něj může okamžitě restartovat firewall, proto bych ho nezkoušel bez připraveného okna údržby. conf reset

7.3 Systémový stav a hardware

Praktické příkazy:

```
get system status
get system performance status
diagnose sys top
diagnose sys top-all
diagnose hardware sysinfo memory
diagnose hardware sysinfo cpu
diagnose debug crashlog read
diagnose sys flash list
execute disk list
execute tac report
```

Pro rozhraní:

```
get system interface
get system interface physical
diagnose ip address list
diagnose hardware deviceinfo nic port1
get system interface transceiver
```

Některé příkazy mohou být dostupné jen na modelech s odpovídajícím hardwarem. high cpu cli cheats

7.4 Administrace, SSH, bezpečnost managementu

Původní ScreenOS:

`get admin user`, `set admin password`, `set admin manager-ip`, `set admin access attempts`, `set admin port`, `set console timeout`.

FortiOS:

```
show system admin
show system accprofile
show system global
```

Nastavení přístupových portů a lockoutu:

```
config system global
    set admin-sport 32000
    set admin-ssh-port 1024
    set admin-lockout-threshold 2
    set admin-lockout-duration 10800
    set admintimeout 5
end
```

V tomto příkladu je HTTPS na portu 32000, SSH na 1024, zamčení po dvou neúspěšných pokusech na 3 hodiny a neaktivní administrátorská relace končí po 5 minutách.

Změny management portů dělej opatrně, protože se můžeš odříznout od zařízení. Samotná změna portu navíc není náhrada za restrikci zdrojových IP a autentizaci. conf global

Omezení administrátorského přístupu podle IP adresy:

```
config system admin
    edit "admin"
        set trusthost1 192.0.2.0 255.255.255.0
    next
end
```

Na FortiGate je potřeba sledovat také:

- `set accprofile` – oprávnění administrátora.
- `set two-factor` – druhý faktor.
- `set ssh-public-key1` – SSH veřejný klíč.
- `set trusthost1` až `trusthost10` – povolené zdrojové sítě.
- `ip6-trusthost...` – IPv6 varianty.

Trusted hosts jsou omezení zdrojových adres pro administrátora, zatímco `allowaccess` určuje, které služby firewall poslouchá na daném rozhraní. Pro přísnější ochranu managementu existují také local-in policies. conf sys admin

7.5 Interface management

Původní ScreenOS:

```
unset interface untrust manage ping|snmp|telnet
set int tru manage ssh
unset int tru manage telnet
```

FortiOS:

```
config system interface
    edit "port1"
        set allowaccess ping https ssh
    next
end
```

Případně přidání samostatné služby bez změny ostatních:

```
config system interface
    edit "port1"
        append allowaccess snmp
    next
end
```

V prvním případě přepíšeš povolené služby výčtem, ve druhém je rozšíříš.

7.6 Routing

Tady je převod téměř přímočarý.

ScreenOS / SRX	FortiOS
get route	get router info routing-table all
get route v6	get router info6 routing-table
get route prefix A.B.C.D/E	get router info routing-table details A.B.C.D
get route | exclude /32	Výpis + CLI filtr, případně externí zpracování
get route id X	Bez přímé obdoby; podle cíle routing-table/database
get vrouter	show system vdom-property, show system interface, VRF/routing context
set route ... gateway ...	config router static

Příklad statické routy:

```
config router static
    edit 10
        set dst 10.20.0.0 255.255.0.0
        set gateway 192.168.1.1
        set device "port2"
    next
end
```

Ověření:

```
get router info routing-table all
get router info routing-table database
get router info routing-table details 10.20.1.1
```

FortiOS podporuje VDOM i VRF. Proti ScreenOS virtual routers je tedy potřeba rozlišit samotnou izolaci VDOM a samostatné routing tabulky VRF. dyn rioting rout concepts

7.7 Address objekty a firewall policies

Původní ScreenOS:

```
set address V1-trust my-pc 1.1.1.11/32
set policy from V1-trust to V1-untrust ...
```

FortiOS:

```
config firewall address
    edit "my-pc"
        set subnet 10.0.1.11 255.255.255.255
    next
end
```

Policy:

```
config firewall policy
    edit 30
        set name "PC-to-WAN"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "my-pc"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

Pro změnu pořadí pravidel se používá například CLI `move` v kontextu firewall policies. Pořadí je důležité, protože firewall vyhodnocuje policies shora dolů.

7.8 NTP a systémový čas

ScreenOS:

```
set ntp timezone -5
set clock ntp
exec ntp update
```

FortiOS:

```
config system ntp
    set ntpsync enable
```

```
    set type custom
    config ntpserver
        edit 1
            set server "192.0.2.123"
        next
    end
end
```

Časovou zónu nastavuje `config system global` → `set timezone`, ale používá číselné identifikátory zón FortiOS, nikoli jednoduše starý zápis ScreenOS `-5`.

Fortinet Document Library

7.9 DNS a DHCP

Základní DNS:

```
config system dns
    set primary 1.1.1.1
    set secondary 9.9.9.9
end
```

DHCP server:

```
config system dhcp server
    edit 1
        set interface "lan"
        set default-gateway 10.0.1.1
        set netmask 255.255.255.0
        config ip-range
            edit 1
                set start-ip 10.0.1.100
                set end-ip 10.0.1.200
            next
        end
    next
end
```

Ověření lease:

```
execute dhcp lease-list
```

Pro DHCP reservation existuje pod `config system dhcp server` sekce `config reserved-address` pro rezervace podle MAC adres. [ipsec diagf]

7.10 IPsec VPN

Tvoje staré ScreenOS poznámky:

`set ike gateway ...`, `set ike p1-proposal ...`, `get ike p1-sec-level`, `get sa`.

FortiOS ekvivalenty:

```
ScreenOS                FortiOS
set ike gateway         config vpn ipsec phase1-interface
set ike p1-proposal     Phase 1 proposal, dhgrp, keylife
Phase 2 SA              config vpn ipsec phase2-interface
get sa                  diagnose vpn tunnel list
Gateway status          diagnose vpn ike gateway list
```

IKE statistics	diagnose vpn ike status
IKE debug	diagnose debug application ike -1

V současném FortiOS bych pro běžný site-to-site tunel preferoval route-based IPsec a IKEv2, pokud to protistrana umožňuje.

Diagnostické příkazy jsou přímo popsány v Fortinet – IPsec related diagnose commands.

7.11 Packet capture a debug

Tohle je přímá obdoba ScreenOS `snoop filter`, `set ffilter` a `debug flow basic`.

Zachycení provozu:

```
diagnose sniffer packet any \
  'host 10.0.1.50 and tcp port 443' 4 100
```

I zde příkaz zadej ve FortiOS jako jeden řádek.

Význam parametrů:

- `any` – všechna příslušná rozhraní.
- Filtr – výraz kompatibilní s tcpdump/BPF stylem.
- `4` – verbosity zahrnující názvy rozhraní a hlavičky.
- `100` – maximální počet paketů.

Provoz můžeš sledovat současně s `diagnose debug flow`, který ukazuje interní rozhodování firewallu. debug flow

7.12 Co ze ScreenOS nemá smysl převádět doslova

Zbylé položky tvého seznamu:

ScreenOS	Poznámka pro FortiOS
get db stream	Flow debug a specifické procesní debugy
get sys-cfg | inc dbuf	diagnose debug ...
clear dbuf	diagnose debug reset
unset all	V kontextu FortiOS raději cílené unset, delete nebo purge
get console	show system console
set ssl encrypt 3des sha-1	Aktuální TLS / cipher suite nastavení
set flow tcp-syn-check	TCP session validity / DoS / anomaly controls
set interface ... phy link-down	Administrativní stav interface, podle modelu
get zone	show system zone

Zvlášť bych byl opatrný u `purge`, `factoryreset`, formátování disků, mazání sessions a zásahů do systémových databází. Na produkčním firewallu je rozdíl mezi výpisem diagnostiky a změnou stavu zařízení opravdu významný.

8. Bonus: FortiOS CLI, které se vyplatí znát

Fortinet má velmi praktický mechanismus pro procházení vlastního CLI stromu:

```
tree
tree system
tree diagnose
tree execute
```

Tohle je užitečné především tehdy, když zjistíš, že příkaz v KB existuje, ale na tvém konkrétním FortiGate ho nevidíš.

V kontextu příkazu používej `?`. FortiOS se totiž liší podle modelu, zapnutých funkcí a firmware. tahák

Praktický diagnostický tahák

Z těchto příkazů bych si udělal samostatnou základní sadu:

FortiGate – prvních 20 diagnostických příkazů

Pouze čtecí a základní diagnostické příkazy; `debug disable/reset` ukončují či resetují existující debug. Nahraď ukázkové IP a rozhraní.

```
get system status
get system performance status
get system interface physical
get router info routing-table all
get router info routing-table database
get system arp
diagnose hardware deviceinfo nic port1
diagnose sys top
diagnose sys session stat
diagnose sys session filter clear
diagnose sys session list
diagnose sys ha status
get system ha status
diagnose sys ha checksum cluster
diagnose sys ha history read
diagnose vpn ike status
diagnose vpn tunnel list
diagnose sniffer packet any 'host 10.0.1.50' 4 100
diagnose debug disable
diagnose debug reset
```

9. Co bych používal jako náhradu za tvou sbírku Juniper KB

Tvoje původní poznámky jsou typické pro technika, který si buduje vlastní provozní znalostní bázi. Fortinet má poměrně dobrý ekosystém, jen je potřeba vědět, kde hledat.

Zdroj	K čemu se hodí
FortiOS CLI Reference	Přesná syntaxe, parametry, defaulty
CLI Troubleshooting Cheat Sheet	Rychlá provozní diagnostika
FortiOS Administration Guide	Konfigurace a souvislosti
Fortinet Community	Technical Tips, řešení konkrétních problémů
FortiManager dokumentace	Centralizovaná správa
FortiAnalyzer dokumentace	Logování a analýza

Pro vyhledávání v Community se často vyplatí hledat konkrétní řetězec `Technical Tip:` nebo `Troubleshooting Tip:` a problém, například `HA checksum mismatch`, `DNAT policy lookup` nebo `FGFM connection`.

Moje doporučení pro další používání: ponechat si tvé historické Juniper KB jako věcný index problémů, ale vedle nich vést samostatnou FortiOS bázi podle témat, nikoli pouze podle čísel článků. Především bych oddělil konfiguraci, kontrolní příkazy, troubleshooting a rizikové zásahy.

Z praktického hlediska jsou nejdůležitější rozdíly, na které bych se při přechodu z NetScreen/SRX soustředil, FGCP vs. JSRP, Central NAT vs. Policy NAT, VDOM vs. virtual routers, FGFM/FortiManager vs. NSM a FortiOS debug flow vs. Junos traceoptions. Zbytek administrace už bude v mnoha ohledech důvěrně známý.