# Popis stávajícího stavu

## Farmaceutická fakulta UK Hradec Králové (FaF)

### Next Generation FireWall (NGFW) na FaF UK

Na FaF je provozována dvojice NGFW FortiGate 200F s UTP subskripcí (do 5/2027) je umístěna v hlavní serverovně FaF. Internetová konektivita je realizována linkovou agregací 2x 10GE.

Součástí UTP subskripce a platného FortiCare kontraktu je:

* Intrusion Prevention System (IPS)
* Advanced Malware Protection (AMP)
* Web Security
* Inline SaaS Application Security (CASB)
* Application Control
* Inline CASB Database
* Device/OS Detection
* GeoIP Updates
* Trusted Certificate Database
* Internet Service (SaaS) Database
* DDNS (v4/v6)

Více informací je na: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiguard.pdf

FireWally jsou zapojeny redundantně k páteřním přepínačům sítě LAN (linková agregace 2x 10GE) a jsou napojeny na Microsoft Active Directory (3400 uživatelů), které je využito pro nastavení pokročilých UTM pravidel včetně SSO. Jiné externí zdroje identit nejsou využívány.

Na NGFW jsou definovány 3 tzv. virtuální kontexty (plně oddělený virtuální FireWall). Jedná se o kontext vyhrazený pro management a kontexty pro EXTERNÍ (DMZ, videokonference) a INTERNÍ komunikaci.

Celkem je na NGFW udržováno 120+ FW pravidel, 40+ DNAT pravidel se zapnutým NGFW (AV, IPS, inspekce certifikátů), 60+ NGFW pravidel (AV, Web filter, DNS, Aplikační kontrola, inspekce certifikátů), 70+ IPv4/IPv6 pravidel. Je nasazen OSPF směrovací protokol, FSSO a SSL VPN.

Směrování zajišťuje OSPF

Měsíční vytížení boxů je uvedeno v následující tabulce:

Obsah obrázku text, snímek obrazovky, Písmo, číslo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

K ukládání logových informací z FortiGate 200E slouží FortiAnalyzer s kapacitou 6GB logů/den. S průměrným denním vytížením 5-6GB logů/den. FortiAnalyzer má platnou podporu výrobce do 11.9.2027 (SN: FAZ-VM0000111530).

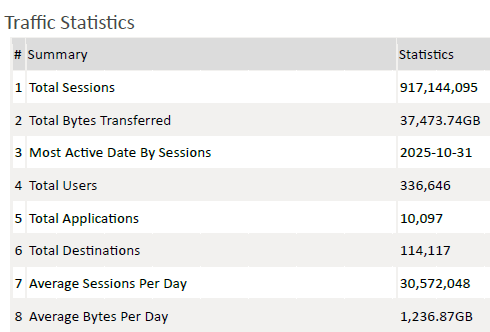
### Next Generation FireWall (NGFW) pro HKNET

Druhá dvojice NGFW FortiGate 300E s UTP subskripcí (do 7/2026) je umístěna v hlavní serverovně FaF.

FireWaly jsou zapojeny v režimu HA, slouží jako perimetrový FW metropolitní sítě HKNET a mají internetovou konektivitu realizovanou linkovou agregací 4x 1GE. Do síťové infrastruktury jsou zapojeny redundantně linkovou agregací 2x 1GE.

Na NGFW je definováno 8 virtuálních kontextů pro různé zóny metropolitní sítě HKNET. Celkem je v těchto kontextech udržováno 20+ VLAN, 30+ FW pravidel a 20+ NGFW pravidel. Je využívána SSL VPN.

Měsíční vytížení boxů je uvedeno v následující tabulce:



K ukládání logových informací slouží FortiAnalyzer s kapacitou 6GB logů/den s průměrným denním vytížením 1-2GB/ logů za den. FortiAnalyzer má platnou podporu výrobce do 11.10.2026 (SN: FAZ-VM0000115164).

## Lékařská fakulta UK Hradec Králové (LF)

Na LF je provozována dvojice NGFW FortiGate 200F s Enterprise subskripcí (do 4/2026) je umístěna v hlavní serverovně LF. Internetová konektivita je realizována linkovou agregací 2x 10GE.

Součástí Enterprise subskripce a platného FortiCare kontraktu je:

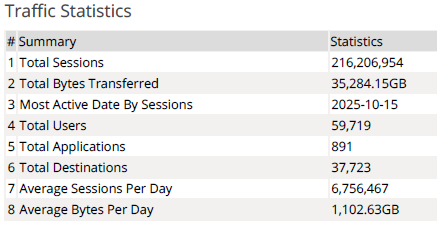
* Intrusion Prevention System (IPS)
* Advanced Malware Protection (AMP)
* AI-based Inline Malware Prevention
* Web Security
* Attack Surface Security Rating
* Inline SaaS Application Security (CASB)
* Data Loss Prevention
* Application Control
* Inline CASB Database
* Device/OS Detection
* GeoIP Updates
* Trusted Certificate Database
* Internet Service (SaaS) Database
* DDNS (v4/v6)

Více informací je na: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/og-fortiguard.pdf

FireWally jsou zapojeny redundantně k páteřním přepínačům sítě LAN (linková agregace 2x 10GE) a jsou napojeny na Microsoft Active Directory (3500 uživatelů), které je využito pro nastavení pokročilých UTM pravidel včetně SSO. Jiné externí zdroje identit nejsou využívány.

Na NGFW jsou definovány 3 virtuální kontexty. Celkem je v těchto kontextech udržováno 6 VLAN, 130+ FW pravidel a 74+ NGFW pravidel. Je využívána SSL VPN.

Měsíční vytížení boxů je uvedeno v následující tabulce:



K ukládání logových informací z FortiGate 200E slouží FortiAnalyzer s kapacitou 6GB logů/den s průměrným denním vytížením 1-2GB/ logů za den. FortiAnalyzer má platnou podporu výrobce do 19.11.2026 (SN: FAZ-VMTM18000655).

# Popis cílového stavu

Po dokončení nové budovy campusu v Hradci Králové budou obě fakulty Univerzity Karlovy (FaF a LF) přestěhovány a budou sdílet vybrané části síťové infrastruktury. Jednou z těchto částí bude zabezpečení internetové komunikace, které bude realizováno dvojicí NGFW v HA zapojení. Kromě této funkce perimetrového FW budou nové firewally plnit roli tzv. Internal Segmentation FireWallu (ISFW). Tzn. že budou sloužit pro hloubkovou inspekci vybraného síťového provozu. Dostatečný výkon a minimální latence NGFW zajistí plnohodnotný provoz interní segmentace bez negativního dopadu na propustnost a odezvu inspektovaných aplikací.

Nové NGFW musí být schopné zajistit veškerou funkcionalitu stávajících 6-ti boxů NGFW, musí mít dostatečný výkon s výhledem navyšování provozu a zlepšování bezpečnostních funkcionalit a musí být podporovány a pravidelně aktualizovány výrobcem min. 5 resp. 7 let.

Součástí řešení musí být také centralizovaný nástroj pro sběr, vyhodnocení a reporting bezpečnostních logů z těchto NGFW s dostatečnou kapacitu pro sběr a retenci těchto logů ve formě virtuální appliance pro platformu Hyper-V.

Schéma zapojení je zřejmé z následujícího obrázku.



## Minimální technická specifikace NGFW (2ks)

* Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, akcelerace IPsec VPN, porovnávání se signaturovou databází, atd.)
* Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu **5 let**. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
* Požadujeme dodání zařízení ve formátu HW appliance o velikosti max. 2U
* Možnost o rozšíření platformy o sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality
* Zařízení musí být vybavené redundantním napájecím zdrojem (1+1). Zdroje musí být vyměnitelné za provozu bez výpadku systému. Zdroje budou součástí dodávky, pokud nejsou integrované.
* Zařízení musí být dodána v režimu vysoké dostupnosti. Bez výpadkový cluster bude sestaven celkem ze 2 zařízení – součástí dodávky musí být všechna zařízení včetně všech potřebných licencí.

### HW parametry

* Počet rozhraní 100 GE QSFP28 / 40 GE QSFP+ – min. 4x
* Počet rozhraní 25 GE SFP28 / 10 GE SPF+ / 1 GE SFP – min. 4x
* Počet rozhraní 10 GE SFP+ – min. 2x
* Počet rozhraní 1 GE RJ45 – min. 8x
* Dedikovaný konzolový port – min 1x
* Dedikované porty pro správu – min 1x
* USB port umožňující připojení USB flash paměti pro zálohování konfigurace, zároveň umožňující připojení USB modemu pro záložní připojení internetu – min. 1x
* Zařízení musí být vybaveno zabezpečovacím krypto procesorem do kterého je možné ukládat citlivé informace, min. IPsec pre-shared klíče, NTP hesla a administrátorská hesla.

### Výkonnostní parametry

* IPv4 propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518B, 512B, 64B – min. 190 Gbps, 190 Gbps, 120 Gbps
* IPv6 propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518B, 512B, 86B – min. 190 Gbps, 190 Gbps, 120 Gbps
* Latence firewallu (64 B UDP paket) – max. 4 mikro sec.
* Počet naráz otevřených spojení – min. 10 000 000
* Počet nových spojení za sekundu - min. 700 000
* Počet firewall pravidel min. 90 000
* Podpora virtualizace, min. 10 oddělených kontextů s možností rozšíření na 250
* Podpora funkce bezdrátový kontrolér – min. 2 000 bezdrátových přístupových bodů v tunelovém režimu

### Networking a Vysoká dostupnost (HA)

* Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nody v clusteru
* HA musí podporovat až 4 nody v HA režimu
* Režim fungování L2 – transparentní režim, L3 – NAT/Router
* Podpora VLAN
* Podpora multicast, vytváření politiky pro multicast routování
* Podpora 802.3ad link aggregation
* Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
* Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
* Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP
* Policy-based routing
* Podpora uplatňování základních pravidel pro kontrolu na přístupové vrstvě (NAC pravidla, politiky)
* Zařízení musí podporovat možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky (SD-WAN).
* Funkce SD-WAN nesmí být licenčně omezeno. V rámci nabízeného řešení musí být dodáno v podobě, jenž umožňuje neomezené využívání i v případě, že dojde k nárůstu počtů zařízeních komunikující skrze SW-WAN do internetu, tak i v případě, že dojde k navýšení počtu konektivit a jejich rychlosti.
* Integrované SD-WAN řešení musí podporovat podle dokumentace výrobce min. 200 členů virtuálního rozhraní, které sdružuje konektivitu a jsou na něj uplatněna pravidla provozu a routingu.

### Funkce SSL VPN

* Nabízené řešení musí podporovat možnost připojení klientů do VPN pomocí proprietární SSL VPN. Aplikace pro do VPN musí být podporována nejběžnějšími operačními systémy, jako například: Windows, macOS, Linux, Android nebo iOS.
* Podpora bez klientského připojení do VPN na úrovni webového portálu, pomocí standardního internetového prohlížeče.
* Možnost zabezpečení připojení do VPN vynucením dvou faktorového ověření. Například pomocí emailu, SMS, hardwarovou klíčenkou, nebo proprietární aplikace dostupná pro Android i iOS.
* Zařízení musí umožňovat rozšíření pro využití dostupného dvou faktorového ověření
* Vynucení ověření klientského certifikátu pro zvýšení zabezpečení.
* Minimální počet současně navázaných SSL VPN tunelů: 5 000
* Minimální propustnost SSL VPN: 10 Gbps

### Funkce IPsec VPN

* Podpora site-to-site VPN
* Podpora klientských VPN
* Dostupnost VPN klienta pro koncové stanice (Windows, MacOS) z veřejně dostupných webových stránek.
* Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů. V opačném případě požadujeme dodání neomezené licence.
* Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 18 000
* Minimální počet klientských IPSEC VPN tunelů: 90 000
* Propustnost IPSec VPN min. 50 Gbps (měřeno při AES256-SHA256, 512 byte)
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování.
* Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování.
* Podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace.
* Podpora VXLAN.
* Podpora L2TP, PPTP, GRE.
* Podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec.

### Firewall

* Možnost nastavovat firewall politiku na základě geografických údajů
* Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem
* Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
* Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
* Viditelnost do provozu na aplikační úrovni
* Možnost dynamického stahování externích seznamů IP adres a jejich následné použití ve firewall policy
* Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
* Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
* Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
* Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
* Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
* Podpora funkce reverzní proxy
* Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
* Administrátorské účty mohou být volitelně zabezpečený pomocí dvou faktorového ověření

### UTM funkce

**Funkce detekce aplikací na L7 (Application Control)**

* + detekce známých aplikací na základě signatur
  + signaturové databáze automaticky aktualizované výrobcem
  + alespoň 4 000 podporovaných aplikací
  + pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login atd. (relevantní k dané aplikaci)
  + možnost tvorby vlastních signatur
  + detekované aplikace je možné: povolit, monitorovat, blokovat
  + na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
  + funkce detekce aplikací se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.

**Funkce detekce a potlačení narušení (IPS/IDS)**

* + signatury automaticky aktualizované výrobcem
  + alespoň 11 000 rozpoznávaných hrozeb (signatur) definovaných výrobcem
  + možnost tvorby vlastních signatur
  + funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
  + funkce tzv. fail-open - při přetížení IPS je možné definovat, zda dojde k blokaci nebo propuštění provozu
  + deklarovaná propustnost IPS inspekce min 20 Gbps

**Funkce antivirové kontroly**

* + ochrana před škodlivým kódem (malware, trojské koně apod.), včetně ochrany před polymorfním kódem
  + signatury automaticky aktualizované výrobcem
  + požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
  + možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce
  + deklarovaná propustnost AV kontroly, v kombinaci s FW, IPS, Application Control a zapnutým logováním min. 15 Gbps
  + funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
  + Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
  + Funkce odstranění škodlivého aktivního obsahu z dokumentů kancelářských aplikací.

**Funkce kategorizace a blokace webových stránek**

* + založená na centrálně spravované databázi výrobce
  + minimálně 50 filtračních kategorií
  + možnost definice vlastních kategorií
  + možnost definice vlastních seznamů zakázaných URL
  + kategorizace musí zahrnovat I české a slovenské internetové stránky

**Funkce blokování video obsahu portálu YouTube**

* + založená na centrálně spravované databázi výrobce
  + minimálně 8 filtračních kategorií
  + možnost definice vlastních kanálů na základně channel ID

**Funkce DNS filtrování**

* + Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
  + Možnost definovat vlastní tzv. deny-list domén
  + Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
  + Možnost importu seznamu blokovaných domén do DNS filtru
  + Detekce a blokování komunikace do botnet sítí

**Funkce blokace stahování konkrétních typů souborů**

* + možnosti zablokovat stahování souborů s konkrétními typy, jako napři. MSI, EXE…
  + funkce blokace stahování konkrétních typů souborů se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.

**Emailový antispamový modul**

* + jednoduchá antispamová a antivirová inspekce elektronické pošty

**Podpora SSL dekrypce**

* + podpora SSL dekrypce a inspekce pro ochranu jak koncových zařízeních, nebo serverů
  + funkce SSL dekrypce se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
  + zařízení musí u SSL inspekce dosáhnout min. propustnost 10 Gbps

**Podpora pravidel pro obranu proti útokům typu DoS**

* + zařízení musí umožnit uplatnit pravidla proti DoS útokům na základě politik, které se aplikují na konkrétní interface zařízení.
  + podpora detekce anomálií na 3. a 4. vrstvě
  + podpora např. TCP SYN FLOOD, ICMP FLOOD, SCTP SRC SESSION
  + funkce musí umožňovat provoz nejen blokovat, ale i sledovat pro možnost orientace na síti

**Explicitní proxy**

* + podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
  + podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
  + funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
  + Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém server

**Integrovaný kontrolér bezdrátových sítí (WiFi)**

* Wifi kontrolér integrovaný do NGFW platformy
* Bezdrátová síť (SSID) může být reprezentována virtuálním síťovým rozhraním – provoz tunelován z AP do kontroléru
* podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi kontroleru
* podpora SSL dekrypce uživatelského provozu přímo na wifi kontroléru
* Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení
* Možnost volby z různých modelů (802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor)
* Podpora BSS Coloring
* On-wire rogue AP detekce a mitigace
* Podpora fast-roamingu (802.11 k,v,r)
* podpora více PSK u jednoho SSID
* podpora IPSEC tunelu pro šifrování data plane (uživatelských dat)
* Podpora WPA3 protokolu

### Multi-tenance (virtualizace)

* Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů atp.
* Každý virtuální kontext je zároveň samostatným wifi kontrolérem
* Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

### Management

* FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
* Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
* Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

## Minimální technická specifikace pro analyzátor provozu a dočasné úložiště logů

Všechny 3 stávající appliance FortiAnalyzer s kapacitou 6 GB logů/den (každá) budou nahrazeny centralizovaným nástrojem pro sběr, vyhodnocení a reporting bezpečnostních logů z NGFW.

* Virtuální appliance pro platformu Hyper-V.
* Plná podpora a integrace s nabízeným řešením NGFW
* Obousměrná integrace s nabízenými NGFW, tedy data se přenáší jednak z firewallu na logovací a reportovací platformu, ale zároveň je možné přímo v GUI firewallu přistupovat k log údajům na logovací a reportovací platformě
* Příjem logů a vytváření reportů pro nabízené NGFW a podpora pro Syslog kompatibilní zařízení
* Výkon logování min. 25 GB/den
* Kapacita úložiště min.10 TB historických dat
* Real-time prohledávání logovaných dat
* Vyhledávání historických dat podle typu události nebo typu provozu. Vyhledávání podle zařízení.
* Funkce zpětné kontroly logů až 7 dnů zpět a zjištění, jestli systém nebyl napaden při přístupu na škodlivou webovou stránku
* Korelace logů
* Podpora prohlížení statistických údajů nad logy
* Předdefinované reporty
* Uživatelská definice reportů (vzhled, obsah apod.)
* Automatické pravidelné generování reportů v daném čase a periodě
* Automatické odesílání reportů emailem
* Automatická reakce na zjištěnou hrozbu

# Implementace

## Rozsah implementačních činností dodávaného řešení bude zahrnovat

* Instalaci, zprovoznění a zapojení nových zařízení do infrastruktury zadavatele
* Kompletní migraci stávajícího řešení na nově dodaný systém
* Přenos všech stávajících konfigurací a bezpečnostních pravidel vč. jejich optimalizace do nově dodaného řešení
* Zaškolení místního správce v rozsahu min. 2 dny
* Přepojení provozu na nový FW, otestování provozu a vysoké dostupnosti, diagnostiku po přepojení ,doladění
* Zpracování dokumentace
* Zpracování projektu realizace
* Provozní podpora dodavatele v rozsahu 2MD měsíčně po dobu 5 let