FORTINET

# NÚKIB

# Povinná ochrana emailové komunikace.

Jste připraveni?

NÚKIB

# Zabezpečení poštovních serverů

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vydal na základě zákona o kybernetické bezpečnosti v říjnu 2021 ochranné opatření formou veřejné vyhlášky, které se týká zabezpečení poštovních serverů.

**Dle toho opatření jsou všechny orgány a osoby uvedené v §3 písm. c) až f) zákona o kybernetické bezpečnosti splnit následující požadavky:**

1. Všechny SMTP servery uvedené v MX záznamech, přes které je přijímána elektronická pošta, a hraniční SMTP servery, přes které je pošta odesílána, podporují zabezpečené spojení dle standardu STARTTLS (IETF RFC 3207).

2. V rámci zabezpečeného spojení všechny servery, přes které je přijímána nebo odesílána elektronická pošta:
   - Podporují protokol TLSv1.2 nebo novější.
   - Nepodporují protokol SSLv3 a starší.

3. Certifikáty všech SMTP serverů uvedených v MX záznamech jsou validní, vystaveny uznávanou certifikační autoritou a s doménovým názvem odpovídající názvu MX záznamu daného serveru.

4. Všechny DNS záznamy relevantní pro funkci přijímání pošty mají zabezpečenou integritu pomocí technologie DNSSEC.

5. Všechny používané MX záznamy SMTP serverů mají zveřejněn odpovídající TLSA záznam v DNS dle technologie DANE.

**Termín splnění těchto požadavků byl stanoven pro některé orgány a osoby na 1. ledna 2022, pro jiné pak nejpozději do 1. července 2022.**

Plné znění vyhlášky lze nalézt na webových stránkách Národního úřadu pro kybernetickou a informační bezpečnost.

PLNÉ ZNĚNÍ VYHLÁŠKY

https://www.nukib.cz/download/uredni_deska/2021-10-08_OchranneOpatreni_final.pdf

# Je vaše organizace připravena na tuto změnu?

Požadavky uvedené ve vyhlášce lze rychle a jednoduše splnit použitím produktů společnosti Fortinet, v tomto konkrétním případě pak použitím jedné z nejlepších emailových ochran na trhu, kterým je FortiMail.

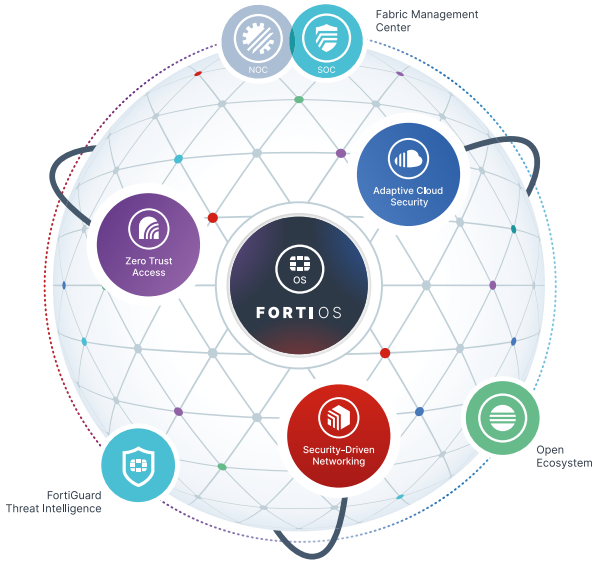
FortiMail je špička na trhu zabezpečení emailové komunikace. Nicméně kryptografická ochrana požadovaná vyhláškou NÚKIB není to jediné, co vám může FortiMail nabídnout. Mezi jeho hlavní funkce patří:

## Antispamová ochrana

FortiMail nabízí řadu základních i pokročilých technik pro boj se spamem. Ať už jde o použití interních reputačních databází spravovaných analytiky z FortiGuard Labs, tak o možnost definice vlastních nebo externích reputačních listů. K dispozici jsou ochranné techniky na úrovni spojení, reputace, autentizace i obsahu. V reálném světě dosahuje úroveň ochrany díky těmto technikám 99,7 %, což je opakovaně potvrzováno nezávislými autoritami. Samozřejmostí je také systémová nebo uživatelsky obsluhovatelná karanténa s moderním webovým rozhraním.

## Ochrana před malware

Stejně jako poskytuje Fortimail vynikající ochrana v boji se spamem, nabízí rovněž špičkovou ochranu v boji s malware. Ochrany je dosahováno vysoce efektivním, rychlým, spolehlivým a prověřeným antivirem společnosti Fortinet, který se pravidelně umisťuje v nezávislých testech na nejvyšších příčkách. Tím ovšem ochrana před malware nekončí. Maximální možné ochrany je možné dosáhnout zapojením techniky tzv. sandboxingu, kdy dojde ke spuštění potenciálně nebezpečného kódu v chráněném virtuálním prostředí a je sledováno, jak se kód chová. Fortimail lze velmi snadno připojit k produktu Fortisandbox, a to jak ve formě on-premise appliance, tak ve formě cloudové služby.




## Ochrana Microsoft 365

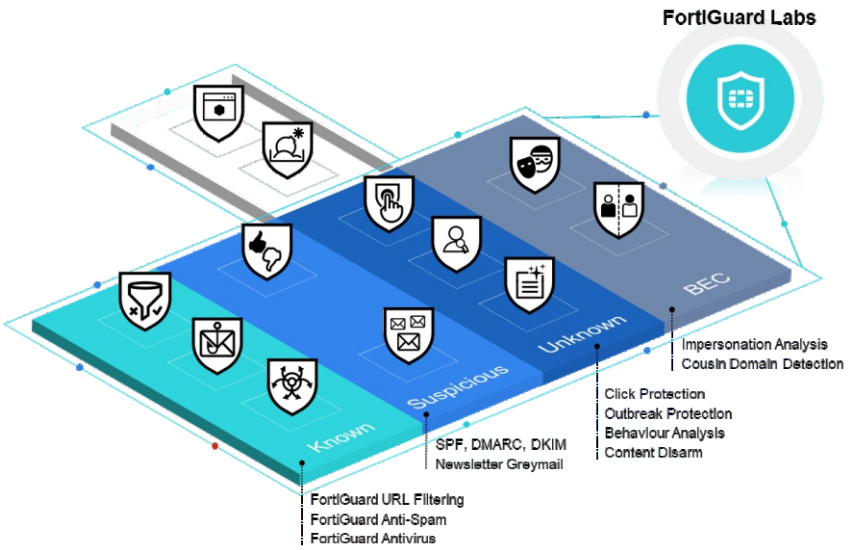
Používáte služby Microsoft 365 a Exchange online? Pro Fortimail žádný problém. Fortimail nabízí nativní integraci s Exchange online buď ve formě přístupu k obsahu poštovních schránek přes nativní API, případně může Fortimail sloužit jako poštovní brána, která může být využita ke kontrole jak příchozích, tak odchozích zpráv elektronické pošty.

## Pokročilé techniky ochrany

Kromě antispamových a antivirových kontrol nabízí FortiMail i další pokročilé funkce ochrany. Mezi ně patří například ochrana citlivých informací (DLP), analýza obrázků, odstranění aktivního obsahu z MS Office a PDF dokumentů, ochrana odkazů v těle emailových zpráv či pokročilá ochrana před phishingem.

## Integrace

FortiMail je pochopitelně možno integrovat v rámci stávající infrastruktury, například s Active Directory, Exchange, LDAP, Radius a podobně. Samozřejmostí je pak podpora nejnovějších šifrovacích algoritmů a integrace a spolupráce s ostatními produkty Fortinet v rámci Fortinet Security Fabric.



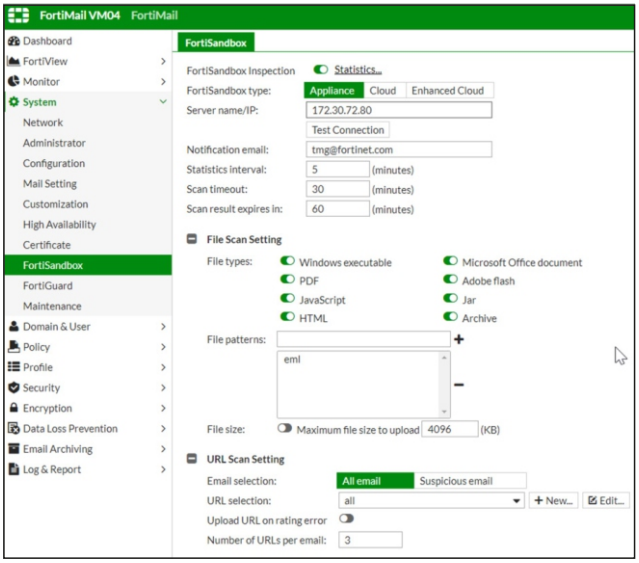
## Škálovatelnost

Produkt FortiMail můžete mít jak ve formě fyzické appliance, tak ve formě virtuálního stroje, kdy podporujeme nejrozšířenější virtualizační platformy jako je VMWare, XenServer, Hyper-V nebo KVM. Stejně tak je možno Fortimail nasadit jako cloud appliance pro Microsoft Azure či Amazon Web Services.

## Jednoduché nasazení a administrace

Nasazení FortiMailu nemusí být noční můrou. Jako zákazník Fortinetu máte k dispozici několik možností, jak FortiMail nasadit a provozovat. Můžete využít gateway mód, kdy si FortiMail v klidu nakonfigurujete a poté pouze změníte MX záznam nebo máte možnost využít transparentní mód, kdy není nutný téměř žádný zásah do stávající infrastruktury. Pro uživatele Microsoft 365 a Exchange online je pak k dispozici možnost připojení FortiMailu k Exchange serveru pomocí API. Pokud vám nevyhovuje váš stávající emailový server, máte možnost ho nahradit, protože FortiMail umí fungovat i jako plnohodnotný emailový server, včetně moderního webmail rozhraní.

Fortinet je znám svým snadným, intuitivním, moderním webovým management rozhraním a FortiMail není výjimkou. K dispozici tak máte HTML 5 rozhraní s podporou moderních technik jako je například drag&drop nebo drill down. Správa nebo prohledávání záznamů tak bude pro správce velmi jednoduchá a nenáročná.




## Špičkový produkt s bezkonkurenčním výkonem

FortiMail poskytuje vynikající výkon měřený nezávislými testery třetích stran.

**99,9 %**
**Detekce škodlivých e-mailů**

**94 %**
**Celková míra detekce**

**99,78 %**
**Míra zachycení spamu**

**100 %+**
**Míra detekce ze seznamu WildList**