Oznámení veřejného náhledu příchozího SMTP DANE s DNSSEC pro Exchange Online – Microsoft Community Hub

techcommunity.microsoft.com/t5/exchange-team-blog/announcing-public-preview-of-inbound-smtp-dane-with-dnssec-for/ba-p/4155257

nedefinováno

Jsme nadšeni, že můžeme oznámit veřejný náhled příchozího SMTP DANE s DNSSEC, novou funkci Exchange Online, která zvyšuje bezpečnost e-mailové komunikace podporou dvou bezpečnostních standardů: DNS-based Authentication of Named Entities (DANE) pro SMTP a Domain Name System. Bezpečnostní rozšíření (DNSSEC).

Veřejný náhled pro příchozí SMTP DANE s DNSSEC se v současné době zavádí. Pokyny pro jeho implementaci ve vašem tenantovi jsou v Jak SMTP DNS-based Authentication of Named Entities (DANE) zabezpečuje e-mailovou komunikaci .

SMTP DANE a DNSSEC

SMTP DANE používá DNS záznam TLS Authentication (TLSA) k ověření identity cílového poštovního serveru a poskytuje zabezpečené spojení mezi odesílajícími a přijímajícími poštovními servery, které je odolné jak proti útokům na nižší verzi TLS, tak proti útokům protivníka uprostřed (forma odposlechu, kdy je komunikace sledována nebo upravována špatným aktérem).

DNSSEC používá kryptografické podpisy, aby se zajistilo, že záznamy DNS cílové domény jsou autentické a nebyly při přenosu zfalšovány.

Tyto dva standardy spolupracují, aby zabránily spoofingu, únosu a zachycení e-mailových zpráv.

Příchozí SMTP DANE s výhodami DNSSEC

Pomocí SMTP DANE s DNSSEC můžete:

- Lepší ochranu vaší e-mailové domény (domén) před předstíráním identity;
- Pomozte zajistit, aby byly vaše zprávy doručeny zamýšleným příjemcům pomocí šifrování a beze změny nebo přesměrování; a
- Vylepšete svou e-mailovou pověst tím, že prokážete soulad s nejnovějšími bezpečnostními standardy.

Zlepšení zabezpečení e-mailů

V roce 2022 jsme vydali Outbound SMTP DANE s DNSSEC a jsme nadšeni, že můžeme spustit Public Preview pro Inbound SMTP DANE s DNSSEC. V rámci našich snah o zlepšení zabezpečení e-mailů pro všechny začleňujeme Inbound SMTP DANE s DNSSEC do našich firemních a spotřebitelských e-mailových nabídek zdarma. Vyzýváme ostatní poskytovatele e-mailu a vlastníky domén, aby přijali tyto standardy a společně zvýšili laťku zabezpečení e-mailů a chránili uživatele před zlomyslnými aktéry.

Již jsme implementovali příchozí SMTP DANE s DNSSEC pro několik e-mailových domén Outlooku a implementaci dokončíme pro zbývající domény Outlooku (včetně Hotmailu) do konce roku 2024.

Těšíme se, až uvidíme dopad této funkce na prostředí e-mailové bezpečnosti, a těšíme se na pokračování inovací a poskytování e-mailové nabídky se špičkovým zabezpečením, jako je SMTP DANE s DNSSEC.

Přihlaste se k veřejnému náhledu ještě dnes

Můžete se přihlásit k veřejnému náhledu ještě dnes a začít používat příchozí SMTP DANE s DNSSEC podle kroků povolení uvedených v této dokumentaci . Uvítáme také vaši zpětnou vazbu a návrhy na vylepšení této funkce.

Plán zabezpečení e-mailu

Naše cílová data pro nadcházející položky plánu jsou:

- Srpen 2024 – Příchozí SMTP DANE se zprávou DNSSEC a MTA-STS v centru pro správu Exchange
- Říjen 2024 – Obecná dostupnost příchozího SMTP DANE s DNSSEC
- Konec roku 2024
    - Nasazení příchozího SMTP DANE s DNSSEC pro všechny domény aplikace Outlook
    - Převod zajišťování poštovních záznamů pro všechny **nově vytvořené** akceptované domény do infrastruktury s podporou DNSSEC pod *.mx.microsoft
- Únor 2025 – Povinný odchozí SMTP DANE, nastavený na tenanta/na vzdálenou doménu

Další informace o změně zřizování naleznete v tématu Implementace příchozího SMTP DANE pomocí DNSSEC pro Exchange Online Mail Flow .

Další informace o .microsoftu a jeho subdoménách najdete na stránce Představujeme cloud.microsoft: jednotná doména pro aplikace a služby Microsoft 365 .

Zpětná vazba

Vítáme vaši zpětnou vazbu a chceme od vás slyšet o vašich zkušenostech s příchozím SMTP DANE s DNSSEC. Pokud máte nějakou zpětnou vazbu nebo obavy, okomentujte tento příspěvek a my vám podle potřeby odpovíme nebo se s vámi přímo spojíme.

Microsoft 365 Messaging Team (dříve Exchange Online Transport Team)

8 lajků

Jako

42 komentářů

Ahoj kluci,

Zdá se, že příkazy zatím nefungují. Bude pro to existovat nová verze modulu Exchange Online Powershell?

Dík,

Tim

Dělám na tom!

/edit: Zdá se, že Enable-DnssecForVerifiedDomain není přítomen v EXO PS 3.5.1 (i když na MacOS).

/Edit2: také ne na W11 (přes Parallels).

Mustafa201085
Měděný přispěvatel

Velmi informativní.

@DMStork @TimJohnsonTech Opravdu jsem se také snažil najít tuto rutinu. Nejnovější verze modulu (3.5.1) jej neobsahuje.

@MaximeRastello @DMStork @TimJohnsonTech rutiny se zavádějí, když mluvíme, a budou ve vašich nájemcích zítra nebo nejpozději v pátek brzy ráno. Velká část nájemců v EU by již měla mít možnost používat rutiny.

5 lajků
Jako

Mohu potvrdit, že rutiny jsou dostupné v mém tenantovi v EU. Právě jsem sledoval dokumentaci a povolil příchozí DANE bez problémů.

2 lajky
Jako

to je dobrá zpráva! Nevidím již zmíněno žádné omezení předplatného. Je E5 pro Dane stále povinné?

@Hitronics , jak říkáme v příspěvku na blogu „ Začleňujeme Inbound SMTP DANE s DNSSEC do našich podnikových a spotřebitelských e-mailových nabídek zdarma jako součást našeho úsilí o zlepšení zabezpečení e-mailu pro každého. “ Všichni zákazníci to tedy získají jako součást služby.

7 lajků
Jako

Hitronics
Měděný přispěvatel

Děkuji!

0 lajků

Jako

MichaelMortenSo nne
MVP

Konečně! 😁

Enable-DnssecForVerifiedDomain zatím není v mém tenantovi z EU, ale později se znovu otestuje @IanMcDonald !

0 lajků

Jako

IanMcDonald
Microsoft

17. července 2024 13:57

Zní to dobře @MichaelMortenSonne ! Dejte nám vědět, jak to jde!

0 lajků

Jako

WKHO-jpa
Měděný přispěvatel

17. července 2024 14:07

Úžasné, aktivace byla snadno provedena za 15 minut (TTL již bylo připraveno ;-))

0 lajků

Jako

IanMcDonald
Microsoft

17. července 2024 14:12

@WKHO-jpa úžasné!! Děkuji za sdílení :)

0 lajků

Jako

Myslím, že dokumentace předpokládá, že example-com.mail.protection.outlook.com

MX has a priority of 0, and that the new MX will initially be added with a lower priority. You then recommend testing that mail is capable of flowing to both endpoints before making the new endpoint the default. It is possible that the old MX has a value greater than 20, and in that scenario the user is making the new endpoints primary earlier than expected.

The documentation also assumes that people have not configured a "backup" MX record. It might be enough to say in the documentation "if you have more than one MX record contact your administrator for guidance", rather than trying to account for every possible complication of MX records.

At several points you mention the need to set the MTA-STS policy to "test". You should also mention the need to update the _mta-sts TXT record every time the policy is updated. If the "id" in the TXT record is not updated Sending MTAs might not check the policy at all until the max_age has expired.

1 Like
Like

@michaelkennedy thank you for taking the time to review the documentation and providing this valuable feedback! I'm updating documentation on all these things :)

We definitely assumed the priority is 0 or 10, because otherwise the domain would appear unhealthy in the M365 Admin Center and one of the prereq's is for the domain to be healthy. But I will add this

assumption in the documentation, because not everyone uses the M365 Admin Center. But the M365 Admin Center health check wouldn't have caught a Fallback MX, so very nice catch on that!

0 Likes

Like

*"February 2025 – Mandatory **Outbound** SMTP DANE, set per-tenant/per-remote domain*" - This looks like a **typo**, Outbound was already set in 2022-23 without any action from the admins. Are you talking about 'Mandatory **Inbound** in 2025', or this is a new feature being introduced to allow more control to relax DANE if needed for Outbound emails.

Releasing: Outbound SMTP DANE with DNSSEC - Microsoft Community Hub
As an Exchange Online customer, you don't have to do anything to reap the benefits of this enhanced email security for outbound email. It's built into the system and once enabled over the coming weeks it will be on by default for all Exchange Online customers.

If an email sent from Exchange Online is blocked, the resolution MUST BE implemented by an admin of the receiving domain. An Exchange Online admin cannot perform any remediation.

Because of this, tenant-level exceptions or opt-out won't be available.

0 Likes

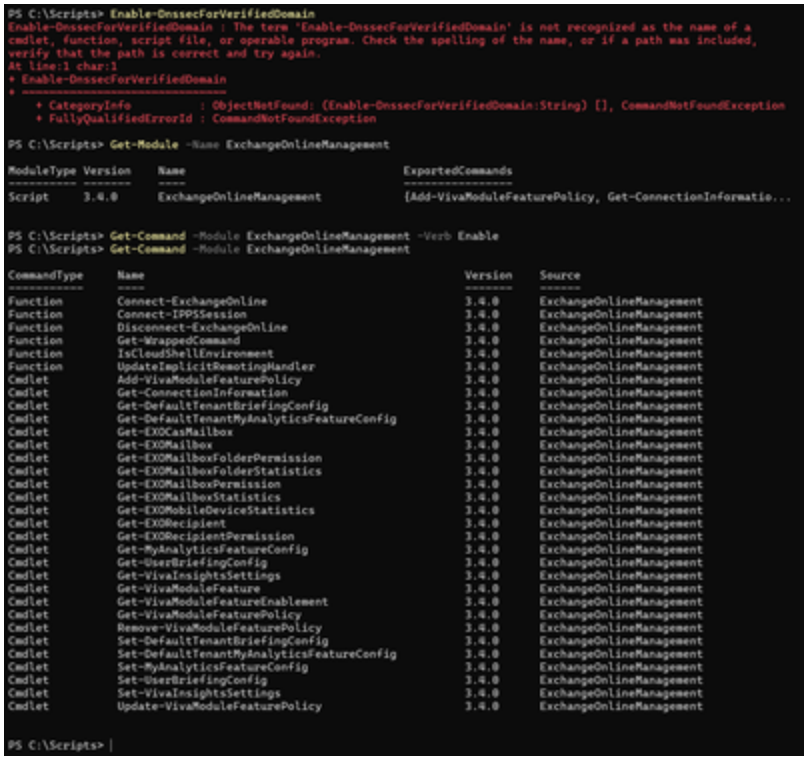
Like

GulabPrasad

Copper Contributor

Jul 18 2024 02:37 AM

I guess I have to wait before I can enable it in my tenant 😶



0 Likes

Like

Hi I have a couple of questions I hope someone from microsoft and someone who is in the preview can
answer @The_Exchange_Team @IanMcDonald

1/ Do any of those in the public preview pass with 100% the third party https://internet.nl/test-mail/ test ?

(anyone in the preview please feel free to comment)

2/ Why do we not have a concrete example domain to test with third party tools to validate setup before commiting ?

3/ Why does the Microsoft Remote Connectivity Analyzer not validate broadcom.com ?

(which is using google domain with DNSSEC enabled is there something that microsoft doesn't acknowledge mx1.smtp.goog or the .goog domain which is ironic since it seems .mx.microsoft domain is being used here)

4/ is .mx.microsoft healthy and can we point to third party statistics to show that ?

thanks for the responses

John Jones

0 Likes

Like

Succes!

@johnjonestag Deployed DANE on at least one domain. Internet.nl does show a phase-out cipher in use, so that prevents the 100% (I assume, as I currently am not IPV6 enabled which also prevents 100%, submitted a support ticket for that).

@The_Exchange_Team The Learn article mentions several times setting MTA-STS mode from "enforce" to "Test" . This however has to be "testing" per RFC.
0 Likes

Like

@Satyajit321 I read that differently, I assumed this is the ability to set per domain whether outbound DANE is mandatory; meaning that if outbound DANE is set to mandatory for example contoso.com and the

receiving domain is not DANE capable (permanent or temporary) you tenant wil *not* send any mails to that domain.

Currently DANE will be used, but will fall back if it would fail. Similar to Opportunistic TLS and Mandatory TLS.

1 Like
Like

@Gulab Prasad (Not a Powershell expert...)

I used these commands to get access to the commandlets.

```
connect-exchangeOnline -CommandName Enable-DnssecForVerifiedDomain
connect-exchangeOnline -CommandName Enable-SmtpDaneInbound
```

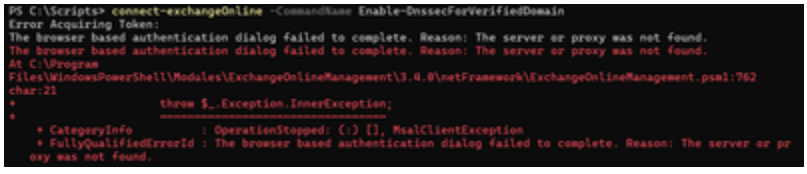
@DMStork

The phase-out cipher will not prevent you getting 100% on internet.nl. All the domains I have enabled for DANE had IPv6 enabled before migrating, and they retained it after enabling DANE. They all show the phase-out cipher, but still score 100% on that test.

2 Likes
Like

Thanks @michaelkennedy it worked.

I noticed that my WARP was connected and the command kept failing erroring out with..



So make sure your device doesn't have any WARP connected at the time of running the command

1 Like
Like

@johnjonestag

- Regarding a sample domain to test, we don't provide sample domains for our features. You'll have to set up a cheap test domain with a DNS Provider, which can be purchased for a couple dollars and last a year.

- The RCA shows the correct output for broadcom.com so maybe we need to improve the interpretability. It shows DNSSEC passing for broadcom.com and DANE not succeeding (emphasis on not succeeding, I did not say DANE failed) because there is no TLSA record for broadcom.com. The TLSA record is required for SMTP DANE validation to succeed. If the TLSA is not present, then we say the SMTP DANE validation didn't succeed and show the yellow warnings you are seeing.

- It's healthy as we've been testing with it for several months. Feel free to use dig to review SOA/NS configuration or DNSViz for the DNSSEC info. Can I ask why you are concerned about this?

@DMStork thanks :) I'm pushing through a doc update ASAP. And your explanation regarding us using Outbound SMTP DANE with DNSSEC in an opportunistic manner is spot on. I will make this clearer in our public documentation.

@Satyajit321 no typo's and DMStork explained it well. We are using SMTP DANE with DNSSEC opportunistically on the outbound path because most destinations don't support SMTP DANE (yet!). Outbound Mandatory SMTP DANE will allow Exchange Online customers to make passing SMTP DANE with DNSSEC validations ***mandatory*** for the email to successfully send. So, if the SMTP DANE or DNSSEC

validation fails, we will not try to fallback to a secondary, unsecured MX record for that same domain, which does happen with current behavior. I'll clean up the documentation so it's clearer.

1 Like
Like

In testing I'm finding gmail will NOT send to a domain configured with the new dane mx but the domain passes connectivity test and can receive from yahoo mail and other senders. There are no NDR's.

The new dane mx configuration has had several hours to propagate.

I have a test domain available if you guys want to help me troubleshoot :)

0 Likes

Like

Hitronics
Copper Contributor

Jul 18 2024 11:27 PM

@LagunaJim changed my test domain to DANE yesterday and gmail delivers just fine.

0 Likes

Like

Hmmn. I'm gonna step away for a while -- I've gone over the setup multiple times, and as I said it passes the inbound connectivity test AND passes mail from everywhere I've tested except for gmail.

0 Likes

Like

ThorstenK2
Brass Contributor

Jul 19 2024 12:29 AM

please kick the Azure team to offer DNSSEC in AzureDNS
FAQ - Azure DNS | Microsoft Learn

0 Likes

Like

@LagunaJim Does that specific domain also have MTA-STS? In testing I had possibly similar issues, the documentation is missing a few import steps that can cause issues, already informed @IanMcDonald about this. Currently I have Inbound DANE and MTA-STS working and GMail is working as well. I posted my findings on all my socials, but forgot this comment section:

Important: For those who already have MTA-STS in place (enforce): do not forget to lower the TTL of your _mta-sts dns recor, wait for the previous to expire AND change your id value when you change anything in the mta-sts.txt policy file and before you change the MX DNS record.

Otherwise MTA-STS only sending servers will not get the update (until max_age is expired), see an invalid MX record and will not send you mail. You won't see that with sending servers that do not support MTA-STS, or servers that do both but prioritize DANE before MTA-STS.

Additionally, the learn text mentioned earlier setting the MTA-STS config mode from "enforce" to "Test", that should be "testing". But that might already been fixed.
GMail does support outbound MTA-STS, but does not support DANE (to my surprise). Some orgs I used for testing have outbound DANE, but do not support MTA-STS: So that explain that very specific difference.

0 Likes

Like

So I ran all the commands but am having an issue receiving GMAIL emails. Outbound (from my tenant to GMAIL) work fine but any messages going from GMAIL to my tenant never arrive. Nothing in trace..no NDR. Any ideas?

0 Likes

Like

Richdc165 that's strange, its working for me and some others. Are you on EOP or 3rd party email security? Is Azure your DNS hosting or?

Look at his for FAQ - Azure DNS | Microsoft Learn ...

0 Likes

Like

@Richdc165 Do you have MTA-STS on your M365 domain configured? Then see my notes in a previous post. M365 DANE requires an MX record change and if you have MTA-STS, you need to take careful steps in order to retain a valid MTA-STS policy published and pushed.

1 Like
Like

@DMStork so I got duped and didn't pick up on the fact the record update said 'test' in the instructions and just fixed that this morning to 'testing'. It's very possible that was part of the issue and need to wait for everyone to see in DNS there is an updated policy file. Feel like we're still missing a lot of emails but yeah...I thought about that one and may just have to wait it out

1 Like
Like

@GulabPrasad thanks. Not on any mail filtering solutions. Just 365. I did fix the MX record in the MTA-STS file to reflect what the new MX record was.

0 Likes

Like

@Richdc165 Don't forget to update the id in your _mta-sts TXT record, otherwise GMail will use the cached policy file with potentially the incorrect values. If the TTL of that record is high, you might want to (temporarily) lower it.

As for the mail sent by Google: All mails eventually dropped in again in my case, basically treating the issue as if you SMTP server was down/unavailable. So, most mails will be delayed unless the sending server has specific retry/fail settings.

1 Like
Like

@DMStork thanks for the advice. Cloudflare had the TTL set to auto so just bumped it down to 5 minutes and updated the policy file. Hopefully that will do it. Considering it's working for others I'm hoping it was just the MTA-STS 'test' was my only miss. Connectivity analyzer says everything is good so fingers crossed.

0 Likes

Like

@Richdc165 More import is to increase the id value of your _mta-sts TXT record, not just the TTL. When the id changes, the sending server is forced to update the policy file live and not wait on the max_age set inside the policy file. That max_age is often several days (604800 seconds is one week)
So, the id triggers an refresh update of the policy file, earlier than the set max_age. However the id change is only seen when the DNS TTL has expired: so two stacked intervals you have to take into account.

1 Like
Like

@DMStork Yes. I did both and look at that I've just received a couple of test emails. You rock. Thank you!

1 Like
Like

@DMStork Thanks for your instructions above. I still have no joy from gmail on two of three domains - one is finally receiving from gmail.

I wonder if today's global meltdown is affecting me :(
0 Likes

Like

Thanks everyone, @DMStork is spot on about making sure you update the policy ID when making changes, the documentation is being updated to reflect this.

0 Likes

Like

@DMStork FYI mail from gmail is finally flowing into the new Dane MX for all my domains -- as is sometimes the case, some server(s) out there were holding on to old information despite my best efforts. Thanks all!

0 Likes

Like

@ThorstenK2

DNSSEC on Azure DNS is in private preview. Please wait for some months.

Raffa

0 Likes

Like

Funguje! Skvělá práce!

Stránka s výsledky na mé e-mailové doméně z internet.nl https://bit.ly/3YdnDKd . https://internet.nl je skvělý bezplatný web pro testování bezpečnosti provozovaný nizozemskou vládou s různými soukromými stranami mimo jiné.

Získává se chyba 4/5.7.323 tlsa-invalid , ale zdá se, že vše funguje dobře bez ohledu na to.

0 lajků

Jako