

Interní služby na IPv6-only

Příběh jednoho neúspěšného pokusu



Interní služby?

Co je to interní služba



- Služba přístupná pouze pro zaměstnance
- **Historicky:** **lokální služby** dostupné pomocí **počítačů v kanceláři**
- **Potom:** **lokální služby** dostupné pomocí **VPN**
- **Dnes:** směs **lokálních** a **cloudových** služeb dostupná pouze **oprávněným uživatelům**



- **Neprivilegovaná sít'** v kanceláři
- **Trvale spuštěný VPN klient** na každém firemním počítači
 - Praktické pro (nečekanou) **práci z domova**
 - Používá se **Split tunnel** (máme pobočku v **Dubaji** a **zaměstnance v zahraničí**)
 - **IPv4 and IPv6** jak **uvnitř** tak **vně** tunelu
- Probíhající migrace **přihlášení pomocí LDAP** na **Single Sign-On**
 - Ověření pomocí SSO je **mnohem silnější** než ověření podle IP adresy
 - Ověření podle IP adresy je **nepoužitelné** s cloudovými službami

IPv6-only vhodné pro interní služby



- Služby přístupné **pouze zaměstnancům**
- Každý zaměstnanec má VPN klienta, který **poskytuje IPv6 konektivitu** k interním službám
- Co by se jen **mohlo pokazit?**



Příběh



- Nový zaměstnanec nastoupí do RIPE NCC. Pamatuje si tričko **IPv6 Act Now** z roku 2010.
- Zeptá se kolegů: “**Můžeme tuhle novou službu spustit IPv6-only?**”
- Jejich odpověď: “**Nejspíš ano.**”

IPv6 ACT NOW



- Systém správy konfigurace serverů **předpokládal dual-stack**
- Dohledový systém předpokládal, že **každý server má IPv4** adresu
- Zaměstnanec: **“Tohle můžeme opravit!”**

Vytvořen první prototyp

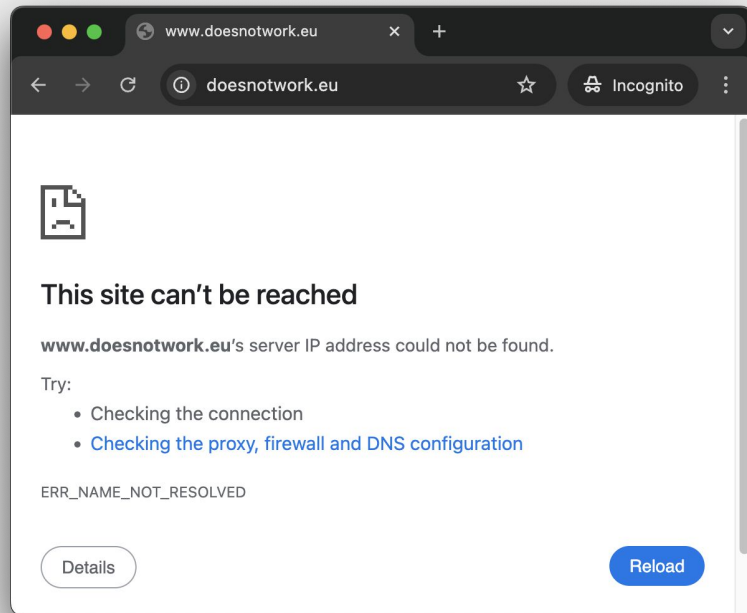


Zaměstnanec: "**První verze služby je hotová. Můžete ji vyzkoušet?**"

Pracovník 1 (v kanceláři): "**Funguje!**"

Pracovník 2 (doma): "**Funguje!**"

Pracovník 3 (doma): "**Vůbec nefunguje!**"





```
$ ping6 www.doesnotwork.eu
PING6(56=40+8+8 bytes) 2001:67c:2e8:1200::b20 --> 2001:1528:132:70::d0e5
16 bytes from 2001:1528:132:70::d0e5, icmp_seq=0 hlim=56 time=99.158 ms
16 bytes from 2001:1528:132:70::d0e5, icmp_seq=1 hlim=56 time=148.704 ms
^C
--- www.doesnotwork.eu ping6 statistics ---
2 packets transmitted, 2 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 99.158/123.931/148.704/24.773 ms

$ curl https://www.doesnotwork.eu
curl: (6) Could not resolve host: www.doesnotwork.eu
```



Připojeno k síti jen s IPv4

```
$ scutil --dns | head
DNS configuration

resolver #1
  search domain[0] : ripe.net
  nameserver[0] : 10.248.43.64
  if_index : 14 (en0)
  flags      : Request A records
```

Připojeno k síti typu dual-stack

```
$ scutil --dns | head
DNS configuration

search domain[0] : ripe.net
nameserver[0] : 2001:67c:2e8:11::c100:1365
nameserver[1] : 193.0.19.101
if_index : 14 (en0)
flags      : Request A records, Request AAAA records
```



- Přinejmenším v **macOS** a na **Windows**
- **Nedokumentovaná pravidla**
- Nekonzistentní chování podle typu použitého API (ping6 vs. curl)
- Nevíme, jak vynutit pokládání AAAA dotazů
- Na macOS lze pomocí *nedokumentovaných funkcí* `scutil` vynutit AAAA dotazy pro full-tunnel VPN

Nepříliš šťastný konec

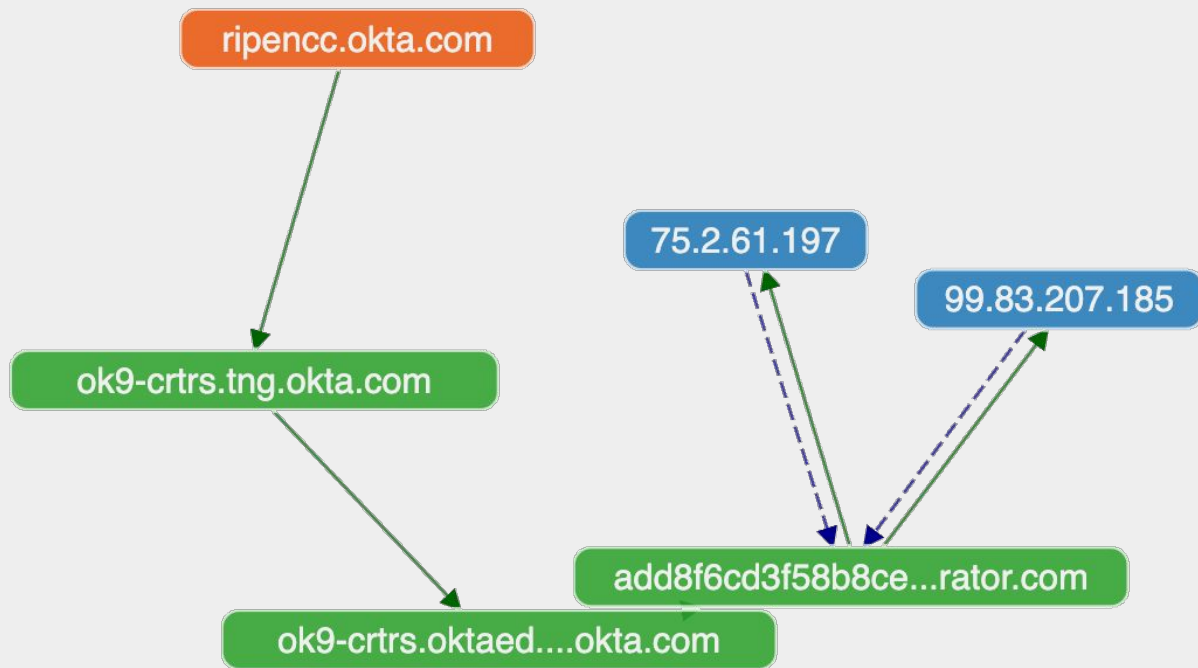


- Vrátili jsme se zpět k **dual-stacku**
- Služba je používána po IPv6 jen zaměstnanci s IPv6 konektivitou
- Naše nástroje jsou ale připraveny pro provoz serverů **pouze s IPv6**
- Objevili jsme **další překážky provozu IPv6-only**



Další překážky

Single Sign-on: Okta





Zeptali jsme se



Damiano Albani (RIPE NCC) asked a question.

March 9, 2022 at 5:28 PM

IPv6 support

Hello,

As far as I know and can see from a simple DNS resolve, Okta doesn't seem to support IPv6 connectivity.

Do you plan add support for it in the short (to medium) term?

I found a single question in the Help Center regarding IPv6, about the IP zone policy functionality:

<https://support.okta.com/help/s/question/0D50Z00008C3jm1SAB/ipv6-support-for-ip-zone-policy>

Could you give an update?

Thanks!



Deactivated User (ojovp)

Edited March 10, 2022 at 4:41 PM

Hello **@Damiano Albani (RIPE NCC)**

I hope you are having a great day

Thank you for posting, Currently IPV6 its not fully supported but we are continually hoping to provide the best customer experience, so perhaps you would like to share your use case to implement this functionality in a future release. The best method for getting our Product Managers' attention is to submit an idea to the community site. Once ideas are submitted, they are visible to other Okta admins, who can vote on them to provide more visibility and allow you to monitor the potential for future [enhancements](#). To Create an Idea:

1. Go to <https://ideas.okta.com/>
2. Enter your Okta tenant name and click "Go" (if necessary)
3. Sign in and search the Ideas page for existing feature requests to upvote, or click "Make a suggestion" to submit your own
4. Encourage the other admins in your org to upvote the idea as well

<https://support.okta.com/help/s/article/Okta-Ideas-Overview-FAQ>

Henry E.

Okta Inc



Odeslali jsme nápad

The screenshot shows the Okta Ideas interface. On the left is a blue sidebar with navigation links: Dashboard, Releases, What's Coming?, and Back to Okta Help Center. The main content area has a header with the 'Okta Ideas' logo, a search bar, and a user profile icon. Below the header is a filter dropdown set to 'Apps / Product Areas' and a 'Reset Global Filters' link. The main content is divided into two columns. The left column contains a 'Submit a Request for Okta Ideas' section with a 'Make a Suggestion' button, and a 'Recently Released' section. The right column contains a 'My Priorities (2)' section with a table of suggestions.

Vote	Title	Status	Priority
22	IPv6 Support for [company].okta.com	☐ Awaiting Feedback	
22	Support for IPv6 in Network Zones	☒ Product Review	

Nápad **nezískal žádný ohlas** od ostatních uživatelů systému Okta. 🙄



Okta nás kontaktovala s pilotní podporou IPv6

- Jsme **první zákazníci** požadující IPv6
- Mají problém **najít businessový případ** pro projekt podpory IPv6
- Mají strach z **nařízení vlády USA o podpoře IPv6-only**
- Nechtějí ztratit zákazníky z veřejného sektoru USA



Malý problém nespadaající do RIPE-772

- Musíme **vyhledávat bezpečnostní incidenty** (NIS2, SOC2, ISO 27001,...)
- Na každý server instalujeme agenta InsightIDR
- Agent sbírá logy o incidentech na **IPv4 i IPv6**
- Agent **potřebuje IPv4** pro komunikaci s centrálou 😞



Někdo se zeptal

IPv6 Proxy for InsightVM agents

■ InsightVM



aobersteiner armin

Mar 2024

How can I use an IPv6 proxy (can proxy IPv4) with the Insight VM agent?
Our servers are in an IPv6 environment with a proxy for IPv4 needs.



176 views

↩ Reply



Jsme to jen my?

Jsme natolik odlišní?



- Žádný prezentovaný problém není nijak unikátní pro **RIPE NCC**
- **Už je rok 2025.** Těžko můžeme být první, kdo něco takového zkouší
- Vláda USA už vyžaduje “**nejméně 50% aktiv používajících protokol IP** na federálních sítích běžících v režimu IPv6-only”



- Naše nástroje jsou ale připraveny pro provoz serverů **pouze s IPv6**
- Snažíme se odstranit **poslední závislosti na IPv4**
- Některé produkty jako SSO nebo SIEM nemají mnoho srovnatelných konkurenčních nabídek a ani my si nemůžeme dovolit **vyměnit podporu IPv6 za jiné důležité vlastnosti**
- Může pomoci IETF?



Otázky, připomínky



Ondrej@Caletka.cz



<https://Ondřej.Caletka.cz>

**Díky za
pozornost!**