PROVOZNÍ ŘÁD NIX.CZ, z.s.p.o.

(Verze 11 ze dne 19.6.2022 s účinností od 1.1.2023)

Článek I.
PŘEDPOKLADY ČLENSTVÍ VE SDRUŽENÍ

1.1 Každá právnická osoba žádající o členství ve sdružení NIX.CZ musí splňovat následující podmínky:

a) má přiděleno vlastní číslo autonomního systému (ASN). V případě, že právnická osoba žádající o členství ve sdružení NIX.CZ nemá přiděleno vlastní ASN, je třeba písemně doložit souhlas vlastníka tohoto ASN.

Článek II.
PŘEDPOKLADY PRO UZAVŘENÍ ZÁKAZNICKÉ SMLOUVY SE SDRUŽENÍM

2.1 Každá právnická osoba žádající o uzavření zákaznické smlouvy se sdružením NIX.CZ musí splňovat následující podmínky:

a) Má přiděleno vlastní číslo autonomního systému (ASN).
b) V případě, že osoba žádající o uzavření zákaznické smlouvy se sdružením NIX.CZ nemá přiděleno vlastní ASN, je třeba písemně doložit souhlas vlastníka ASN nebo doložit poskytování služeb IPTV či VoD.
c) Zaváže se k dodržování podmínek stanovených v Provozním řádu sdružení a v Ceníku sdružení.

Článek III.
PROVOZNÍ PODMÍNKY

3.1 Připojení do uzlů NIX.CZ, z.s.p.o. bude povoleno po zaplacení vstupního členského příspěvku dle stanov sdružení (člen sdružení) nebo po podpisu smlouvy o poskytování služeb (zákazník sdružení).

3.2 Každý člen/zákazník bude při zřízení přípojky do uzlů NIX.CZ, z.s.p.o. a při její údržbě spolupracovat s pověřeným pracovníkem sdružení NIX.CZ (dále jen „**technikem sdružení**").

3.3 Každý člen/zákazník je povinen před připojením k infrastruktuře NIX.CZ, z.s.p.o. na Extranetu sdružení uvést a nadále udržovat aktuální následující informace:

a) provozní kontakt obsahující:
   i) telefonní spojení, dosažitelné 24 hodin denně, 7 dní v týdnu,
   ii) e-mail adresu na své NOC (Network Operation Center);

b) e-mailové adresy, které budou uvedeny v seznamu NIX.CZ, sloužící pro korespondenci mezi členy/zákazníky;

c) číslo autonomního systému (ASN) pod kterým je člen/zákazník připojen;

d) plné kanonické jméno pro směrovač člena/zákazníka, které bude uvedeno v reverzních doménách (in-addr.arpa a ip6.arpa) adresního prostoru přiděleného NIX.CZ, z.s.p.o.;

e) URL na webové stránky člena/zákazníka, pokud člen/zákazník požaduje vytvoření odkazu z webových stránek sdružení;

f) e-mail pro zasílání žádostí o peering;

g) kontaktní informace člena/zákazníka.

3.5 V případě ohrožení stability a funkčnosti zařízení NIX.CZ, z.s.p.o. ze strany zařízení/přípojky člena/zákazníka má sdružení právo takový port člena/zákazníka zablokovat do doby, než dojde k vyřešení problému na straně člena/zákazníka. Technici sdružení budou v takovémto případě neodkladně informovat NOC kontakt (dle extranetu sdružení) e-mailem nebo telefonicky. Tato informační povinnost se nevztahuje na automatické zablokování portu dle bodu PI/13 přílohy I tohoto Provozního řádu.

3.6 Technické provozní podmínky pro veřejný peeringový segment (VLAN) jsou uvedeny v příloze I tohoto Provozního řádu. Technické provozní podmínky pro privátní segment (VLAN) jsou uvedeny v příloze II tohoto Provozního řádu. Technické provozní podmínky pro multicast segment (VLAN) jsou uvedeny v příloze III tohoto Provozního řádu.

Článek IV
OSTATNÍ PODMÍNKY UŽÍVÁNÍ UZLU NIX.CZ

4.1 Členové/zákazníci musí zajistit, aby jejich připojení do uzlu NIX.CZ nezpůsobilo újmu v užívání služeb NIX.CZ ostatním členům/zákazníkům.

4.2 Členové/zákazníci nesmějí provozovat nelegální aktivity přes uzel NIX.CZ.

4.3 Porušením tohoto Provozního řádu není použití některé z technik mitigace kybernetických útoků provozovaných sdružením v souladu s dokumentací publikovanou na extranetu Sdružení.

Článek V
POJIŠTĚNÍ A ODPOVĚDNOST

5.1 V případě jakýchkoliv nároků na náhradu škody, způsobené kterýmkoliv členem/zákazníkem sdružení jinému členu/zákazníku sdružení nebo přímo sdružení NIX.CZ, bude postupováno v souladu s platnými právními předpisy.

Přílohy:
Příloha I – Technické provozní podmínky pro veřejný peeringový segment (VLAN)
Příloha II – Technické provozní podmínky pro privátní segment (VLAN)
Příloha III – Technické provozní podmínky pro multicast segment (VLAN)

Příloha I

TECHNICKÉ PROVOZNÍ PODMÍNKY PRO VEŘEJNÝ PEEERINGOVÝ SEGMENT (VLAN)

PI/1. Technologií sdíleného media v uzlech NIX.CZ, z.s.p.o. je Ethernet (IEEE 802.3)

PI/2. Předávacím bodem NIX.CZ jsou následující rozhraní:

a) optický 1Gb/s port s modulem 1000BASE-LX;
b) optický 10Gb/s port s modulem 10GBASE-SR nebo 10GBASE-LR;
c) optický 100Gb/s port s modulem 100GBASE-SR10 nebo 100GBASE – LR4;
d) optický 400Gb/s port s modulem 400GBASE-FR4 nebo 400GBASE-LR4;
e) v případě požadavků na jiný, dříve nezmíněný modul, se bude postupovat dle domluvy s techniky sdružení (zejména jde o moduly ER, ZR, xWDM apod.);

PI/3. Členové/zákazníci jsou oprávnění použít veřejný peeringový segment NIX.CZ pro vnitřní tranzit jejich sítí.

PI/4. Více fyzických portů téhož člena/zákazníka zakončených na témže přepínači NIX.CZ může být spojeno do jednoho logického portu (EtherChannel). Spojení portů je konfigurováno s pomocí LACP (Slow LACPDUs).

PI/5. Každá přípojka člena/zákazníka do peeringového segmentu je omezena na 1 zdrojovou MAC adresu.

PI/6. Ethernetové rámce zasílané připojeným zařízením do sdíleného segmentu musí mít jeden z následujících ethertypes:

a) 0x0800 – IPv4;
b) 0x0806 – ARP;
c) 0x86dd – IPv6;

PI/7. Rámce zasílané do sdíleného segmentu nesmí být adresovány na multicastovou či broadcastovou MAC s následující výjimkami:

a) ARP broadcast;
b) IPv6 neighbor discovery;
c) případně další na základě povolení sdružení NIX.CZ, z.s.p.o.

PI/8. Broadcastové a multicastové rámce zasílané do sdíleného segmentu jsou omezovány.

PI/9. Provoz link-local protokolů (viz. bod PI/10) nesmí být směrován do sdíleného segmentu s výjimkou:

a) ARP (nezahrnuje Proxy-ARP);
b) IPv6 neighbor discovery.

PI/10. Link-local protokoly jsou zejména: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protokoly (CDP apod.), vnitřní směrovací protokoly (OSPF, ISIS, EIGRP), BOOTP/DHCP, PIM-SM/PIM-DM, DMVRP, Mikrotik Neighbor Discovery Protocol (MNDP), IPv6 RA a další.

PI/11. Provoz generovaný ARP, IPv6 neighbor-discovery nebo pro neznámý unicast nesmí překročit 50 paketů za vteřinu pro každý z jmenovaných

PI/12. Peeringový port hraničního routeru musí mít vypnutou funkci Proxy-ARP. Sdružení bude provádět periodickou detekci nastavení Proxy-ARP v peeringovém segmentu.

PI/13. Nově instalované porty jsou připojeny nejprve do izolovaného testovacího segmentu, kde se ověří správnost konfigurace zařízení na straně člena/zákazníka. Připojení do produkční sítě je možné po odstranění případných zjištěných nedostatků.

PI/14. V případě překročení maximálního povoleného počtu MAC adres na portu/přípojce nebo porušení bodu PI/9 může být port automaticky zablokován jako opatření pro zajištění stability infrastruktury sdružení.

PI/15. Porty připojené do sdíleného segmentu smějí využívat pouze IP adresu a masku sítě přidělenou techniky sdružení. K jednomu fyzickému (logickému) portu náleží jedna IPv4 adresa a jedna IPv6 adresa.

PI/16. IPv6 adresy musí být nakonfigurovány staticky (bez využití automatické konfigurace). IPv6 site-local adresy nesmí být používány.

PI/17. Do sdíleného segmentu nesmí být portem člena/zákazníka zasílány IP pakety s broadcast adresou sdíleného segmentu.

PI/18. Směrovacím protokolem uzlů NIX.CZ, z.s.p.o. je BGP-4 (RFC-4271) s možným použitím rozšíření MP-BGP-4 (RFC4760, RFC-2545) – pouze unicast IPv4 a IPv6 a Four-octet ASN (RFC-6793).

PI/19. Adresy sítě peeringového segmentu nesmí být oznamovány do ostatních sítí bez souhlasu NIX.CZ, z.s.p.o.

PI/20. Provoz z přípojky člena/zákazníka smí být směrován na cílovou adresu jiného člena/zákazníka pouze po vzájemném odsouhlasení, například na základě vzájemné dohody o peeringu a pouze prostřednictvím protokolu BGP-4 (viz. PI/17).

PI/21. Všechny sítě oznamované přes sdílený segment smí ukazovat pouze na router, který je oznamuje. Výjimka je možná pouze v případě aplikace technik pro mitigaci kybernetických útoků po souhlasu NIX.CZ.

PI/22. Zatížení portu(ů) používaných členy/zákazníky nesmí přesahovat 90 % v pětiminutových průměrech.

PI/23. Členy/zákazníky žádáme o dodržování níže uvedených doporučení.

a) Doporučená **peeringová politika**:

1) Mít registrovanou svoji směrovací politiku (routing policy) pro každé připojené ASN v databázi RIPE či podobném registru a udržovat ji aktuální.
2) Pro všechny sítě propagované prostřednictvím BGP mít registrovány route (resp. route6) objekty v databázi RIPE či podobném registru a udržovat je aktuální.
3) Používat as-set objekt registrovaný v RIPE db či v podobném registru.
4) Mít registrovaný záznam své firmy v PeeringDB a udržovat jej aktuální.
5) Používat monitorovací nástroje pro dohled nad propagovanými prefixy.

b) Doporučená konfigurace **peeringového routeru**:

1) Používat Control Plane Policing (CoPP) pro zabezpečení zdrojů peeringového router.
2) Používat monitoring provozu, funkce a nástroje pro detekci průniků.
3) Používat mitigační nástroje proti (D)DoS a jiným útokům, např. RTBH, IPS.
4) Používat doporučení BCP 38 pro svůj hraniční router

c) Doporučená konfigurace **peeringového portu**:

1) Vypnout ICMP a ICMPv6 redirect zprávy.
2) Vypnout ICMP a ICMPv6 unreachable zprávy.
3) Vypnout IPv6 Multicast Listener Discovery protokol.
4) Potlačit vysílání IPv6 Router Advertisementů.
5) Používat limitaci IPv6 ND cache.
6) Používat min. BFD interval 1000ms s násobitelem 5.
7) Vypnout nepoužívané služby, např. NTP.
8) Používat nastavení MTU přípojky na 1500 B.

d) Doporučená konfigurace **BGP peeringu**:

1) Nevytvářet zbytečně "route flaps".
2) Nepropagovat zbytečně specifické cesty při peeringu s ostatními peery.
3) Používat limitaci maximálního počtu komunit v atributu komunit na 64.
4) Používat limitaci maximálního počtu prodloužených komunit v atributu prodloužených komunit na 64.
5) Používat limitaci maximálního počtu čísel autonomních systémů v AS-path atributu.
6) Používat limitaci maximálního počtu povolených prefixů od IPv4 a IPv6 peerů, s automatickým, časově zpožděným restartem relace.
7) Používat agregaci IPv4 a IPv6 směrovacích záznamů v BGP databázi.
8) Používat BFD fall-over protokol pro IPv4 and IPv6 peery.
9) Používat ověřovací mechanismus pro TCP spojení s IPv4 a IPv6 peery.
10) Používat Generalized TTL Security Mechanism kontrolu IPv4 and IPv6 BGP peerů.
11) Podepsat všechny své prefixy pomocí RPKI mechanismu a vyžadovat podepisování po zákaznících které propagujete.
12) Preferovat RPKI podepsané prefixy.

e) Konfigurace BGP peeringu s Route Servery

1) Maximální délka akceptovaných prefixů je /24 v IPv4 a /48 u IPv6
2) Falešné (bogon) a nesmyslné (martian) prefixy nejsou akceptovány
3) AS-PATH není delší než 64 ASN a není podporováno agregování AS-PATH je vynucena shoda s doporučením BCP172/RFC6472
4) Číslo ASN použité pro BGP relaci s RS se musí shodovat s číslem prvního ASN v AS-PATH propagovaného prefixu
5) IP adresa parametru „next-hop" propagovaného prefixu se musí shodovat s IP adresou peeru BGP relace
6) IP prefix nesmí obsahovat Tier 1 ASN v AS-PATH
7) „Origin ASN" propagovaného prefixu musí být obsaženo v AS-SETu BGP peeru, jenž chce daný prefix propagovat
8) Router server provádí validaci RPKI, prefixy se statusem „RPKI INVALID" nejsou povoleny
9) Prefix je dále porovnáván s IRRDB (radb.net) a je povolen pouze v případě, že ma definován „route-object" v seznamu povolených ASN

Příloha II

TECHNICKÉ PROVOZNÍ PODMÍNKY PRO PRIVÁTNÍ SEGMENT (VLAN)

PII/1. Fyzické připojení se řídí dle PI/1 – PI/2 a PI/4

PII/2. Každá privátní VLAN člena/zákazníka je omezena na 2 zdrojové dynamické či statické MAC adresy (dle použité technologie).

PII/3. Broadcastové a multicastové rámce zasílané do sdíleného segmentu jsou omezovány.

PII/4. Rámce zasílané do sdíleného segmentu nesmí být typu: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protokoly (CDP apod.), vnitřní směrovací protokol PIM-SM/PIM-DM, DMVRP, a další.

PII/5. Provoz generovaný ARP by neměl překročit 20 paketů za vteřinu.

PII/6. Nově instalované porty jsou připojeny nejprve do izolovaného testovacího segmentu, kde se ověří správnost konfigurace zařízení na straně člena/zákazníka. Připojení do produkční sítě je možné po odstranění případných zjištěných nedostatků.

PII/7. V případě překročení maximálního povoleného počtu MAC adres na portu/přípojce nebo porušení bodu PII/8 může být port automaticky zablokován jako opatření pro zajištění stability infrastruktury sdružení.

PII/8. Zatížení portu(ů) používaných členy/zákazníky nesmí přesahovat 90 % v pětiminutových průměrech.

PII/9. Členům/zákazníkům se doporučuje:

a) Realizovat přímé připojení do svého hraničního směrovače bez dalších L2 zařízení.

b) Privátní VLAN je možné využít k přenášení vnitřních protokolů jako OSPF, ISIS, EIGRP, iBGP, BOOTP/DHCP, IPv6 router advertisment a dalších.

PII/10. Na portech, využívající služby privátní VLAN, je možné po písemné dohodě s techniky sdružení zvýšit nastavení MTU přípojky na nejvýše 9216 B. Člen/zákazník se zavazuje že bude dodržovat velikost MTU velikost v peeringového segmentu dle PI/22.c)9).

Příloha III

TECHNICKÉ PROVOZNÍ PODMÍNKY PRO MULTICAST SEGMENT (VLAN)

PIII/1. Fyzické připojení se řídí dle PI/1 – PI/2 a PI/4

PIII/2. Broadcastové rámce zasílané do sdíleného segmentu jsou omezovány.

PIII/3. Rámce zasílané do sdíleného segmentu nesmí být typu: IRDP, ICMP redirect, IEEE 802 Spanning Tree, VTP, vendor discovery protokoly (CDP apod.) a další.

PIII/4. Provoz generovaný ARP by neměl překročit 20 paketů za vteřinu.

PIII/5. Nově instalované porty jsou připojeny nejprve do izolovaného testovacího segmentu, kde se ověří správnost konfigurace zařízení na straně člena/zákazníka. Připojení do produkční sítě je možné po odstranění případných zjištěných nedostatků.

PIII/6. V případě překročení maximálního povoleného počtu MAC adres na portu/přípojce nebo porušení bodu PIII/8 může být port automaticky zablokován jako opatření pro zajištění stability infrastruktury sdružení.

PIII/7. Zatížení portu(ů) používaných členy/zákazníky nesmí přesahovat 90% v pětiminutových průměrech.

PIII/8. Multicast segment (VLAN) topologie je řešena jako point-to-point (zdroj-cíl).

PIII/9. Člen/zákazník je povinen se řídit IP adresací multicast provozu určenou organizací IANA, tedy skupinou adres třídy D – 224.0.0.0/4

PIII/10. Členům/zákazníkům se doporučuje:

a) Realizovat přímé připojení do svého hraničního směrovače bez dalších L2 zařízení.

b) Nepoužívat překrývající multicast adresy při mapování multicast IP na MAC adresy 32:1.

Příklad překrývajících se adres:

224.1.1.1
224.129.1.1
225.1.1.1
225.129.1.1
.
.
.
238.1.1.1
238.129.1.1
239.1.1.1
239.129.1.1

c) Multicast vlan je možné využít pro distribuci IPTV, VoD atd.

PIII/11. Na portech, využívající služby multicast VLAN, je možné po písemné dohodě s techniky sdružení zvýšit nastavení MTU přípojky na 9216 B. Člen/zákazník se zavazuje že bude dodržovat velikost MTU v peeringovém segmentu dle PI/22.c)9).