tuzfal

H.323 és a tűzfalak

Ez a dokumentum tűzfal adminisztrátorok számára készült. Amennyiben javaslata van a dokumentummal kapcsolatban, kérjük keressen meg minket a video-admin@niif.hu e-mail címen.

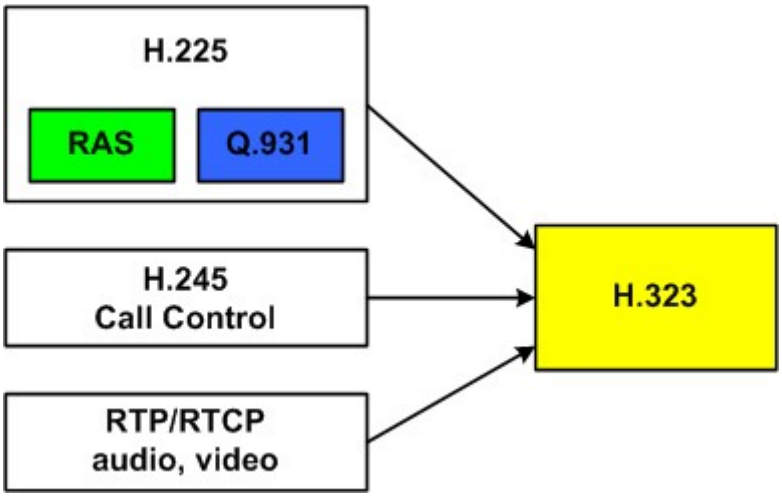
Miért nehéz ügy a H.323 és a tűzfalak együttműködése?

- H.323 egy rendkívül komplex protokoll-rendszer. A protokoll üzenetek ASN.1-gyel kódoltak, ezek vizsgáltata/visszafejtése rendkívül erőforrás-igényes a tűzfalak és NAT eszközök számára.
- Több fix és dinamikusan allokált TCP és UDP protot használ (H.245, RTP/RTCP az audió és videó stream-ek számára).
- NAT használata esetén a NAT eszközök döntő hányada nem ismeri a H.323 protokollt, így képtelen teljesíteni a címfordítással járó követelményeket (IP címek átírása a protokoll-üzenetekben).

Milyen részei vannak a H.323 protokoll-rendszernek?

A H.323 fontosabb elemei:

- H.225:
  - RAS (Registration, Admission and Status): a végpont és a gatekeeper közötti jelzések (regisztráció, hívás-engedélyezés, stb.).
  - Q.931: Hívásfelépítés jelzés-rendszer.
- H.245: Hívás-vezérlés (végpontok képességeinek egyeztetése, hívás közbeni változtatások, stb.).
- RTP/RTCP: audió és videó stream-ek szállítása és a hozzá tartozó vezérlő protokoll.



Milyen portokat használ a H.323?

A H.323 egyes alkotórészei (H.225, H.245 és RTP) az alábbi portokat használják:

H.323 protokoll	Protokoll	Port(ok)	Kommunikáció iránya
H.225	-	-	-
RAS	UDP	1719	Kétirányú, végpont-gatekeeper
Q.931	TCP	1720	Kétirányú, végpont-gatekeeper
H.245	TCP	dinamikus (1024-65535)	Kétirányú, végpont-végpont
RTP/RTCP	UDP	dinamikus (1024-65535)	Kétirányú, végpont-végpont

A dinamikus portok (1024-65535) allokációja az eggyel "alacsonyabb" szintű protokoll-kommunikációban történik (pl. H.245 esetén a Q.931, az RTP esetében a H.245 üzenetekkel).

Mit tegyek a tűzfallal?

Amit mindenképpen ki kell nyitnunk:

- RAS és Q.931 portok mindkét irányban
- RTP portok: Mivel az RTP portok dinamikusan osztódnak ki, így itt nehéz dolgunk van. A videókonferencia végpontok általában megengedik a port-tartomány korlátozását, pl. 4-8 portra. írjuk elő a fix porttaromány használatát felhasználóink számára, így nem kell felesleges biztonsági kockázatot vállalnunk (ld. példák).
- A H.245 üzeneteket fix porthasználat esetén a Q.931-es kapcsolatban tunnelezik az eszközök, így - elvileg - ezzel nem kell foglalkoznunk.

Néhány példa

Például Polycom ViewStation FX esetén navigáljunk az alábbi menüponthoz:

```
System Info
 Admin Setup (ha van, akkor admin jelszó megadása)
   LAN/H.323
     LAN/Intranet
       Firewall/LAN Connection

Use Fixed Ports: (pipa, és meg kell adni TCP és UDP fix címtartomány kezdetét, ami
alapértelmezésben 3230)
```

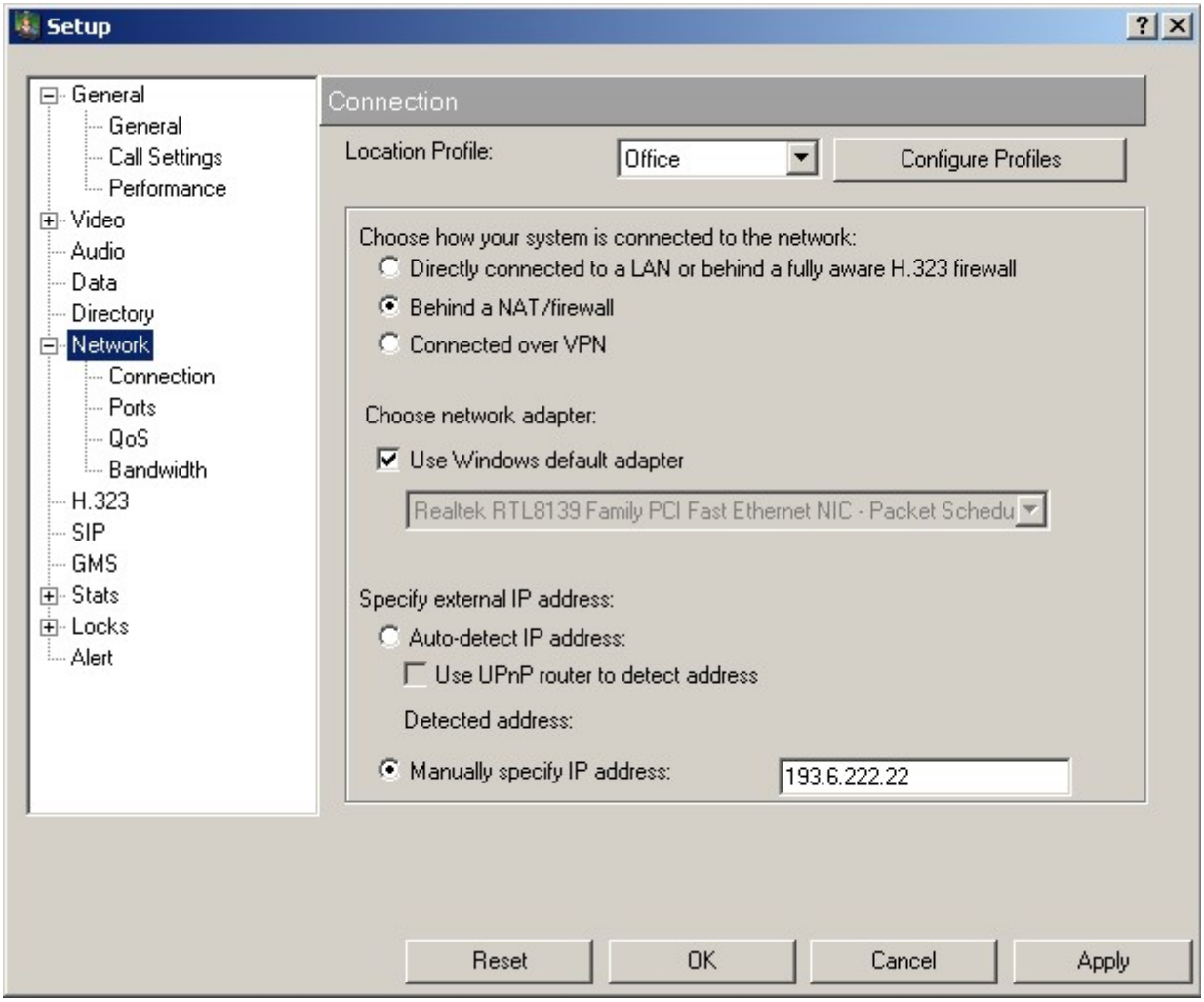
Polycom VSX 7000 végpont esetén:

```
System
  Admin Settings (ha van, akkor admin jelszó)
    Network
      IP
        Firewall

Fixed ports (pipa, TCP esetén 3230-3235, UDP esetén 3230-3253 az alapértelmezett)
```

A hardveres végpontok gyakran tartalmaznak belső MCU-t (azaz maguk tudnak max. 4-6 kliens számára osztott képernyős módban működni). Egyetlen pont-pont videókapcsolat esetén minimálisan 8 RTP (UDP) portra lesz szükségünk (1-1 az audió, videó, content és far-end camera control számára, továbbá a 4 RTCP csatorna). A belső MCU használatakor számítsunk arra, hogy ennek a többszörösére lesz szükség (csatlakozott végpontok száma x 8 port).

Polycom PVX szoftveres videókonferencia kliens esetén (Preferences menü, csavarkulcs ikon bal felül, ld. ábra):

```
Network
  Behind a NAT/firewall
  Specify external IP address (itt vagy autodetect (UPnP) vagy manuális IP megadás)

Network
  Ports
    Media port range (UDP and TCP): (alapértelmezésként a 3230-3237 tartomány van beállítva,
ezt kell a tűzfalon is megnyitni)
    Use UPnP port forwarding: (UPnP használata esetén)
```



Mi a helyzet a NAT-tal?

A H.323 kommunikáció kétirányú (kimenő és bejövő hívások), így a következő konfigurációt kell alkalmaznunk:

- Fix címfordítás beállítása (egy-egy hozzárendelés),
- Fix port-fordítás beállítása (ajánlott a fent részletezett port-tartomány szűkítést alkalmazni),
- A végpont számára allokált publikus cím beállítása a videókonferencia eszközben (külső cím) vagy UPnP használata.

Tipikus tűzfal hibák

Az alábbi tipikusan tűzfalak és/vagy NAT által okozott hibák:

- A végpont nem tud regisztrálni a gatekeeperhez: nincs nyitva a H.225 RAS port.

- A hívás kicseng (sokszor), de nem épül fel: a tűzfal nem engedi át megfelelően (mindkét irányban) a hívás-felépítéshez szükséges üzeneteket (H.225 Q.931).
- A hívás felépül, de nincs kép és/vagy hang (aszimmetrikus is lehet, azaz egyik végponton minden jónak tűnik): az RTP/RTCP portok nincsenek megfelelően kinyitva.

Proxy gatekeeper

A proxy gatekeeper egy elegáns megoldás a tűzfal és NAT átjárhatóság biztosítására. A tűzfal belső oldalára elhelyezett proxy módban működő gatekeeper tulajdonképpen egy alkalmazás szintű gateway-ként funkcionál. Ebben az esetben egy adott szervezetnek saját gatekeeper-t kell működtetnie (ilyenkor különálló GDS számtartomány igénylése is szükséges ehhez). Proxy gatekeeper megvalósításakor az ingyenes GnuGk használata ajánlott. Bővebb információ és konfigurációs példák itt.

NIIF szolgáltatás-specifikus dolgok

Directory szolgáltatás (GAB, Global Address Book): 3601 TCP port megnyitása a gab.vvc.niif.hu gép felé.

Szoftver upgrade: Amennyiben Ön NIIF tulajdonú eszközzel rendelkezik, igény lehet a végpont (általunk elvégzett) szoftver-frissítésére. Ehhez a következő tűzfal-konfiguráció módosításokat kell életbe léptetni:

- FTP: 20, 21 TCP (active FTP)
- HTTP: 80 TCP
- SNMP: 161,162 UDP
- A fentieket elegendő a 193.6.222.0/25 (menedzsment) tartomány felé engedélyezni.

Változat #1
document-uploader hozta létre 2025-08-07 12:00:01 CEST
document-uploader frissítette 2025-08-07 12:00:01 CEST