Ontwerpfase

CSNN: Virtual IoT Labs

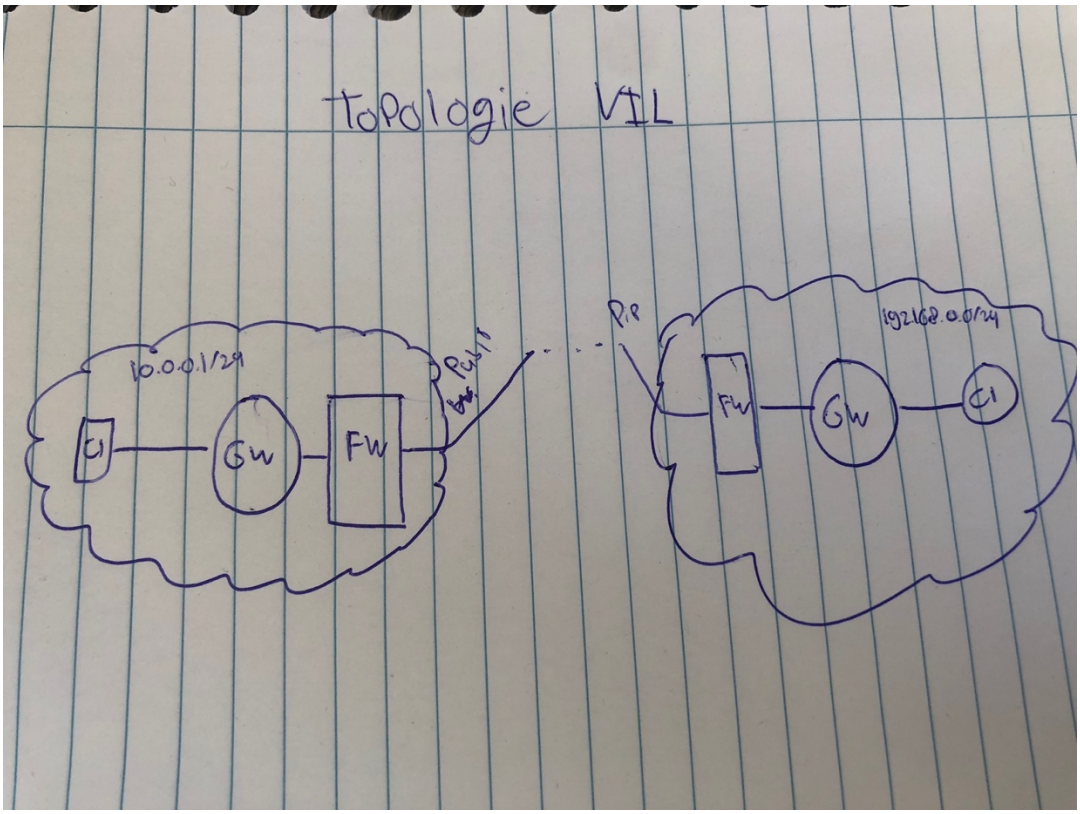
Mogelijke oplossingen

In dit onderdeel worden mogelijke oplossingen bekend gemaakt voor het, in de analysefase, gestelde probleem.

Mogelijke protocollen die achter NAT een Peer-tot-Peer verbinding kunnen faciliteren zijn:

1. STUN
2. TURN
3. ICE
4. Eenzijdige configuratie

Vervolgens zijn deze protocollen door middel van een experiment onderzocht op aansluiting bij de vereisten en randvoorwaarden die gesteld zijn door Cybersecurity Noord-Nederland. Het onderzoek is uitgevoerd in de volgende topologie:



De resultaten zijn weergegeven in de onderstaande tabel.

Protocol	Secure-By-Design	ZeroConfig	(Bijna) gratis	P2P-verbdinding
STUN	Ja	**Ja**	**Ja**	**Nee**
TURN	**Ja**	**Ja**	**Nee**	**Nee**
ICE	**Ja**	**Ja**	**Ja**	**Ja**
Eenzijdige Configuratie	**Ja**	**Nee**	**Ja**	**Nee**

Ontwerpfase

CSNN: Virtual IoT Labs

Gekozen oplossing

In dit onderdeel wordt het gekozen protocol bekend gemaakt.

ICE staat voor Interactive Connectivity Establishment en is een protocol waarmee Peer-tot-Peer verbindingen in stand gebracht kunnen worden achter NAT. Het wordt voornamelijk gebruikt in VOIP-diensten, omdat het een conceptueel vrij simpel protocol is. ICE controleert ook de verbinding op eventuele stabiliteitsproblemen. In geval van het wegvallen van de verbinding wordt de verbinding opnieuw tot stand gebracht.

Voortvloeiend uit de onderzoeksresultaten lijkt het een logische aanname om enkel voor ICE te kiezen. Echter, in de praktijk blijkt een combinatie van STUN, ICE en TURN nodig te zijn voor stabiele NAT-traversal. STUN wordt gebruikt om het publieke IP-adres van de interne client te achterhalen, hiermee kan enkel op niet-symmetrische NAT in combinatie met ICE een Peer-tot-Peer verbinding opgezet worden. In geval van symmetrische NAT is het noodzakelijk om ICE in combinatie met TURN te gebruiken om een Peer-tot-Peer verbinding te faciliteren.

Cybersecurity Noord-Nederland heeft klanten die voornamelijk gebruik maken van '*enterprise'* NAT. Hiernaast had Cybersecurity Noord-Nederland ook vragen met betrekking tot de stabiliteit van de verbinding. Ook hier biedt ICE de oplossing voor.

ICE in combinatie met STUN zal voor het grootste gedeelte genoeg zijn om een Peer-tot-Peer verbinding op te zetten achter NAT. Echter, in extreme situaties zal het nodig zijn om ICE te gebruiken in combinatie met TURN.

Door tijdslimiet is het niet aannemelijk om hiervoor een eigen implenatie voor te schrijven. Om deze reden is gekozen om gebruik te maken van het OpenSource project *Netbird*. Echter, wordt dit wel aangeraden zodat Cybersecurity Noord-Nederland niet afhankelijk is van het onderhoudt van *Netbird*.