Virtual IoT Lab

Ontwikkelen van een ZeroConfig client-to-client secure channel

Analyse

Sean Visser
Cybersecurity Noord-Nederland

Samenvatting

Inhoudsopgave

1. Inleiding

Gemakkelijk op afstand veilig een laboratorium ontsluiten, een pentestuitvoeren of toegang krijgen tot interne gedeeltes van een netwerk is niet zonder complicaties. Het opzetten van een *client-to-client secure channel* tussen twee bedrijfsnetwerken wordt verhindert door Network Address Translation(NAT). Wanneer een datapakket binnenkomt op het NAT-netwerk, zonder dat er een sessie aanwezig is in de NAT tabel, zal dit datapakket *gedropped* worden. Veel bedrijfsnetwerken hebben een of meerdere NAT(s) aanwezig in hun netwerk wegens veiligheidsoverwegingen en het gebrek aan beschikbare publieke IP adressen voor elke host/client in het netwerk. In dit verslag worden manieren onderzocht waarmee, zonder configuratie in de bedrijfsnetwerken, gemakkelijk en veilig een client-to-client verbinding opgezet kan worden.

Cybersecurity Noord-Nederland is een stichting die zich inzet voor onderzoek en kennisontwikkeling op het gebied van Cybersecurity te versnellen en zichtbaar te maken. Met deze kennis wil Cybersecurity Noord-Nederland de cyberweerbaarheid van (MKB) bedrijven vergroten. Cybersecurity Noord-Nederland wil twee bedrijfsnetwerken met elkaar verbinden zonder configuratie om een veilige omgeving te faciliteren voor lab ontsluiting, en remote pentesting.

Het verhinderen van *client-to-client* verbindingen tussen NAT netwerken is een veel voorkomend probleem binnen *IPv4-networking.* Om deze reden zijn er verscheidende manieren bedacht om de NAT te omzeilen. Dit wordt ook wel NAT-traversal genoemd. Echter veel beschreven NAT-traversal methodes zoals UDP/TCP *pinholing* en *relaying* voldoen niet aan de randvoorwaarden en vereisten gesteld door CyberSecurity Noord-Nederland. De randvoorwaarden en vereisten kunnen worden ingezien in *2.3: Vereisten en randvoorwaarden*.

Onderzoeken hoe gemakkelijk en veilig een *client-to-client* verbinding kan worden opgezet tussen twee bedrijfsnetwerken ondersteunt CyberSecurity Noord-Nederland bij haar doel om bij te dragen aan cyberweerbaarheid van (MKB) bedrijven.

In dit verslag zal allereerst de context nader verklaard worden in hoofdstuk 2. Hierna wordt de probleemstelling SMART geformuleerd in hoofdstuk 3. Vervolgens wordt in hoofdstuk 4 het probleem nader en concreet geanalyseerd. Aansluitend worden mogelijke oplossingen voor het NAT probleem geanalyseerd ten opzichte van de randvoorwaarden en vereisten in hoofdstuk 5. Verder worden Secure Channel protocollen geanalyseerd ten opzichte van de randvoorwaarden en vereisten in hoofdstuk 6. Tot slot zal er in hoofdstuk 7 een conclusie gevormd worden over welke mogelijke oplossing het best aansluit bij Cybersecurity Noord-Nederland. Hierna wordt de literatuurlijst verklaard.

2. Context

In dit onderdeel wordt de context van de opdracht verklaard. Allereerst zal het onderwerp geïntroduceerd worden in *2.1: Introductie onderwerp*. Vervolgens wordt een stakeholderanalyse uitgevoerd in *2.2: Stakeholderanalyse*. Hierna wordt in *2.3: Vereisten en randvoorwaarden* de opgestelde vereisten en randvoorwaarden van Cybersecurity Noord-Nederland verklaard. Vervolgens wordt in *2.4: Geraadpleegde literatuur* de geraadpleegde literatuur verklaard en de toepassing hiervan binnen de opdracht.

2.1. Introductie onderwerp

In dit onderdeel wordt het onderwerp van de opdracht geïntroduceerd.

Steeds meer apparaten hebben de mogelijkheid verbinding te maken met andere apparaten over het internet. Microscopen, televisies en andere meet- en huishoudapparatuur zijn hier geen uitzondering meer op. Laboratoria kunnen met deze functionaliteit mogelijk apparatuur op afstand beschikbaar stellen, televisiefabrikanten kunnen hiermee pentesters de mogelijkheid bieden om op afstand producten te pentesten, en nog veel meer is mogelijk met toegang tot het internet. Echter, het is essentieel dat het ontsluiten van laboratoria en het faciliteren van remote pentesting gemakkelijk veilig gefaciliteerd wordt. Het opzetten van de veilige verbinding dient zonder eindgebruiker configuratie voldaan te worden.

Om deze reden wil Cybersecurity Noord-Nederland het veilig ontsluiten van laboratoria, remote pentesting toegankelijk maken voor (MKB) bedrijven door een tool waarmee gemakkelijk een client-to-client secure channel opgezet kan worden tussen twee bedrijfsnetwerken.

2.2. Stakeholderanalyse

In dit onderdeel wordt een stakeholderanalyse uitgevoerd om een overzicht te krijgen van belanghebbende partijen.

Stakeholder	**Primair** Heeft direct invloed op projectaanpak of resultaat	**Secundair** Heeft indirect invloed op projectaanpak of resultaat
Interne stakeholder Betrokken bij het project vanuit de eigen organisatie	Projectmanager Teamleden	Cybersecurity Noord-Nederland
Externe stakeholder Bij het project betrokken buiten de eigen organisatie	-	Hanzehogeschool Groningen
Interface stakeholder Niet bij het project betrokken partij, die wel een legitiem belang heeft	Lokale overheid	Laboratoria (MKB) Bedrijven

Stakeholder	**Belang** Belang van stakeholder in het project	**Aanpak** Passende benaderingsaanpak voor stakeholder
Projectmanager	Bijdrage aan bedrijfsdoelstelling	Tevreden houden
Teamleden	Bijdrage aan bedrijfsdoelstelling	Tevreden houden
Cybersecurity Noord-Nederland	Bijdrage aan cyberweerbaarheid van (MKB) bedrijven	Sleutelfiguur
Lokale overheid	Verantwoording cybersecurity op nationaal niveau	Informeren
Hanzehogeschool Groningen		Informeren
Laboratoria	Verhuur van laboratoria apparatuur	Informeren
(MKB) bedrijven	Faciliteren van een veilige manier voor het ontsluiten van (gevoelige) apparatuur voor bijvoorbeeld pentesting	Informeren

2.3. Vereisten en randvoorwaarden

In dit onderdeel worden de gestelde eisen en randvoorwaarden vanuit Cybersecurity Noord-Nederland bekend gemaakt.

De opgestelde randvoorwaarden vanuit Cybersecurity Noord-Nederland zijn als volgt:

Randvoorwaarden	**Toelichting**
Security By Design	*Security by Design* is een belangrijke pilaar van Cybersecurity Noord-Nederland
ZeroConfig	ZeroConfig is een gestelde eis vanuit Cybersecurity Noord-Nederland, op deze manier kan worden bijgedragen aan de cyberweerbaarheid van (MKB) bedrijven waar geen spreke is van adequate kennis over informatie beveiliging
OpenSource Development	OpenSource development tijdens dit project draagt bij aan het beschikbaar stellen van kennis op het gebied van cybersecurity en hierdoor aan de cyberweerbaarheid van (MKB) bedrijven
(Bijna) geen kosten voor het gebruik van product	Cybersecurity Noord-Nederland wil het laagdrempelig houden voor (MKB) bedrijven om gebruik te maken van dit product. Een (hoge) prijskaart kan gebruik van het product minder aantrekkelijk maken. Hiernaast kan het voor (MKB) bedrijven aantrekkelijk zijn om bestaande betaalde diensten in te ruilen voor de (bijna) gratis dienst van Cybersecurity Noord-Nederland.

Voor het veilig faciliteren van een secure channel wordt gebruik gemaakt van het BIV-model uit informatiebeveiliging. Cybersecurity Noord-Nederland stelt hoge eisen aan het niveau van veiligheid in haar diensten en producten.

Aspect	**Vereiste gradatie**	**Implementatie** Implementatie van het BIV model wordt verder toegelicht in de design fase
Beschikbaarheid	Hoog	98% - 99,9%
Integriteit	Hoog	SHA256 (of vergelijkbaar)
Vertrouwlijkheid	Hoog	AES-256 (of vergelijkbaar) RSA-2048 (of vergelijkbaar)

2.4. Geraadpleegde literatuur

In dit hoofdstuk wordt de geraadpleegde literatuur verklaard en de toepassing van de literatuur op het ondersteunen van de probleemanalyse en de bijdrage aan mogelijke oplossingen.

De eerste bron is *TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem* van *Jeffrey L. Eppingen*. De tweede geraadplegde bron is *Peer-to-Peer Communication Across Network Address Translators* van *Bryan Ford, Pyda Srisuresh & Den Kegel*. Uit deze bronnen is algemene informatie opgedaan over NAT-traversal methoden. Hiernaast bieden deze bronnen informatie over de onderliggende werking van NAT, en wat de complicerende factoren zijn.

Ten derde is *WireGuard Endpoint Discovery and NAT Traversal using DNS-SD* van *Jordan Whited* geraadpleegd. Ten vierde is *NAT-to-NAT VPN with WireGuard* van *Staaldraad* geraadpleegd. Ten vijfde is RFC 4787 geraadpleegd voor identificatie van het probleem in het NAT protocol. Ten zesde is RFC 3489 geraadpleegd voor het identificeren van verschillende type NAT. Tot slot is *Peer-to-Peer NAT-Traversal for IPSEC* geraadpleegd. Deze bronnen bieden informatie over de implementatie van NAT-Traversal methode binnen VPN-protocollen.

3. Probleemanalyse

Er kan geen client-to-client verbinding worden opgezet in een bedrijfsnetwerk door NAT/PAT. NAT/PAT accepteert geen binnenkomende verbindingen als zij niet onderdeel zijn van een sessie. Om een sessie te beginnen dient er eerst een uitgaand pakket vanuit het netwerk verstuurd te worden. Voor het opzetten van een client-to-client verbinding tussen bedrijfsnetwerken, waarbij beide een NAT/PAT aanwezig is, is het nodig om eerst een uitgaand pakket te versturen of een poort open te zetten(pinholing). Echter, hier komen problemen bij kijken in het scenario wat Cybersecurity Noord-Nederland schetst voor het gebruik van het product. Er kan geen client-to-client verbinding worden opgezet tussen twee bedrijfsnetwerken waar NAT/PAT aanwezig is, omdat de *destination port* bij beide netwerken niet bekend is zonder pinholing.

Wanneer gekeken wordt naar RFC 4787 wordt duidelijk dat het probleem veroorzaakt wordt door NAPT. NAPT biedt de mogelijkheid voor meerdere interne hosts om gebruik te maken van hetzelfde externe IP-adres. Dit wordt mogelijk gemaakt door een sessie waarin NAPT een combinatie van publiek IP en publieke poortnummer toewijst aan het interne IP en interne poort nummer. Deze sessie wordt enkel aangemaakt wanneer een interne host eerst een uitgaand verzoek verstuurd. In de casus die Cybersecurity Noord-Nederland schetst is er geen sprake van pinholing. Hierdoor is het niet mogelijk om een NAPT-sessie te krijgen, omdat de combinatie van publiek IP en publiek poort nummer niet bekend zijn bij beide netwerken. Om deze reden zal het pakket gedropped worden.

Hiernaast zijn in de praktijk meer problemen dan de NAPT-sessie. Er zijn verschillende soorten manieren waarop een NAT zich kan gedragen. Volgens RFC 3489 zijn er vier verschillende NAT categorieën, namelijk: Full Cone NAT, Restricted Cone NAT, Port Restricted Cone NAT en Symmetric NAT.

Ook zijn er twee verschillende manieren waarop NAT sessies *mapped*, dit wordt ook wel NAT modes genoemd. De eerste is *Endpoint Independent Mapping*(EIM) en de tweede is *Endpoint Dependent Mapping*(EDM). EDM is lastiger om mee te werken voor NAT traversal, doordat EDM meer informatie bijhoudt over de sessie. Welke informatie bijgehouden wordt in EIM en EDM is in de onderstaande tabel weergegeven.

NAT mode	**Sessie informatie**
Endpoint Independent Mapping (EIM)	- Bron IP-adres - Bron IP-poort - Protocol - FIB table index
Endpoint Dependent Mapping (EDM)	- Bron IP-adres - Bron IP-poort - Bestemming IP-adres - Bestemming IP-poort - Protocol - FIB table index

4. Probleemstelling

In dit onderdeel wordt het probleem SMART geformuleerd aan de hand van het probleemanalyse in *3: Probleemanalyse*.

Er kan geen zeroconfig client-to-client verbinding worden opgezet tussen bedrijfsnetwerken, omdat NAPT geen sessie heeft in de routeringstabel voor inkomende verbindingen waarbij niet eerst een uitgaand pakket verstuurd is.

5. Mogelijke oplossingen

In dit onderdeel worden mogelijke passende NAT traversal methodes onderzocht voor Cybersecurity Noord-Nederland. NAT traversal methodes worden geanalyseerd op basis van de vereisten en randvoorwaarden die gesteld zijn door Cybersecurity Noord-Nederland.

5.1. TURN

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Nee	TURN is niet secure by design, omdat verkeer unencrypted verstuurd wordt als standaard
ZeroConfig	Nee/ja	In de casus van CSNN dient elke gebruiker van het product hun eigen STUN server in te richten, dit kan niet gemakkelijk ZeroConfig gebeuren door het verschil in factoren. Orchestration kan wel
OpenSource Development	Ja	https://github.com/coturn/coturn
Kosten	ja	Docker op azure
Beschikbaarheid	Nee	TURN kan op firewal tegengehouden worden binnen bedrijfsnetwerken, omdat het afwijkt van verkeer dat normaal is op poort 443. Hierdoor kan een hoge (schaalbare) beschikbaarheid niet gegarandeerd worden.
Integriteit	-	-
Vertrouwlijkheid	Ja	TLS kan gebruikt worden

5.2. STUN

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Nee	Verkeer wordt standaard unencrypted verstuurd
ZeroConfig	Nee	
OpenSource Development	Ja	https://www.stunprotocol.org/
Kosten	Nee	
Beschikbaarheid	Ja	Volgens “Research on Symmetric NAT Traversal in P2P applications”(DOI:10.1109/ICCGI.2006.60) kan STUN een succesratio van 99% behalen
Integriteit	-	-
Vertrouwlijkheid	Ja	Kan gebruik maken van TLS

5.3. Domain Name System - Service Discovery (DNS-SD)

Deze methode is door Cybersecurity Noord-Nederland afgekeurd vanwege moreel/ethisch bezwaar. Om deze reden is de tabel niet ingevuld.

5.4. Eenzijdige configuratie

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja*	*Afhankelijk van secure channel protocol
ZeroConfig	Nee	Een partij dient configuraties aan te brengen aan het netwerk
OpenSource Development	Ja*	*Afhankelijk van secure channel protocol
Kosten	Ja	
Beschikbaarheid	Ja*	*Afhankelijk van secure *channel protocol
Integriteit	Ja*	*Afhankelijk van secure channel protocol
Vertrouwlijkheid	Ja*	*Afhankelijk van secure channel protocol

5.5. Tweezijdige configuratie

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja*	*Afhankelijk van secure channel protocol
ZeroConfig	Nee	Beiden partijen configuraties aan te brengen aan het netwerk
OpenSource Development	Ja*	*Afhankelijk van secure channel protocol
Kosten	Ja	
Beschikbaarheid	Ja*	*Afhankelijk van secure *channel protocol
Integriteit	Ja*	*Afhankelijk van secure channel protocol
Vertrouwlijkheid	Ja*	*Afhankelijk van secure channel protocol

6. Secure Channel Protocollen

In dit onderdeel worden Secure Channel protocollen onderzocht voor Cybersecurity Noord-Nederland. De Secure Channel protocollen worden geanalyseerd op basis van de vereisten en randvoorwaarden die gesteld zijn door Cybersecurity Noord-Nederland.

6.1. OpenVPN

https://openvpn.net/

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja/Nee	Ja, omdat het veel verschillende manieren voor het opzetten van een secure channel ondersteund. Nee, omdat de attack surface groot is dankzij de grote LOC
ZeroConfig	Ja	Setup kan volledig gescript worden
OpenSource Development	Ja	OpenVPN is opensource
Kosten	Ja	OpenVPN kan gratis gebruikt worden
Beschikbaarheid	-	Afhankelijk van netwerk
Integriteit	Ja	Keuze uit verschillende hash methodes voor integriteit
Vertrouwlijkheid	Ja	Keuze uit verschillende ciphers

6.2. WireGuard

https://www.wireguard.com/

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja	WireGuard is gemaakt met de ‘security through simplicity’ mentaliteit
ZeroConfig	Ja	Setup kan volledig gescript worden
OpenSource Development	Ja	WireGuard is opensource
Kosten	Ja	WireGuard is gratis
Beschikbaarheid	-	Afhankelijk van netwerk
Integriteit	Ja	BLAKE2
Vertrouwlijkheid	Ja	ChaCha20 & Poly1305

6.3. IPSec

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja	Ja, het is een standaard bedacht met security als gr
ZeroConfig	Ja	Setup kan volledig gescript worden
OpenSource Development	Ja	IPSec is een opensource standaard
Kosten	Ja	IPSec is gratis
Beschikbaarheid	-	Afhankelijk van netwerk
Integriteit	Ja	IPSec is een standaard waarbij invullingen zoals Hashing algoritmes door de implementatie ingevuld kan worden
Vertrouwlijkheid	Ja	IPSec is een standaard waarbij invullingen zoals Encryptie algoritmes door de implementatie ingevuld kan worden

IPSec in AH mode is niet geschikt voor NAT-traversal omdat IPSec in AH mode faalt zodra de buitenste IP header aangepast wordt. Dit heeft geen invloed op IPSec in ESP mode.

6.4. SSL/TLS

Randvoorwaarde/vereiste	**Voldoet** Geeft aan of de NAT traversal methode voldoet	**Reden** Geeft beredenering voor de keuze
Security By Design	Ja	Ja, het is een standaard bedacht met security als gr
ZeroConfig	Ja	Setup kan volledig gescript worden
OpenSource Development	Ja	IPSec is een opensource standaard
Kosten	Ja	IPSec is gratis
Beschikbaarheid	Nee*	Afhankelijk van netwerk. *SSL/TLS VPN's kunnen traag zijn doordat zij hogere implementaties zijn(Webbased VPN).
Integriteit	Ja	IPSec is een standaard waarbij invullingen zoals Hashing algoritmes door de implementatie ingevuld kan worden
Vertrouwlijkheid	Ja	IPSec is een standaard waarbij invullingen zoals Encryptie algoritmes door de implementatie ingevuld kan worden

7. Conclusie

TURN NAT Traversal methode voldoet aan de vereisten en randvoorwaarden die gesteld zijn door Cybersecurity Noord-Nederland. Secure Channel protocollen voldoen aan de gestelde eisen, echter wordt er voor dit project gebruik gemaakt van “WireGuard”. Er is voor “WireGuard” gekozen, omdat “WireGuard” voldoet aan de gestelde eisen en “WireGuard” heeft minder overhead dan andere secure channel protocollen.

Discussie

Er kan ook gekeken worden naar oplossingen waarbij een derde partij geïntroduceerd wordt om de secure channel te faciliteren. Hiermee kan voor afnemende partijen ZeroConfig een secure channel opgezet worden. Echter, hier kunnen extra kosten bij komen.

Lage kosten manieren waarbij een derde partij geïntroduceerd wordt zijn:

1. OpenDHT(https://github.com/manuels/wireguard-p2p)
2. Azure Lambda Serverless
3. Discord Project NAT Traversal
4. Detour Encrypted Routed Protocol (tailscale)

Literatuurlijst

De eerste bron is *TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem* van *Jeffrey L. Eppingen*. De tweede geraadplegde bron is *Peer-to-Peer Communication Across Network Address Translators* van *Bryan Ford, Pyda Srisuresh & Den Kegel*. Uit deze bronnen is algemene informatie opgedaan over NAT-traversal methoden. Hiernaast bieden deze bronnen informatie over de onderliggende werking van NAT, en wat de complicerende factoren zijn.

Ten derde is *WireGuard Endpoint Discovery and NAT Traversal using DNS-SD* van *Jordan Whited* geraadpleegd. Ten vierde is *NAT-to-NAT VPN with WireGuard* van *Staaldraad* geraadpleegd. Ten vijfde is RFC 4787 geraadpleegd voor identificatie van het probleem in het NAT protocol. Ten zesde is RFC 3489 geraadpleegd voor het identificeren van verschillende type NAT. Tot slot is *Peer-to-Peer NAT-Traversal for IPSEC* geraadpleegd. Deze bronnen bieden informatie over de implementatie van NAT-Traversal methode binnen VPN-protocollen.

1. *TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem* van *Jeffrey L. Eppingen*
2. *Peer-to-Peer Communication Across Network Address Translators* van *Bryan Ford, Pyda Srisuresh & Den Kegel*
3. *WireGuard Endpoint Discovery and NAT Traversal using DNS-SD* van *Jordan Whited*
4. *NAT-to-NAT VPN with Wireguard* van *Staaldraad*
5. *RFC 4787*
6. *RFC 3489*
7. *Peer-to-Peer NAT-Traversal for IPSec*