OPC in der Praxis

Damit sie das Praktikum im Zusammenhang verstehen, und die Kommunikationswege nicht "geheimnisvoll" bleiben, reden wir zunächst über praxisgerechte Zugriffe auf Anlagen über das Internet.

1) Firewallzugriff

Jedes ernsthafte Netz ist über Firewalls gesichert. Betrachten Sie hierzu das Labornetz der Technikerschule :
https://portal.ts-muenchen.de/index.php/labornetz-ait

Es gibt hier zwar auch einen Teil vor der Firewall (demilitarisierte Zone DMZ), in der die Server selber auf ihre Sicherheit achten müssen. Aber der größte Teil des Netzes befindet sich hinter der Firewall. Das liegt vor auch daran, daß nicht für alle Rechner gültige IP-Adressen vorhanden sind (die kosten ja was !).

Die Kommunikation nach außen geschieht nun so, daß bei einem Request von innerhalb des Intranet (hinter der Firewall) als Router die Firewall selbst konfiguriert ist.
Diese merkt sich, wer gefragt hat, und schickt die Frage unter ihrer eigenen Adresse ins Internet. Wenn eine Antwort kommt, schaut sie nach wer gefragt hat, und leitet dem die Antwort weiter. Diese Methode heißt "Source-NAT" (network address translation).

Das geht auch andersrum, das nutzen wir :

Wenn von außen angefragt werden soll, kann man die Anfrage (z.b. auf einen OPC-Server innen) wieder direkt an die Firewall stellen. Es wird z.b. der Socket 62.245.200.166:4841 als Ziel angegeben. 62.245.200.166 ist die IP der Firewall, 4841 habe ich als Zielport für OPC von außen festgelegt.
Die Firewall erkennt am Port 4841, daß sie das weitergeben muß, und schickt die Anfrage an 1.0.7.10:4840, das ist eine SPS im Labornetz. Diese Methode heißt "Destination NAT".

2) SecureShell – Tunnel

Man braucht dazu im Netz einen Rechner, der sowohl von außen mit einer gültigen IP erreichbar ist (also in der DMZ steht), als auch einen Zugang (zweite Netzkarte) ins Intranet hinter der Firewall hat.

Dieser Rechner muß ein verschlüsseltes Kommunikationsprotokoll beherrschen, das in der Lage ist, andere Protokolle zu "tunneln". Man verwendet meist das "Secure Shell" – Protokoll (ssh) aus der UNIX-Welt. Es werden dabei die Datenpakete anderer Protokolle (bei uns OPC) in die Pakete des verschlüsselten Protokolls (ssh) eingebaut, und im Internet geschickt.

Im Labornetz sind dafür zwei linux-Rechner installiert : brunello (62.245.200.163) und chianti (62.245.200.162).

Wenn ich auf meinem Windows-Rechner daheim einen ssh-Tunnel zu chianti öffne, kann ich auf den damit konfigurierten Ports z.b. OPC-Daten an chianti schicken, die dieser dann auf seiner zweiten Netzkarte an den gewünschten Teilnehmer im Intranet weitergibt. Für mich erscheint das so, als würde ich direkt lokal den Zielteilnehmer ansprechen.

Praktikum (Vorbereitung)

Machen Sie erst weiter, wenn Sie die obigen 3 Seiten wirklich verstanden haben. Bei Schwierigkeiten suchen sei erst mal im Web, da gibt es für DNat und ssh-Tunneling massenhaft gute Erklärungen !

OPC-Client
Am Besten verwenden sie den im Skript beschriebenen von Softing. Damit können sie OPC-Requests schicken :
https://portal.ts-muenchen.de/Portaldateien/praxis/Softing_OpcUaClient1.47.0.exe

Videostream :
Bauen Sie einen Stream mit dem VLC-Player (Medien/Netzwerk-stream zur Adresse : rtsp://62.245.200.164/12) auf. Login : Gast, Passwort : tsm

Installieren Sie den OPC-Client in ihrem Windows.
(Keine Sorge, seriöse Software, keine Virengefahr)

Bei ersten Start wird eventuell ihre Firewall fragen, ob sie Ports freigeben darf, das müssen Sie bestätigen.

Praktikum (Anlage)

Sie sollen von zuhause auf die Modellfabrik zugreifen, und zwar auf einem "professionellen" also mit ausreichend Security ausgestatteten Weg.

Das kann jeweils immer nur Einer !
Deshalb gibt es dafür eine timetable, in der Sie sich Zeiten an der Modellfabrik buchen können. Ich habe keine Prüfmechanismen hinterlegt und baue auf ihre Kooperation. Arbeiten Sie bitte ausschließlich in den von Ihnen reservierten timeslots !

https://portal.ts-muenchen.de/index.php/modellfabrik
dort den link "Praktikum"

Ich habe für Sie die SPS-Programme so verändert, daß sie mit einer Fehlbedienung nichts beschädigen können. Als Schnittstelle zu der SPS stehen am OPC-Servern der SPS (Modul 1 : Wago) die Tags “Ready”, “Start” und “Order” bereit.
Dies ist eine vereinfachte Variante der “Standardschnittstelle” in der Modellfabrik.
Die Tags haben folgende Funktionen :

Ready : Mit Ready = 1 zeigen die Anlagenmodule ihre Betriebsbereitschaft. Vor steuernden Zugriffen auf die Anlage prüfen Sie, ob Ready = 1. Ist das nicht der Fall, dürfen sie keine Aktionen ausführen, es muß auf SPS-Ebene der Fehler gesucht werden. Dazu schicken Sie mir eine Email.

Order : Im Normalbetrieb habe die Anlagenmodule eine Reihe von Funktionsabläufen, die durch verschiedene Orders ausgelöst werden. Für unser Praktikum habe ich alle Orders bis auf “10” deaktiviert. Vor Starten des Moduls ist Order auf 10 zu setzen, das Aktiviert den Testbetrieb. Einer der Bandstopper wird hin- und herlaufen.

Start : Mit Start = 1 wird die in Order angelegte Funktion getriggert. Die Anlagenfunktion läuft ab. Für das Praktikum wird Order und Start automatisch rückgesetzt.

Busy : Busy = 1 zeigt eine laufende Mechanikaktion.

Modellfabrik :

Nutzen Sie die Gelegenheit, sich schon mal ein wenig mit der Anlage vertraut zu machen. Lesen Sie hierzu die Beschreibung : Anlagenfunktion im Detail auf dieser Seite : https://portal.ts-muenchen.de/index.php/modellfabrik

Um die Funktion beobachten zu können, machen Sie parallel zum OPC-Client einen Stream auf, wie oben beschrieben.

Praktikum

Sie haben die Software geladen und installiert.
Sie haben sich die Bedienung der Software angeschaut.
Sie haben die Steuerung der Anlage im Testbetrieb verstanden
Sie haben sich ein Zeitfenster reserviert

Versuch 1 :

Greifen Sie auf Modul 1 (Wago) über die Firewall des Labornetzes zu. Die Firewall wird auf Anfragen nach Port 4841 mit DNat reagieren, und diese an 1.0.7.10:4840 weiterleiten. Machen Sie den selben Versuch wie oben !

Versuch 2 :

Legen Sie bei Versuch 2 eine Subscrition auf Busy, so daß sie die Funtkionsdauer der Mechanik in OPC sehen können.

Den dreitten Versuch, über einen ssh_tunnel zuzugreuifen, habe ich rausgenommen, weil er bei vielen große Probleme gemacht hat. vermutlich lassen manche Provider die OPC-Ports nicht durch.