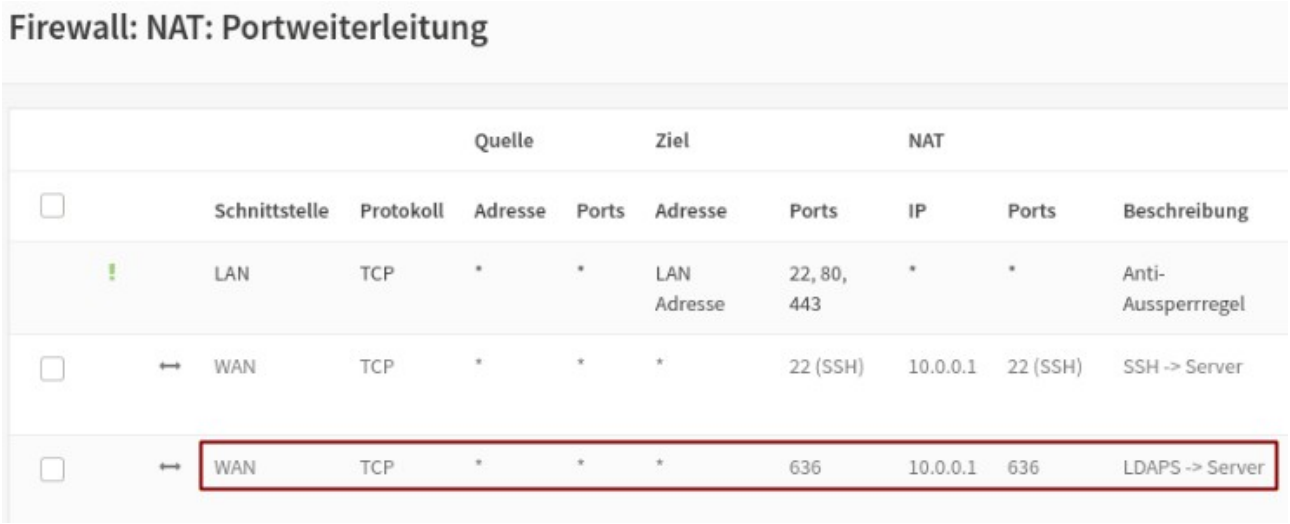
Externe Authentifizierung von Moodle gegen das AD von linuxmuster.net 7

1. Firewall-Einstellungen

Die OPNsense-Firewall muss so konfiguriert werden, dass Anfragen über den LDAPS-Port 636 an den Server weitergeleitet werden. In der Konfigurationsoberfläche ist unter *Firewall | NAT | Portweiterleitung* eine entsprechende Regel anzulegen. Wenn Sie die vom Verein bereitgestellte Appliance verwendet haben, ist die Regel schon vorbereitet.



In dem Fall muss die Regel nur noch aktiviert

und übernommen werden.

2. Moodle-Einstellungen

Unter *Website-Administration | Plugins | Authentifizierung | LDAP-Server* sind die folgenden Einstellungen zu machen. Nicht aufgeführte Optionen lassen Sie auf der Standard-Einstellung bzw. leer.

LDAP-Server-Einstellungen	
Host Url[1]	ldaps://server.linuxmuster.lan
Version	3
TLS benutzen	Nein
LDAP-Codierung	utf-8
Bind-Einstellungen	
Anmeldename[2]	CN=global-binduser,OU=Management,OU=GLOBAL,DC=linuxmuster,DC=lan
Kennwort[3]	geheim
Nutzertyp	MS ActiveDirectory
Kontexte[4]	OU=schools,DC=linuxmuster,DC=lan
Subkontexte	Ja
Kennwortänderung fordern	
Kennwortänderung fordern	Nein
Standardseite zur Kennwortänderung nutzen	Nein
Kennwortformat	Nein
Einstellungen zum Ablauf von LDAP-Kennwörtern	
Ablauf	Nein
Ablaufwarnung	Leer
Ablaufmerkmal	Leer
GraceLogins	Nein

1 Verwenden Sie hier den vollständigen Namen ihres Servers oder die IP-Adresse.
2 Ersetzen Sie *DC=linuxmuster,DC=lan* entsprechend Ihrer Domäne.
3 Das Kennwort des Bind-Users finden Sie auf dem Server in der Datei `/etc/linuxmuster/.secret/global-binduser` (root-Rechte erforderlich).
4 Ersetzen Sie *DC=linuxmuster,DC=lan* entsprechend Ihrer Domäne.

Merkmal für GraceLogin	Leer
Nutzererstellung aktivieren	
Nutzer/innen extern anlegen	Nein
Kontext für neue Nutzer/innen	Leer
Zuordnung von Systemrollen	
Kursersteller/in-Kontext[5]	OU=teachers,OU=default-school,OU=schools,DC=linuxmuster,DC=lan
Synchronisierung von Nutzerkonten	
Entfernte externe Nutzer	Intern löschen
Status von lokalen Nutzerkonten synchronisieren	Nein
NTLM-SSO	
Aktivieren	Nein
Subnet	Nein
MS IE fast path?	NTLM mit allen Browsern versuchen
Datenzuordnung	
Daten übernehmen (Vorname)	givenName
Daten übernehmen (Nachname)	sn
Daten übernehmen (E-Mail-Adresse)	Leer

Vergessen Sie nicht abschließend die Änderungen zu sichern (Schaltfläche am Seitenende) und den LDAP-Server in der Übersicht der *Aktiven Plugins zur Authentifizierung* zu aktivieren.

5 Ersetzen Sie *DC=linuxmuster,DC=lan* entsprechend Ihrer Domäne.

3. Host-Einstellungen

Gegebenenfalls muss auf dem Moodle-Host sicher gestellt werden, dass das selbstsignierte Zertifikat des Servers bei der LDAP-Abfrage akzeptiert wird.

Auf dem Host selbst geschieht das durch den Eintrag

```
TLS_REQCERT never
```

in der Datei */etc/ldap/ldap.conf*.

Läuft die Moodle-Instanz in einem Docker-Container, reicht man diese Datei als readonly Volume an den Container durch. Der Eintrag in der Datei *docker-compose.yml* lautet dann:

```
    volumes:
      - '/etc/ldap/ldap.conf:/etc/ldap/ldap.conf:ro'
```

[Netzwerke/Linux]
[Thomas Schmitt]
[16.03.2020]