

Technische Doku

BelWü

Besonderheiten von OctoGate
Firewalls in Zusammenarbeit mit
BelWü

OctoGate
EINFACH. SICHER. GESCHÜTZT. -

Version 1.0 FINAL

Inhalt

1	Zusammenfassung	4
2	Anpassung der MTU – Size	5
3	IP Adress – Umsetzung	9

1 Zusammenfassung

Historie

Die OctoGate Firewall wird in Baden Württemberg zusammen mit der Musterlösung des Landesmedienzentrums in großer Stückzahl eingesetzt. In der Praxis ergeben sich bei einem Anschluß an das BelWü – Netz einige Dinge die es zu beachten gilt.

MTU - Size

Eine Netzwerkverbindung über das Internet besteht aus einem logischen Datenkanal. Beide Parteien können auf dem Kanal kommunizieren durch das Senden von Datenpaketen einer festen Größe, der sogenannten MTU – Size.

https://de.wikipedia.org/wiki/Maximum_Transmission_Unit

Die MTU Size der BelWü – Leitungen befindet sich nicht in dem von der OctoGate vorkonfigurierten Bereich und muss daher OctoGate – Seitig angepasst werden.

Außenanbindung / IP Adresse

Im Internet existieren private und öffentliche IP – Adressen. Diese dienen der einwandfreien Paketsteuerung in der Kommunikation zwischen verschiedenen Systemen. So ähnlich wie eine postalische Adresse in der richtigen Welt. BelWü setzt die Adressen der Schule teilweise und unnötigerweise auf andere Adressen um. Das ist so lange kein Problem wie man nicht aktiv aus dem Internet auf Schulhalte (Dokumente, Sharepoint, Terminalserver in der Schule, etc.) von außen zugreifen muss. Dann wird die BelWü Adressumsetzung für die OctoGate zum Problem.

2 Anpassung der MTU – Size

Wie erkenne ich fehlerhafte MTU – Size ?

Zunächst sei nochmals betont dass es sich nicht um einen Fehler seitens BelWü sondern um eine Konfigurationsinkompatibilität handelt die es zu beseitigen gilt. Auch nicht jeder BelWü Anschluß ist betroffen.

Ein einfacher Test vom paedML Active Directory Controller aus sollte Aufschluß geben:

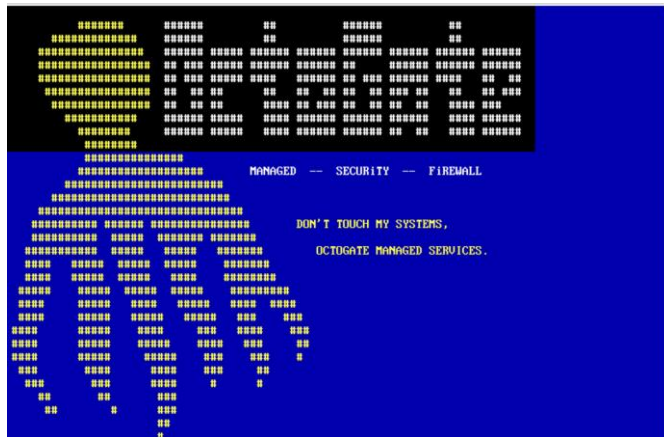
```
C:\Users\Frank Menne>ping -l 1500 8.8.8.8

Ping wird ausgeführt für 8.8.8.8 mit 1500 Bytes Daten:
Antwort von 8.8.8.8: Bytes=1500 Zeit=10ms TTL=56
Antwort von 8.8.8.8: Bytes=1500 Zeit=11ms TTL=56
Antwort von 8.8.8.8: Bytes=1500 Zeit=10ms TTL=56
Antwort von 8.8.8.8: Bytes=1500 Zeit=10ms TTL=56
```

Mit „-l 1500“ werden Pakete mit einer 1500 byte MTU Size verschickt und beantwortet. In o.g. Fall besteht kein MTU - Problem. Kommt hier eine Fehlermeldung muß man der OctoGate auf der VMware ESXI Konsole eine veränderte MTU – Size vorgeben.

Welche MTU Size das ist, kann man durch weitere PING – Kommandos herausfinden. Reduzieren Sie die Zahl 1500 in kleinen Schritten bis minimal 1290 und prüfen Sie das Ergebnis des PING.

Einstellung auf der Konsole der OctoGate (ab Version 3.0.24)



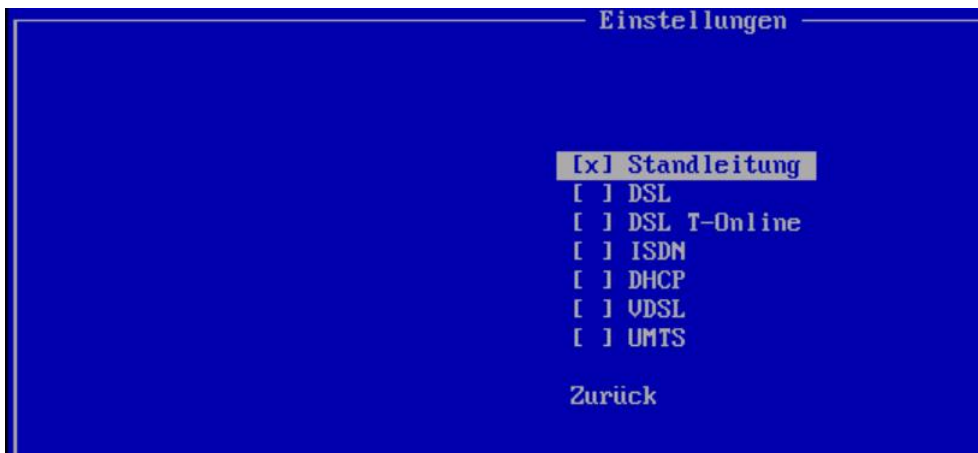
Mit ALT+F2 kommt man in den Einstellungsdialog:



Auf „Einstellungen“ gehen (Pfeil unten + ENTER)



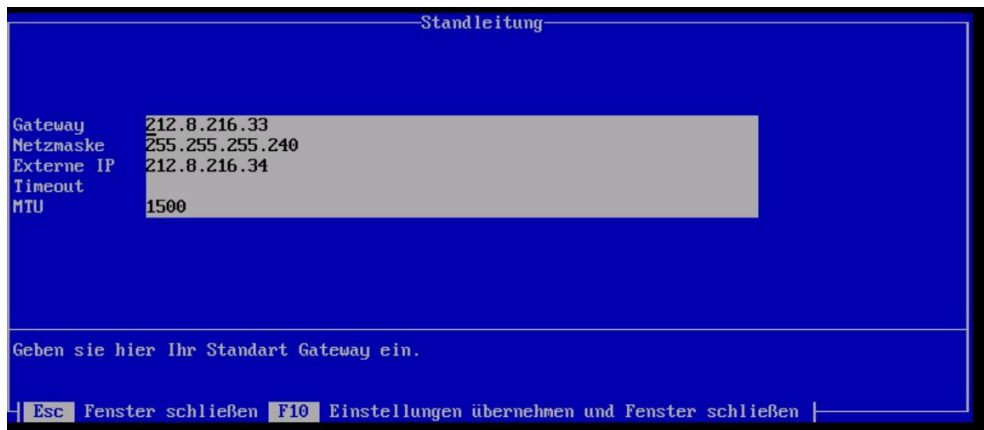
Internetverbindung



Dort sollte „Standleitung“ angewählt sein. Dann ENTER

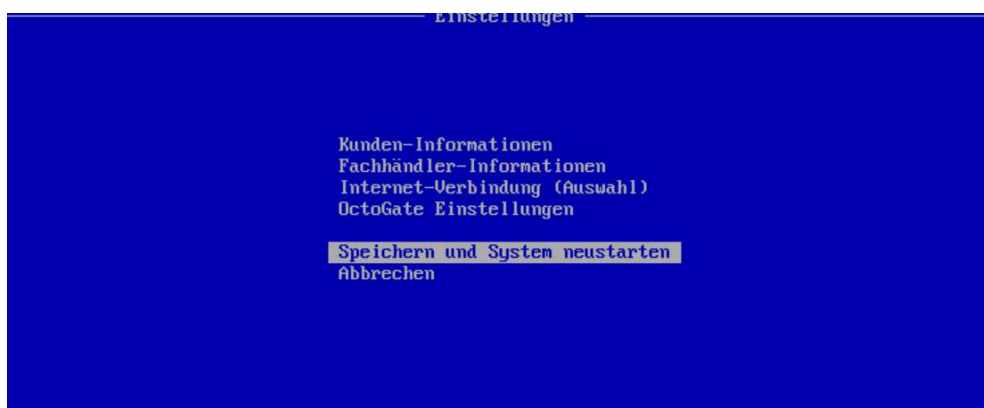
Achtung:

Ist hier nicht „Standleitung“ angewählt, so haben Sie kein MTU – Problem und können mit ESC abbrechen.



Nun die MTU ändern und mit F10 speichern.

Dann 2 x ESC und „Speichern und Neustart“ anwählen:



3 IP Adress – Umsetzung

In einer BelWü – Standleitungskonfiguration wird der OctoGate eine Öffentliche IP zugewiesen. Verbindet sich die OctoGate mit einem „Ziel – Webserver“ im Internet, so ändert BelWü die Quell – IP (141.131.12.14 im Beispiel) in eine BelWü – Sammel – IP um (141.125.1.1) welche der Ziel – Webserver sieht und darauf antwortet. BelWü schickt dann die Antwort an die OctoGate weiter.

Geht ein „Schüler mit Dokumentenzugriff“ aktiv von außen auf die echte OctoGate IP (hier 141.131.12.14) so kommt er auch ohne Umsetzung seitens BelWü zum Ziel . Die Antwort der OctoGate (vor allem bei UDP Paketen) wird aber wieder von BelWü verändert. Dadurch funktionieren einige Dienste in der OctoGate (OctoVPN beispielsweise) nicht korrekt.

