Einrichtung von TightGate-Pro (Active Directory)

Nachdem die Vorbereitung des Active Directory Servers für die Benutzerauthentisierung mit TightGate-Pro abgeschlossen ist und die erzeugte Keytab-Datei sowie die CA für die LDAPS-Kommunikation ins Transfer-Verzeichnis des Benutzers ***config*** auf TightGate-Pro kopiert wurden, kann mit der abschließenden Konfiguration am TightGate-Pro begonnen werden.

So geht's

- Anmeldung als Administrator ***config*** und Wechsel in das Menü **System-Vorgaben.**
- Auswahl des Menüpunkt **Benutzerverz. automatisch für** und dort **Ja** auswählen.
- Auswahl des Menüpunkts **Authentisierungs-Methode** und dort **AD** auswählen. Nach der Auswahl erscheinen unterhalb des Menüpunktes weitere Menüpunkte.
- Die Konfiguration der weiteren Menüpunkte erfolgt anhand der nachfolgenden Tabelle.

Menüpunkt	Beschreibung	Beispielwert
Kerberos Realms*	Angabe des REALMS,der DNS-Domäne, des Kerberos Admin Servers sowie der zuständigen KDCs in der Form: REALM:DNS-Domäne:Admin-Server:KDC1:KDC2... **Hinweis:** Der Admin-Server, sowie die KDCs können sowohl als IP-Adresse oder als Name (FQDN) eingetragen werden.	AD.DOMAIN.LOCAL:ad.domain.local:192.168.5.100:192.168.5.100
Importiere Kerberos Host Keytab*	Auswahl der im Transfer-Verzeichnis von ***config*** abgelegten Keytab-Datei. **Hinweis:** Die Keytab-Datei kann nach dem **Speichern** und **Anwenden** der Einstellungen wieder aus dem Transfer-Verzeichnis gelöscht werden.	mp.keytab
Transfer-MIME-Typen-Gruppen*	Definiert Anzahl und Inhalt der Gruppen von MIME-Typen, die AD-gesteuert über die Dateischleuse von TightGate-Pro transferiert werden dürfen. Es können maximal 99 Gruppen angelegt und beliebig mit MIME-Typen bestückt werden. Jeder dieser Gruppen können im Active Directory (AD) Benutzer zugewiesen werden. Ist ein Benutzer in keiner Transfergruppe, kann er keine Dateien über die Dateischleuse übertragen. Die Transferberechtigungen der Gruppen sind kumulativ.	2
TG-Gruppenbasierte Anmeldung*	Legt fest, ob die tg*-Gruppen aus dem AD ausgelesen werden. Bei **Nein** wird nur geprüft, ob der Benutzer existiert und authentisiert wird. Nur wenn für diesen Menüpunkt **Ja** ausgewählt wurde, werden die nachfolgenden Menüpunkte verfügbar.	Ja
Weitere AD-Servern automatisch suchen*	Wird dieser Menüpunkt aktiviert, so wird im Hintergrund bei den eingetragenen DNS-Servern nach SRV-Einträgen der Kerberos-Domänen gesucht. In den SRV-Einträgen sind die zuständigen LDAP-Server zu finden. Ohne diese Einstellung werden nur die im REALM genannten Server genutzt. Wird dieser Menüpunkt aktiviert, so erscheint nachfolgend ein Menüpunkt zum Ausschließen bestimmter AD-/LDAP-Server.	Nein
Ausgeschlossene LDAP-Server*	Hier können einzelne Server (DCs oder GCs) explizit von der Nutzung ausgeschlossen werden.	-
LDAP-Protokoll*	Festlegung des zu verwendenden Protokolls für die Anbindung an den Active-Directory Server. **Hinweis:** Grundsätzlich sollte die Kommunikation von TightGate-Pro mit dem AD-Server nur mit einem funktionierenden Protokoll (LDAP oder LDAPS) erfolgen. Vorzugsweise sollte das Protokoll LDAPS eingesetzt werden. Zu Testzwecken können beide Protokolle aktiviert werden.	LDAPS

Menüpunkt	Beschreibung	Beispielwert
TLS-Zertifikat für LDAPS ignorieren	Ignoriert die Gültigkeit eines LDASP-Zertifikats bei der Anmeldung. Diese Option sollte möglichst nicht verwendet werden, kann aber bei der Übergangsphase wenn ein LDAPS-Zertifikat ausgetauscht wird hilfreich sein.	
Importiere LDAPS-Custom-CA*	Dieser Menüpunkt erscheint nur, sofern beim LDAP-Protokoll LDAPS oder LDAP+LDAPS ausgewählt wurde. Hier wird das notwendige Zertifikat zur verschlüsselten LDAPS-Kommunikation importiert. Die benötigte CA muss sich bereits im Transfer-Verzeichnis des Administrators ***config*** befinden, dann kann sie über diesen Menüpunkt importiert werden. **Hinweis:** Die Custom-CA muss in der Base64-Kodierung vorliegen und kann nach dem Import wieder aus dem Transfer-Verzeichnis gelöscht werden. Es ist darauf zu achten, dass der Dateiname der CA keine der Sonderzeichen "()§!`°&; enthält, da der Import sonst fehlschlägt. **Achtung:** Alle Zertifikate müssen einzeln importiert werden, es ist nicht möglich eine Zertifikatskette in einer Datei zu importieren!	-
Entferne LDAPS-Custom-CA*	Entfernen einer bereits hinterlegten Custom-CA für die LDAPS-Kommunikation. Dieser Menüpunkt erscheint nur, wenn eine LDAPS-Custom-CA auf TightGate-Pro importiert wurde.	-
Klarname beim Anmelden aus AD lesen*	Wird dieser Menüpunkt auf **Ja** gesetzt, so werden bei jeder Anmeldung einer Benutzerkennung der zugehörige Klarname aus dem AD-Server abgefragt und im TightGate-Pro gespeichert. Als Administrator ***maint*** werden diese dann unter der **Benutzerverwaltung** angezeigt. Wird der Wert auf **Nein** gesetzt, so erfolgt eine weitere Abfrage, ob alle bisher im TightGate-Pro gespeicherten Klarnamen gelöscht werden sollen. Wird dies bestätigt, werden alle Klarnamen gelöscht und fortan keine Klarnamen mehr bei Benutzeranmeldungen vom AD-Server abgerufen.	Ja

Nachdem die Einstellungen vorgenommen wurden, sind diese über den Menüpunkt **Speichern** zu sichern und über den Menüpunkt **Anwenden** zu aktivieren.

Überprüfung der Einstellungen

Die Korrektheit der Einstellungen bei der Nutzung eines Active Directory kann als Administrators ***config*** über den Menüpunkt **Netzwerk prüfen** kontrolliert werden. Folgende Tests sollten von TightGate-Pro mit OK bestätigt werden, damit die Voraussetzung für die Zusammenarbeit mit dem AD gegeben ist:

Testname	Bei bestandener Prüfung	Bei Fehlern	Fehlerbehebung
Kerberos realm [Names des AD-Servers]			
KDC 1 mit TCP:	OK	Failed!	Der TightGate-Pro kann den KDC nicht über den TCP Port 88 erreichen. Häufigste Ursache dafür ist, dass eine Firewall zwischen TightGate-Pro und dem KDC dies verhindert.

Testname	Bei bestandener Prüfung	Bei Fehlern	Fehlerbehebung
KDC1 IP DNS reverse:	OK	Failed!	Es ist zu prüfen, ob einer der als Administrator ***config*** unter dem Menüpunkt **Netzwerk > Nameserver** oder **Netzwerk > Lokale Domänen-Namensserver** eingetragenen Server die IP-Adresse und den Namen des AD-Servers vorwärts und rückwärts auflösen kann.
KDC1 DNS forward:	OK	Warning!	
KDC1 DNS = IP:	OK		
Keytab Principal with SSL CN:	OK	Failed!	Schlägt dieser Test fehl, so stimmen die Angaben zur Domäne/REALM nicht überein. Es ist zu prüfen, dass die Domäne und der REALM an folgenden Stellen übereinstimmen: 1) Domänen-Name in der **Keytab-Datei** 2) Unter dem Menüpunkt **Grundeinstellungen > DNS-Name im Zertifikat** 3) Unter dem Menüpunkt **System-Vorgaben > Kerberos Realms**
TGT request (with keytab):	OK	Failed!	Sofern dieser Test fehlschlägt, der Test zur **Keytab Principal with SSL CN** aber **OK** ist, so liegt das daran, dass die Keytab-Datei nicht mit administrativen Rechten erzeugt wurde. Es ist sicherzustellen, dass die Erzeugung der Keytab-Datei mit einer Kennung **Standard-Sicherheitsgruppe Administrator** erstellt wird.
AD GCs and DCs (with ports):			
GC ldap Port Check:	OK	Failed!	Der TightGate-Pro kann den GC-Server (Global Catalog) nicht über den TCP Port 3268 erreichen. Häufige Ursachen dafür sind: 1) Eine Firewall zwischen TightGate-Pro und dem GC verhindert dies. 2) Der GC-Server unterstützt das LDAP-Protokoll nicht. Es ist sicherzustellen, dass die Firewall die Verbindung zulässt und der GC-Server das LDAP-Protokoll unterstützt.
GC ldaps Port Check:	OK	Failed!	Der TightGate-Pro kann den GC-Server (Global Catalog) nicht über den TCP Port 3269 erreichen. Häufige Ursachen dafür sind: 1) Eine Firewall zwischen TightGate-Pro und dem GC verhindert dies. 2) Der GC-Server unterstützt das LDAPS-Protokoll nicht. Es ist sicherzustellen, dass die Firewall die Verbindung zulässt und der GC-Server das LDAPS-Protokoll unterstützt.

Testname	Bei bestandener Prüfung	Bei Fehlern	Fehlerbehebung
DC ldap Port Check:	OK	Failed!	Der TightGate-Pro kann den DC-Server (AD-Server) nicht über den TCP Port 389 erreichen. Häufige Ursachen dafür sind: 1) Eine Firewall zwischen TightGate-Pro und dem DC verhindert dies. 2) Der AD-Server unterstützt das LDAP-Protokoll nicht. Es ist sicherzustellen, dass die Firewall die Verbindung zulässt und der AD-Server das LDAP-Protokoll unterstützt. **Hinweis:** Grundsätzlich sollte die Kommunikation von TightGate-Pro mit dem AD-Server nur mit einem funktionierenden Protokoll (LDAP oder LDAPS) erfolgen. Vorzugsweise sollte das Protokoll LDAPS eingesetzt werden.
DC ldaps Port Check:	OK	Failed!	Der TightGate-Pro kann den DC-Server (AD-Server) nicht über den TCP Port 636 erreichen. Häufige Ursachen dafür sind: 1) Eine Firewall zwischen TightGate-Pro und dem DC verhindert dies. 2) Der AD-Server unterstützt das LDAPS-Protokoll nicht. Es ist sicherzustellen, dass die Firewall die Verbindung zulässt und der AD-Server das LDAPS-Protokoll unterstützt. **Hinweis:** Grundsätzlich sollte die Kommunikation von TightGate-Pro mit dem AD-Server nur mit einem funktionierenden Protokoll (LDAP oder LDAPS) erfolgen. Vorzugsweise sollte das Protokoll LDAPS eingesetzt werden.
AD server 1:			
Forward DNS:	OK		
Reverse DNS:	OK		
GSSAPI support (ldap):	OK		
GSSAPI support (ldaps):	OK		
LDAPS certificate:	OK	Failed!	Zeigt an, ob das verwendete LDAPS-Zertifikat noch gültig ist. Es wird eine Warnung ausgegeben, wenn das Zertifikat innerhalb von 60 Tagen ablaufen wird. Schlägt der Test fehl, ist das Zertifikat bereits abgelaufen oder ungültig.
–			
ggf. weitere AD Server ...			