Collax SSL-VPN

Howto

Dieses Howto beschreibt wie ein Collax Server innerhalb weniger Schritte als SSL-VPN Gateway eingerichtet werden kann, um Zugriff auf ausgewählte Anwendungen im Unternehmensnetzwerk von außen zu ermöglichen. Für die Nutzung ist außer einem gängigen Browser kein Client (“Client-less”) notwendig

Voraussetzungen

- Collax Security Gateway
- Collax Business Server oder Collax Platform Server inkl. Collax Modul SSL-VPN

Browser mit SSL und Java, welcher auf praktisch jedem Rechner ebenso wie auf vielen mobilen Geräten bereits vorhanden ist

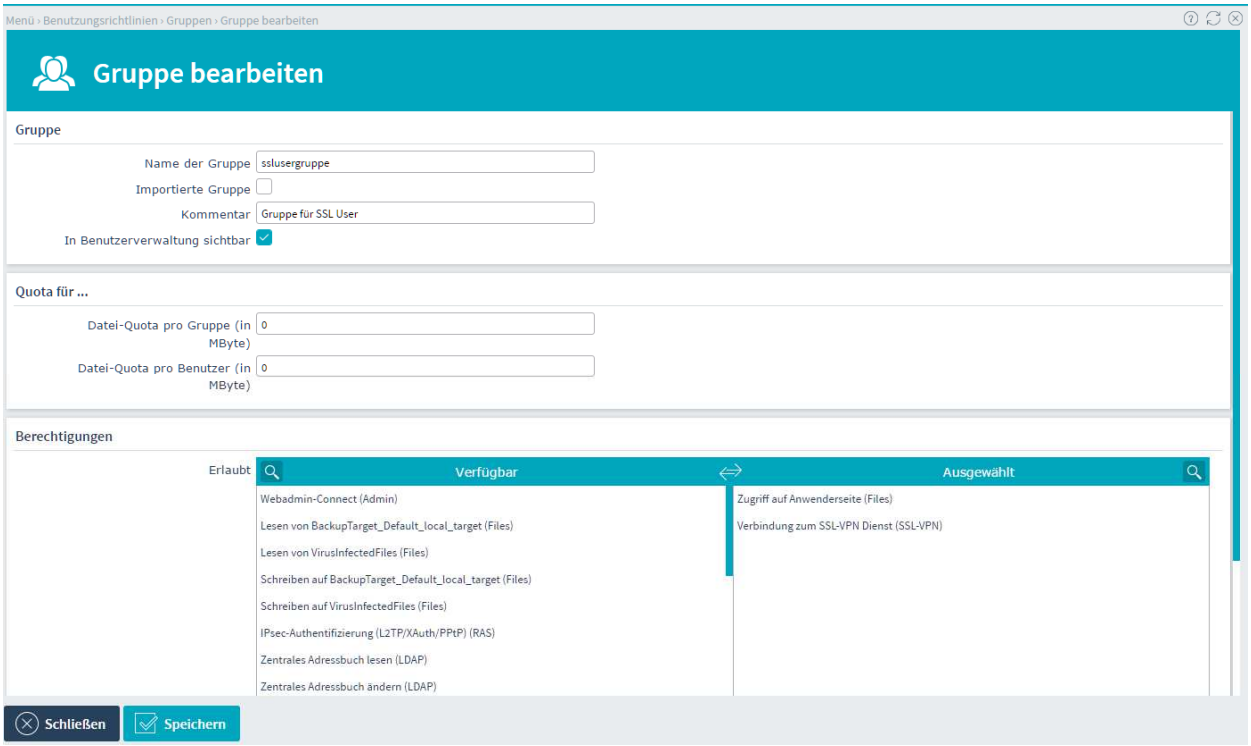
Hintergrund

Viele Web-Anwendungen sind von außerhalb oft nicht nutzbar. Sie sind innerhalb des Firmennetzes unverschlüsselt oder ein Zugang aus dem Internet ist nicht vorgesehen. Diese Anwendungen können nun bei Zugriffen von außerhalb eigens verschlüsselt und ohne Anpassungen nutzbar gemacht werden. Die Integration von SSL-VPN vereinfacht die Unterstützung solcher Anwendungen, wie etwa Outlook Web Access, an externen Arbeitsplätzen. Außerdem ist es künftig auch auf SSL-Basis möglich, alle Applikationen zu verwenden, deren Protokolle nur einen Port nutzen. Auf diese Weise kann beispielsweise der dezentrale Zugriff auf Mail-Programme in vollem Umfang unterstützt werden. Collax stellt mit seiner SSL-VPN-Lösung auch Agenten für die Verwendung von Terminaldiensten bereit. Auf diese Weise können sowohl das Microsoft Remote Desktop Protocol (RDP) als auch Citrix ICA Client Verbindungen oder das offene Virtual Network Computing (VNC) unterstützt werden. Diese Agenten werden als Java-Applet automatisch gestartet, so dass neben dem VPN-Client auch auf die Installation eines Terminal-Clients verzichtet werden kann.

Benutzer und Gruppen

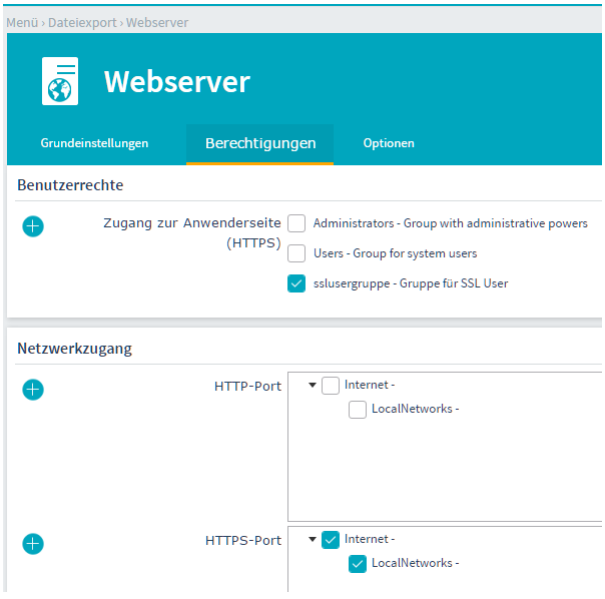
Für den Zugriff auf SSL-Anwendungen legen wir uns eine separate Berechtigungsgruppe und einen Benutzer an. Dieser Dialog befindet sich unter *„Benutzungsrichtlinien → Richtlinien → Gruppen“* bzw. *„Richtlinien → Benutzer“*

Die neu angelegten Gruppe nennen wir *„sslusergruppe“* und den Benutzer *„ssluser“*. Als Berechtigung vergeben wir „Zugriff auf Anwenderseite“ und „Verbindung zum SSL-VPN Dienst“.



Anwenderseite

Der Zugriff auf die Ressourcen erfolgt später über die Anwenderseite mittels HTTPS. Um den Zugriff zu ermöglichen, konfigurieren wir den Webserver unter *„Dienste → Dateiexport → Dienste → Webserver“*. Dort hinterlegen wir für den Webserver ein Serverzertifikat, sofern dies mit dem Intranet-Assistenten noch nicht erfolgte und wählen für den Netzwerkzugang auf den HTTPS-Port die Netzwerkgruppen „Internet“ und „LocalNetworks“.



Im Abschnitt *„Erlaubte Dienste“* unter *„System → Benutzungsrichtlinien → Richtlinien → Netzwerkgruppen“* kann die Gruppe auch direkt bearbeitet und der Netzwerkzugang für den HTTPS-Port dort gesetzt werden.

SSL-VPN-Ressourcen

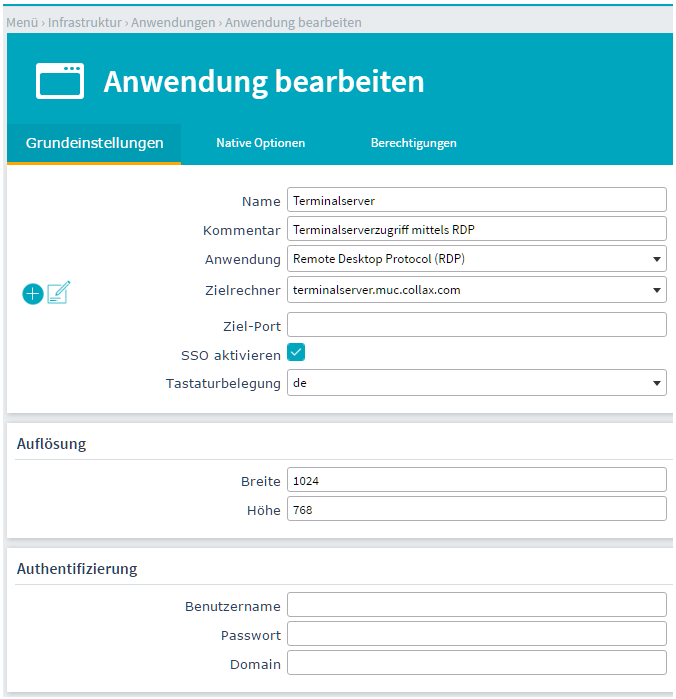
Als SSL-VPN-Ressourcen stehen vier verschiedene Varianten zur Verfügung.

- Anwendungs-Applets mit eigener Benutzeroberfläche
- Reverse-Proxy für Web-Weiterleitungen
- Getunnelte Web-Weiterleitungen
- SSL-Tunnel für Verbindungen mit der nativen Anwendung

Anwendungen

Für einen Fernzugriff auf interne Rechner, können in diesem Formular die entsprechenden Anwendungen eingerichtet und den gewünschten Gruppen über die Anwenderseite zur Verfügung gestellt werden. Zu den unterstützten Protokollen zählt das Remote Desktop Protocol (RDP), VNC und Citrix ICA.

Dieser Dialog befindet sich unter *„Dienste → Infrastruktur → SSL-VPN → Anwendungen“*



Anwendung Aus dieser Liste kann hier die gewünschte Anwendung ausgewählt werden. Es stehen dabei Remote-Desktop-Verbindungen, VNC-Verbindungen und Citrix ICA Client Verbindungen zur Verfügung.

Zielrechner Die gewählte Anwendung verbindet sich mit einem Zielrechner.

Ziel-Port Ist der Dienst des Zielrechners auf einem speziellen Port gebunden, muß hier dieser Ziel-Port angegeben werden. Läuft der Dienst des Zielrechners auf dem Standard-Port der Anwendung, kann dieses Feld leergelassen werden.

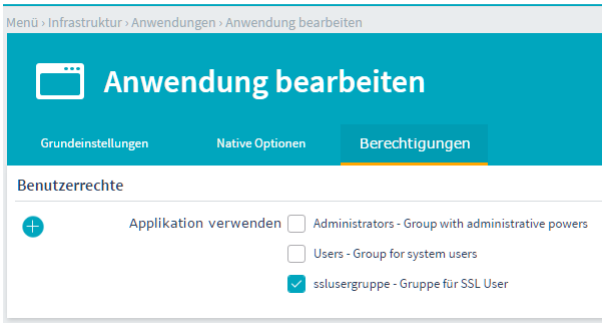
SSO aktivieren Die Einstellung übernimmt den Benutzer des Web-Access zur Authentifizierung der Anwendung.

Sofern die Option *„SSO aktivieren“* nicht gesetzt ist, können Benutzername und Kennwort für die Verbindung manuell angegeben werden. Alternativ können Benutzername und Kennwort auch leer gelassen werden, dann erfolgt die Authentifizierungsabfrage nach dem Aufbau der Verbindung.

Für eine optimale Fensterdarstellung werden für die gewählte Anwendung verschiedene Auflösungen zur Auswahl gestellt. Wird die Anwendung im Vollbild-Modus gestartet, kann dieser mit der Tastenkombination *„Alt-Return“* wieder beendet werden.

Weitere Optionen lassen sich über das Tab *„Native Optionen“* konfigurieren.

Nun muss nur noch die Gruppe ausgewählt werden, deren Benutzer autorisierten Zugriff auf die Anwendung erhalten.

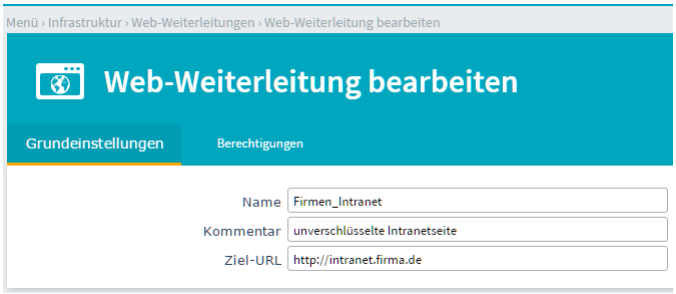


Web-Weiterleitungen und Reverse Proxy

Mit Hilfe von Web-Weiterleitungen können Web-basierte Anwendungen verschlüsselt angesteuert werden.

Über den Reverse-Proxy hingegen werden die an die Ziel-URL gerichteten Daten durch den Collax Server umgeschrieben. Hier wird kein Java Applet benötigt.

Dieser Dialog befindet sich unter *„Dienste → Infrastruktur → SSL-VPN → Web-Weiterleitungen“* bzw. „Reverse-Proxy“



Über die Berechtigungen werden sie den gewünschten Gruppen über die Benutzerseite zur Verfügung gestellt.

SSL-Tunnel

Mit der Definition eines SSL-Tunnel wird ein beliebiger Dienste-Port vom lokalen Rechner durch den Collax Server auf einen Zielrechner und Ziel-Port getunnelt. Wenn der SSL-Tunnel aufgebaut ist, kann die Zielanwendung von dem lokalen Rechner aus mit „localhost:Ziel-Port“ angesprochen werden.

Dieser Dialog befindet sich unter *„Dienste → Infrastruktur → SSL-VPN → SSL-Tunnel“*

Lokaler Port Hier wird der gewünschte lokale Netzwerk-Port angegeben. Er kann im Bereich von 1 bis 65535 definiert werden. Um eventuell auftretende Konflikte mit lokal gestarteten Diensten zu vermeiden, wird empfohlen, einen Port im Bereich zwischen 1024 und 65535 zu wählen.

Zielrechner Hier wird der gewünschte Zielrechner mit IP-Adresse oder Host-Namen angegeben.

Ziel-Port Hier wird der zu erreichende Dienste-Port des Zielrechners angegeben. Er kann im Bereich von 1 bis 65535 definiert werden. Die Erreichbarkeit dieses Dienste-Ports und die Authentifizierung an diesem Dienst obligt den Einstellungen auf dem Zielrechner.

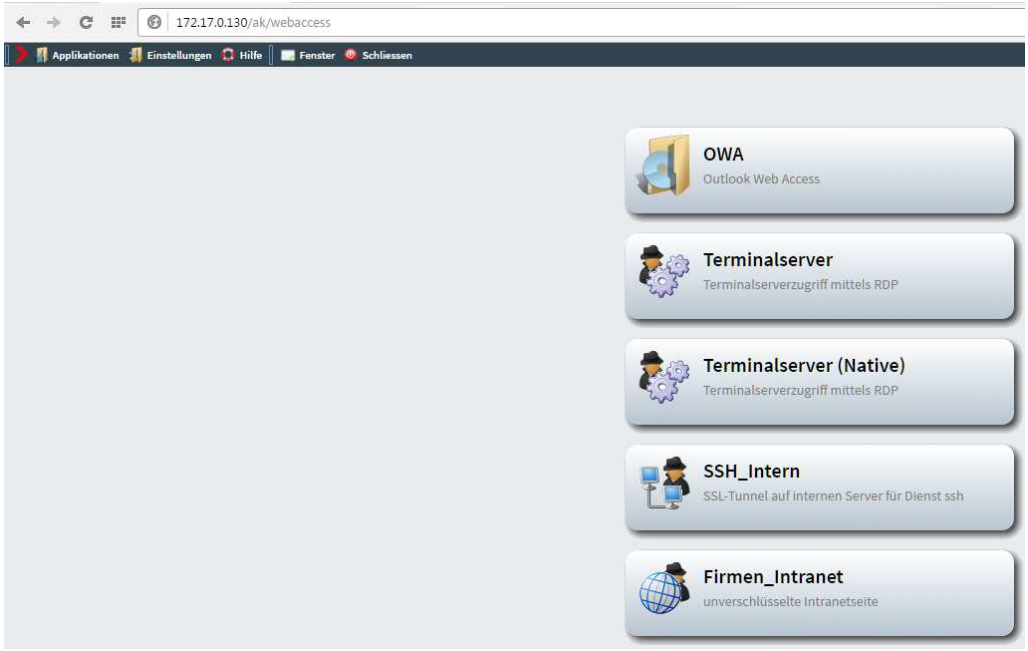
Über die Berechtigungen wird er den gewünschten Gruppen über die Benutzerseite zur Verfügung gestellt.

Hiermit wird der Zugriff auf einen internen SSH-Server auf den lokalen Port 10022 getunnelt. Somit ist durch Angabe des Servers 127.0.0.1 (Localhost) und dem Port 10022 eine Verbindung mittels eines SSH-Clients auf den Zielserver möglich.

Bedienung über den Webaccess

Nach der Eingabe von **https://IP-des-Collaxservers** im Browserfenster öffnet sich eine Anmeldemaske für die Anwenderseite.

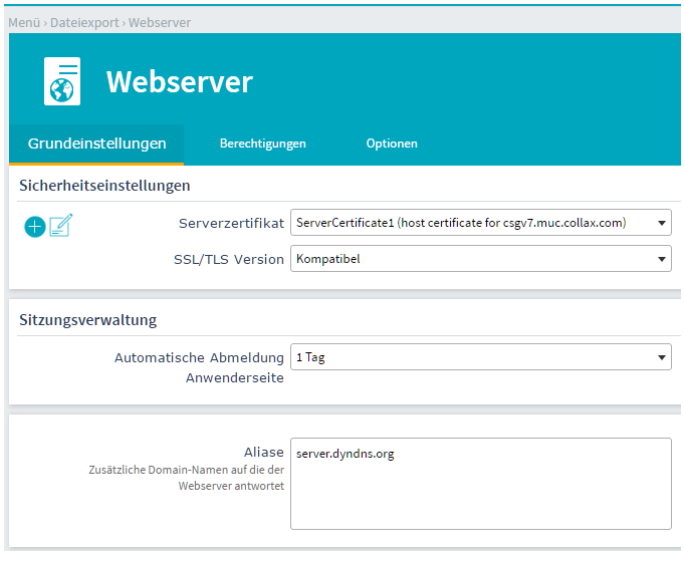
Nach erfolgreichem Login kann der Benutzer auf seine SSL-VPN-Ressourcen zugreifen.



Troubleshooting

Wenn das SSL-VPN Java Applet aufgrund der Fehlermeldung „ClassNotFoundException“ nicht gestartet wird, kann es daran liegen, dass man über einen DNS-Namen auf den Server zugreift, der nicht gleichlautend ist wie der FQDN des Servers.
z.B. lautet der FQDN des Servers „server.firma.de“, der DynDNS-Name lautet jedoch server.dyndns.org

In diesem Fall kann für den Webserver ein Alias unter „System → Dateiexport → Webserver“ konfiguriert werden.



Sofern der DNS Eintrag (zum Aufruf) gleichlautet wie der FQDN des Servers und es immer noch nicht funktioniert, kann folgende Client-Einstellung von Java Abhilfe versprechen.

Start -> Programme -> Java -> Configure Java

Reiter "Erweitert" bzw engl. "Advanced"

"SSL 2.0-kompatibles ClientHello-Format" verwenden anhaken.