Sichere Netzwerklösungen für Genossenschaftsbanken

banking & network it solutions GmbH

Genossenschaftsbanken stehen vor großen Herausforderungen. Die Digitalisierung durchdringt die Gesellschaft immer mehr. Der Kostendruck steigt. Gerade deshalb müssen Genossenschaftsbanken ihr Profil als lokaler Ansprechpartner in allen Bereichen schärfen. Dies geschieht nicht nur, aber auch mit einem performanten Filialnetzwerk.

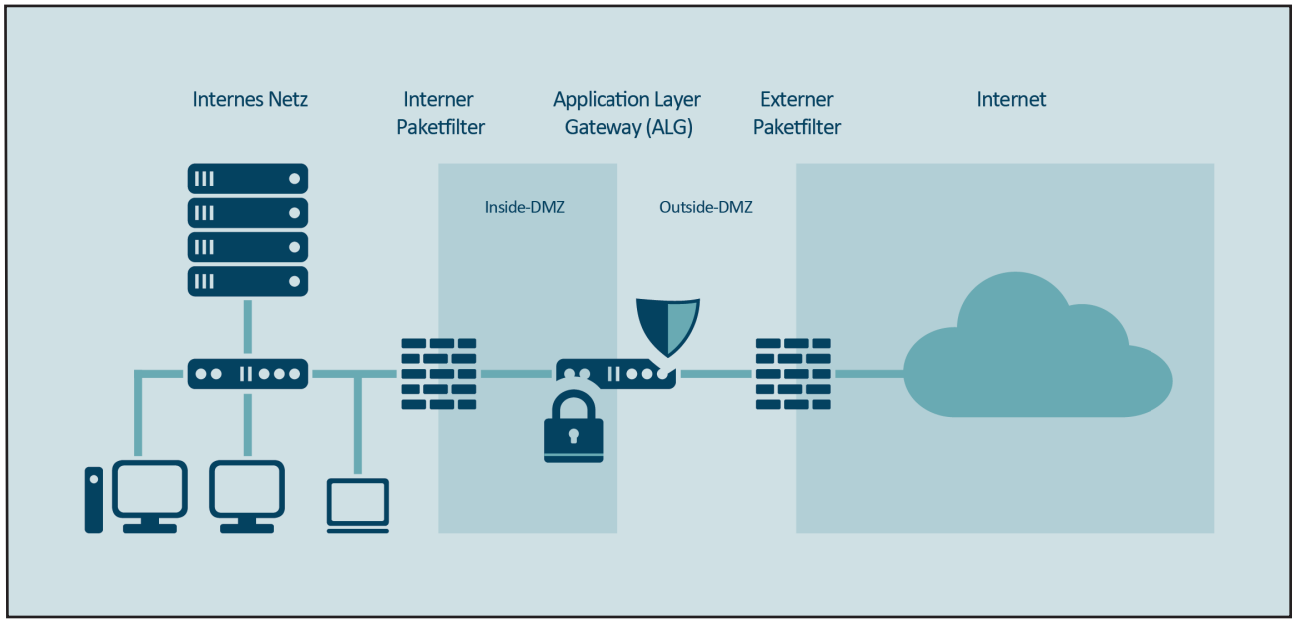
Ebenfalls wird die Bindung von Leistungsträgern immer wichtiger. Ein moderner Arbeitsplatz mit flexiblen Arbeitsmodellen ist heute für viele Arbeitnehmer eine Grundvoraussetzung. Hierzu zählt auch die Möglichkeit bequem vom Homeoffice aus arbeiten zu können. Die IT-Sicherheit muss aber auch hier zu 100% gewährleistet sein. Der Gesetzgeber hat die Anforderungen an den Betrieb einer sicheren IT-Infrastruktur deutlich erhöht.
Daher ist es für ein Unternehmen enorm wichtig dezentrale Strukturen sicher und standardisiert aufzubauen.

Wir bieten Ihnen die Möglichkeit einen beliebigen Internetanschluss von einem Provider Ihrer Wahl nutzen zu können. Unser Konzept erfüllt hierbei sowohl die Anforderungen des Rechenzentrums an eine Drittnetzanbindung als auch die Anforderungen des BSI nach IT-Grundschutz an einen sicheren Internetzugang.

Auf Basis dieses sicheren Internetzugangs können alle Geschäftsstellen mit hoher Bandbreite, redundant, sicher und kostengünstig angebunden werden. Eine flexible und für den Anwender komfortable VPN Einwahllösung rundet unser Konzept ab.

Zusätzlich ist es möglich eine eigene DMZ aufzubauen und diverse Dienste in der DMZ sicher über das Internet bereitzustellen.

Internetzugang



Die Absicherung des Internetzugangs ist ein wichtiger Baustein im IT-Sicherheitskonzept. Unser mehrstufiges Firewall-Konzept bildet die Anforderungen des BSI an einen sicheren Internetzugang ab. Das durch zwei Firewalls geschützte Application Layer Gateway (ALG) ermöglicht eine umfassende Absicherung Ihres Internetzugangs. Die Kombination von Firewall-Systemen unterschiedlicher Hersteller sorgt für eine weitere Erhöhung der Sicherheit.

Ein Zugriff aus dem internen Netz auf Inhalte im Internet ist nur über das ALG möglich. Das ALG verfügt über Antivirus-Komponenten mit zwei Engines um Viren, Würmer, Trojaner und andere Malware abzuwehren. Ein erweiterter Schutz vor Zero-Day-Attacken wird mit der Advanced Threat Protection (ATP) realisiert. Das ALG erkennt hierbei Botnet-Verbindungen und blockt diese, ebenso wie den Zugriff auf bekannte Phishing URLs. Mittels IPS-Mustern und Deep Packet

Inspection werden anwendungs- und protokollbezogene Probes und Angriffe zuverlässig identifiziert und abgewehrt. Die umfangreiche Signaturdatenbank mit Mustern und Regeln wird automatisch alle 15 Minuten aktualisiert.
Die Nutzung eines eigenen Internetanschlusses bietet den Vorteil, dass die Bandbreite für den Zugriff auf Inhalte aus dem Internet deutlich erhöht werden kann – und dies ist in der Regel deutlich kostengünstiger als eine Erhöhung der Bandbreite der Primär-Anbindungen zum Rechenzentrum.
Gleichzeitig sorgt die Verlagerung des Internettraffics von der Primäranbindung auf den eignen Internetzugang dafür, dass die Primäranbindung entlastet wird und somit mehr Bandbreite für den Zugriff auf Dienste des Rechenzentrums zur Verfügung steht.

Schutz für öffentlich zugängliche Server und Anwendungen (Web Server Protection)

Schützen Sie Ihre öffentlich zugänglichen Server und Anwendungen vor Manipulations- und Hacking-Versuchen.

Statisches URL Hardening verhindert, dass Hacker so genannte „Deep Links“ manuell erstellen, über die sich Unbefugte Zugriff verschaffen können. Form Hardening sorgt dafür, dass schädliche Skripts und Codes nicht genutzt werden können, um Ihre Datenbanken auszuspähen. Cookie Protection stellt zudem sicher, dass Cookies signiert und somit nicht manipulierbar sind.

Beispiele aus der Praxis:

- Telefonanlagen
- Bereitstellung von Cloud-Diensten z.B. zum sicheren Dokumentaustausch mit Kunden
- Web-Server
- Bereitstellen von Intranetlösungen für den externen Zugriff (z.B. Intrexx)
- Video-Kommunikationsplattform

Funktionen

- Web Application Firewall
- Serverhärtung
- Reverseproxy-Authentifizierung
- Antivirus-Scans
- SSL Offloading

Weitere Details zu unserer Lösung finden Sie unter:
https://www.bn-its.de/it-security/firewall/

Proxy (Web Protection)

Die Anbindung an das Internet erfolgt über den Proxy-Dienst des ALG.
Dieses bietet einen umfassenden Schutz vor aktuellen Web-Bedrohungen. Eine frei konfigurierbare URL-Filterung mit welcher der Zugriff auf einzelne Seiten und/oder ganze Kategorien von Seiten unterbunden wird. Die integrierte Layer 7-Inspection (Next-Generation Firewall) erlaubt die Kontrolle und Priorisierung von einzelnen Webanwendungen Das ALG sorgt dafür, dass Ihre Benutzer sicher und produktiv im Internet surfen können.

Funktionen

- Schutz vor Web-Malware mit zwei unabhängigen Antivirus-Engines
- URL-Filterrichtlinien
- SafeSearch, YouTube und Google Apps
- HTTPS-Scans
- Layer-7 Application Control

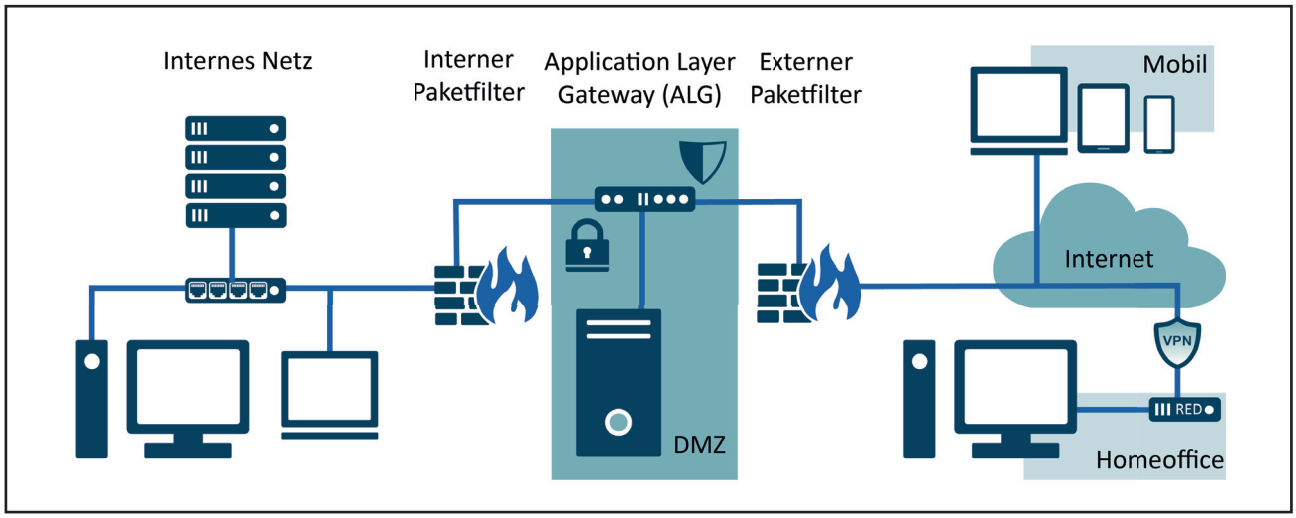
Penetrationstest

Das BSI empfiehlt die regelmäßige Durchführung eines Penetrationstests um die Sicherheit des Internetzugangs und des Netzwerks zu überprüfen.

Unser Konzept zur Drittnetzanbindung hat bisher alle Pen-Tests, die bei diversen Kunden von externen Firmen durchgeführt wurden, ohne Mängel bestanden.

VPN - Homeoffice

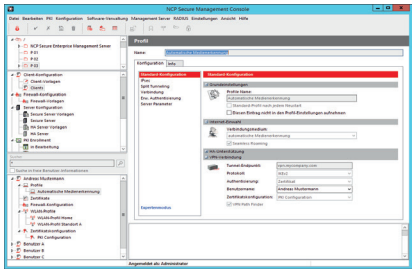
Laut einer ESET-Studie vom April 2020 wünschen sich 68% der Arbeitnehmer eine Lockerung der Regelung zur Arbeitsplatzwahl auch für die Zukunft. Wir stellen die hierfür erforderliche, sichere technische Infrastruktur kostengünstig bereit.
Unser sicherer Internetzugang ist auch die Grundlage für die Homeoffice Anbindung über Sophos RED Devices. Ein Sophos RED Device ist ein vorkonfiguriertes VPN-Gateway, welches beim Mitarbeiter zu Hause aufgebaut werden kann. Für die Inbetriebnahme des RED-Devices ist kein technisches Fachwissen erforderlich. Sobald das Gerät mit dem Internet verbunden ist, stellt es automatisch eine VPN-Verbindung zur Firewall in der Zentrale her. Alle Daten zwischen dem RED-Device und der zentralen Firewall werden auf Basis von AES-256 verschlüsselt. Dies garantiert eine sichere Verbindung, die weder manipuliert noch kompromittiert werden kann.
Notebook und Telefon werden an das RED-Device angeschlossen und können transparent auf die Dienste und Applikationen der Zentrale zugreifen. Der Mitarbeiter kann dann bequem von zu Hause arbeiten. Die Option auch eine Nebenstelle der zentralen Telefonanlage zu Hause nutzen zu können gibt Ihnen die Möglichkeit eine Vielzahl von Mitarbeitern im Homeoffice zu beschäftigen.



VPN – mobiles Arbeiten, standortunabhängig und flexibel

Auf Basis unseres sicheren Internetzugangs bieten wir in Kombination mit dem NCP Secure Enterprise Client eine vollintegrierte Lösung zur sicheren und einfachen Anbindung mobiler Mitarbeiter an das Firmennetzwerk.

Die vom BSI geforderte zwei-Faktor-Authentifizierung setzen wir konsequent um (Computerzertifikat + Benutzername und Kennwort).



Das NCP Secure Enterprise Management (SEM) ermöglicht einen automatisierten Rollout der Clients und eine zentrale Konfiguration. Das automatische Update-Verfahren ermöglicht dem Administrator für alle entfernten NCP Secure Enterprise Clients zentral Konfigurations- und Zertifikats-Updates bereitzustellen. Sobald eine Verbindung zwischen Client und Firmennetzwerk besteht, werden diese Komponenten automatisch auf der Client-Seite eingespielt.
Völlig egal, ob es um die Vernetzung weltweiter Standorte oder die Anbindung tausender mobiler Mitarbeiter geht, alle für die Überprüfung und Einhaltung der Sicherheitsrichtlinien, den Rollout und Betrieb erforderlichen Aktivitäten können automatisiert werden:

- Software- und Kofigurationsupdates
- Verwaltung von Usern, Lizenzen und Zertifikaten
- vollautomatische Benutzeranmeldung

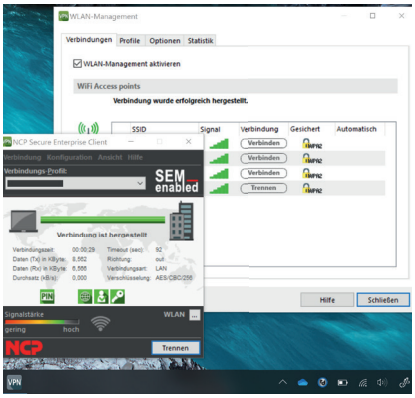
Sichere Netzwerklösungen für Genossenschaftsbanken

banking & network it solutions GmbH

Der NCP-VPN Enterprise Secure Client bietet unter anderem folgende Vorteile:

Zum einen kann vor der VPN-Einwahl die Verbindung zu einem WLAN hergestellt werden. Über zentral definierte Richtlinien steuern Sie, welche Anforderungen das WLAN erfüllen muss, damit eine Verbindung aufgebaut werden kann (eine Verbindung zu nicht sicheren WLAN's kann somit beispielsweise unterbunden werden).

Zum anderen kann die VPN-Verbindung bereits aufgebaut werden, bevor Sie sich am Arbeitsplatz anmelden (VPN-before-Login) – so dass der Arbeitsplatz bei der Anmeldung schon mit dem Firmennetzwerk verbunden ist. Somit ist gewährleistet, dass Anmelde-Skripte, die Zugriff auf Ressourcen im Firmennetzwerk benötigen, fehlerfrei ausgeführt werden.



Das Pay-Per-Use-Modell

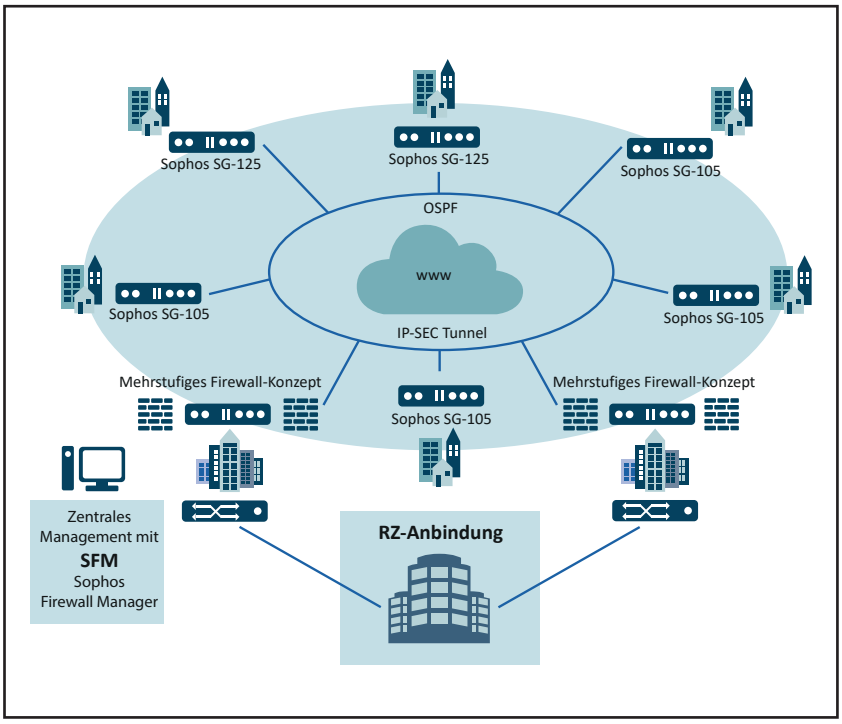
Das Pay-per-Use-Modell gibt Ihnen die Möglichkeit, den NCP-VPN-Client auf allen benötigten Geräten zu installieren – abgerechnet werden lediglich die Clients, die innerhalb des Abrechnungszeitraums (monatlich) eine VPN-Verbindung aufgebaut haben, mindestens jedoch 40% der am Anfang der Vertragslaufzeit definierten max. Anzahl an Clients. Die vertraglich definierte Anzahl der Clients ist während der 36-monatigen Laufzeit fix – es können aber bei Bedarf mehr Clients genutzt werden.

Dieses Abrechnungsmodell bietet somit maximale Flexibilität bei geringen Investitionskosten.

Unternehmensvernetzung - sichere Anbindung von Geschäftsstellen

Die Grundlage unseres Konzepts zur Unternehmensvernetzung basiert auf unserem sicheren Internetzugang bestehend aus zwei Firewalls und einem ALG. Aus Redundanzgründen wird dieser Internetzugang idealerweise in der Zentrale und einem weiteren Standort (Kopfstelle) vorgehalten. Die einzelnen Geschäftsstellen werden über normale Internetanschlüsse mittels VPN mit diesen beiden Standorten verbunden.

Eine durchdachte Konzeption und der Einsatz von dynamischen Routingprotokollen wie OSPF und BGP sorgen für eine intelligente Lastverteilung und die erforderliche Redundanz.
Fällt einer der beiden zentralen Stellen aus, weichen die von dem Ausfall betroffenen Geschäftsstellen automatisch auf den verbleibenden zentralen Standort aus.



Sichere Netzwerklösungen für Genossenschaftsbanken

banking & network it solutions GmbH

Zugriff auf das Netzwerk des Rechenzentrums

Der Zugriff auf das Netzwerk des Rechenzentrums erfolgt über die Primärleitungen an den beiden zentralen Standorten (Zentrale/ Kopfstelle) mittels eines Transfer Netzes.
Bei der Beantragung der notwendigen Transfernetz-Umstellung unterstützen wir Sie gerne.
Bei einer redundanten Vernetzung mit wenigsten zwei zentralen Standorten inkl. Primäranbindung kann auf eine TO-Leitung des Rechenzentrums verzichtet werden.

DSL-Leitungen

Der Einsatz von Standard- Internetanschlüssen ermöglicht die Nutzung von hoher Bandbreite zu geringen Kosten.

Insbesondere an den zentralen Standorten empfehlen wir den Einsatz von schnellen Internetanbindungen – hier ist speziell auf ausreichende Upload-Bandbreite zu achten.
An allen Standorten können aus Redundanzgründen auch mehrere Internetanbindungen genutzt werden, um den Ausfall einer Leitung automatisch zu kompensieren.
An den Geschäftsstellen ist auch eine Anbindung mittels LTE möglich. In der Praxis nutzen viele unserer Kunden einen Kostengünstigen LTE-Anschluss als Backupleitung.
Aus Sicherheitsgründen ist für jeden Internetanschluss eine feste IP-Adresse erforderlich.

Monitoring / Überwachung

Die Auslastung und die Verfügbarkeit der einzelnen Datenleitungen wird über ein zentrales Monitoring mittels PRTG lückenlos überwacht und dokumentiert.

Wir haben die richtige Lösung für Sie!

banking & network it solutions GmbH

Klosterdorf 38
91443 Scheinfeld

Tel. +49 9162-527999 0
Fax +49 9162-527999 8

info@bn-its.de
www.bn-its.de