Vorarlberger
Telekommunikations-
Gesellschaft mbH.

A-6900 Bregenz
Weidachstraße 6

Produkthandbuch

P-001	CNV-Teleworker
Kurzbeschreibung	Es wird der Remote-Zugang von Einzelarbeitsplätzen aus fremden Netzen auf Netze des Corporate Network Vorarlberg beschrieben. Dieser Dienst wird für Telearbeiter und Zugänge von Wartungsfirmen benötigt.

Inhaltsverzeichnis

Version	Gültig ab	Bearbeiter	Freigabe durch
1.1	29.11.2004	Stefan Holzmüller	Christoph Märk

1. Versionsverzeichnis

Version	Erstellt durch	Datum	Anmerkungen
1.0	Christoph Märk	20.2.2003 10.3.2003	Ersterstellung Freigabe durch Heinz Loibner
1.1	Stefan Holzmüller	29.11.2004	Überarbeitung, R56 Client Trennung in Produkt- und Installationshandbuch

2. Vertraulichkeit und Verteilung

Dieses Dokument ist für den internen Gebrauch und darf an CNV-Teilnehmer und Wartungsfirmen weitergegeben werden. Eine generelle Veröffentlichung ist nicht vorgesehen. Diese Produktbeschreibung ist für alle CNV-Kunden im Intranet unter www.intra.cnv.at enthalten.

3. Geltungsbereich

Diese Produktbeschreibung beschreibt den Remote-Zugang von Einzelarbeitsplätzen aus fremden Netzen auf Netze des Corporate Network Vorarlberg (CNV). Dieser Dienst wird für Telearbeiter und Zugänge von Wartungsfirmen benötigt.

4. Allgemeines

Um Dienste des CNV und Dienste der am CNV angeschlossenen Netzwerke über einen Remote-Arbeitsplatz nutzen zu können, ist es erforderlich, den Anwender zu authentifizieren und die Verbindung stark zu verschlüsseln. Mit der CNV-Teleworker-Lösung wird dieses Ziel erreicht. Je nach Erfordernis der benötigten Dienste und der Festlegung der Security-Policy bietet die VTG mehrere Lösungsvarianten an, die sich in der Stärke der Authentifizierung und in der „Desktop Security“ unterscheiden.

Auch die Einbindung von Remote-LANs via VPN ist möglich. Dies ist jedoch eine Lösung, die bei der VTG gesondert beantragt werden muss und in diesem Dokument nicht beschrieben ist.

5. Verantwortlichkeiten

Applikationsverantwortlicher:
Der Applikationsverantwortliche entscheidet, wer aus externen Netzen Zugriff auf seine Anwendungen und Daten bekommt. Er ist auch verantwortlich für das Vertrauen in diese Personen und Wartungsfirmen. Er muss sich auch darum kümmern, wie lange der Dienst bereitgestellt wird.

Serververantwortlicher:
Der Serververantwortliche entscheidet, wer aus externen Netzen Zugriff auf seine Server für Wartungszwecke bekommt. Er ist auch verantwortlich für das Vertrauen in diese Personen und Wartungsfirmen. Er muss sich auch darum kümmern, wie

lange der Dienst bereitgestellt wird. Der Serververantwortliche ist in der Regel auch ein VTG-Mitarbeiter.

Die VTG:
Die VTG bietet als Dienstleister die technische Infrastruktur für den sicheren Zugang und die verschlüsselte Kommunikation an. Von der VTG werden die Zugänge eingerichtet und die notwendigen Freischaltungen durchgeführt. Dazu braucht die VTG entweder den Auftrag des Applikationsverantwortlichen oder des Serververantwortlichen.

Ein Formular für die Beantragung dieses Dienstes ist im Anhang dieses Dokuments enthalten oder kann im Internet von unserer Homepage heruntergeladen werden.
http://www.vtg.at/dl/tw-anmeldeformular.doc

6. Voraussetzungen

Für einen Einzelplatz-CNV-Teleworker-Zugang ist notwendig:

- Internet-Zugang
- Betriebssystem Windows 2000 oder höher
- Administrator-Rechte für die Installation der Client-Software
- USB–Anschluss, wenn Hardware-Token als Zertifikatsspeicher verwendet wird
- Anmeldung durch den CNV-Kunden und Freischaltung bei der VTG
- Unterschriebene Sicherheitsvereinbarung

7. VPN-Client-Software

Um die Teleworker-Anbindung verwenden zu können, ist am PC die Installation der Client-Software von Checkpoint notwendig. Diese Software kontrolliert den Netzwerk-Verkehr und fordert einmalig zur Authentifizierung auf. Wird eine Verbindung zum CNV-Netzwerk aufgebaut, werden die Datenpakete verschlüsselt übertragen. Kommen verschlüsselte Datenpakete aus dem CNV-Netzwerk an, werden diese entschlüsselt weitergeleitet.

Für den Betrieb des VPN-Clients gibt es eine Option „enable auto connect“. Ist diese Option aktiviert, erscheint das Authentifizierungsfenster sobald ein Paket in ein CNV-Netzwerk transportiert werden soll. Ohne diese Option verhält sie sich wie eine DFÜ-Verbindung, d.h., zuerst muss die Verbindung aufgebaut werden – und erst danach ist der CNV-Zugang nutzbar.

Die Verschlüsselung erfolgt in jedem Fall mit mindestens 3DES. Die Stärke der Verschlüsselung wird von der Teleworker-Zentrale vorgegeben.

Eine ausführliche Beschreibung und Installationsanleitung wird nach der Anmeldung für dieses Produkt gemeinsam mit den Zugangsdaten bereitgestellt.

Je nach Anforderung an die Desktop-Sicherheit bestehen zwei Möglichkeiten für den Betrieb des VPN-Clients (wird als Option bei der Installation unterschieden):

- SecuRemote
- SecureClient

Download des VPN-Clients unter http://www.vtg.at/dl/vpnclient.exe
Obwohl von Checkpoint laufend neue Versionen des VPN-Clients zur Verfügung gestellt werden, sollte nur die von uns im Intranet bereitgestellte Version verwendet

werden. Andernfalls kann bei Problemen mit der VPN-Verbindung von uns kein Support übernommen werden.

7.1 SecuRemote

Diese VPN-Software ist lizenzfrei und deckt die Bereiche der Authentifizierung und der Verschlüsselung ab. Sie bietet aber keinerlei Schutz für den lokalen PC. Bei dieser Variante muss sich der Benutzer selbstständig um den Schutz des eigenen PCs gegenüber Drittnetzwerken kümmern.

7.2 SecureClient

Beim SecureClient ist eine Personal-Firewall integriert, welche eine Standard-Desktop-Policy von der Teleworker-Zentrale bezieht. Weiters bietet dieser Client den Vorteil einer zentralen IP- und DNS-Zuweisung. Die für diese Variante anfallenden Lizenzkosten sind im angeführten Produktpreis enthalten.

8. Authentifizierungsarten

Jeder Verbindungsaufbau muss authentifiziert sein. Je nach Anforderung der Sicherheitsvorschriften bestehen mehrere Möglichkeiten, die Benutzerauthentifizierung durchzuführen.

- Persönliches Zertifikat auf Hardware-Token (iKey)
- Persönliches Zertifikat („Soft-Zertifikat)

Die Entscheidung, welche Variante zulässig ist oder nicht, muss der jeweilige lokale Dienste- und Sicherheitsverantwortliche treffen.

Download der iKey-Software unter http://www.vtg.at/dl/ikey.zip
Obwohl von Rainbow laufend neue Versionen der iKey-Software zur Verfügung gestellt werden, sollte nur die von uns im Intranet bereitgestellte Version verwendet werden. Andernfalls kann bei Problemen mit dem iKey von uns kein Support übernommen werden.

8.1 Persönliches Zertifikat auf Hardware-Token (iKey)

Die Authentifizierung erfolgt über ein persönliches User-Zertifikat, das von der VTG ausschließlich auf einem Hardware-Token (iKey) ausgegeben wird. Der Hardware-Token ist durch einen persönlichen PIN geschützt. Der User kann diesen PIN ändern.

ACHTUNG:
Der PIN des Benutzers ist der Schutz für unberechtigten Gebrauch des Zertifikats auf dem Hardware-Token (z.B. falls er verloren geht). Wird der PIN mehr als 5-mal falsch eingegeben, wird er gesperrt und kann nicht mehr verwendet werden. Es muss dann von der VTG ein neues Zertifikat ausgestellt und auf den Hardware-Token kopiert werden.

Der iKey ist eine Smartcard und beinhaltet einen zertifizierten Cryptoprozessor. Es besteht keine Möglichkeit, diesen iKey zu kopieren. Für den Betrieb des iKey wird ein Treiber des Herstellers und eine freie USB-Schnittstelle am PC benötigt.

Diese Variante ist die stärkste und somit die empfohlene Authentifizierungsvariante. Sie ist geeignet, Zugänge für Systemadministratoren und „Power-User“ frei zu schalten.

8.2 Persönliches Zertifikat („Soft-Zertifikat)

Das persönliche User-Zertifikat wird auf der Festplatte gespeichert. Es entfällt die Installation des USB-Treibers. Diese Variante wird nur dort zugelassen, wo sichergestellt ist, dass das Zertifikat durch einen bekannten Administrator „sicher“ (PIN-Vergabe und Einstellung: „nicht exportierbar“) installiert wird, und eine Windows-Policy dem User keine Möglichkeit gibt, den Private Key auszulesen bzw. zu kopieren.

Diese Variante eignet sich dort, wo von einer zentralen Stelle aus viele Teleworker installiert werden, die alle unter einer einheitlichen Sicherheitsverantwortung und unter einer zentralen Betreuung stehen.

9. Security-Policy

- In jedem Fall ist jeder Teleworker auf die benötigten Dienste beschränkt.
- Jede Verbindung wird protokolliert.
- Jeder Account ist mit einem Ablaufdatum versehen.
- Ein Account wird erst dann eingerichtet, wenn die Sicherheitsvereinbarung unterschrieben bei der VTG vorliegt.
- Der CNV-Kunde bestätigt mit dem Anmeldeformular schriftlich, welcher Teleworker auf welche Dienste (die im Zuständigkeitsbereich des CNV-Kunden liegen) Zugriff haben darf.
- Ansonsten gelten die bestehenden Sicherheitsvorschriften.

Die Sicherheitsvereinbarung ist im Anhang dieser Produktbeschreibung enthalten oder kann im Internet abgerufen werden:
http://www.vtg.at/dl/tw-sicherheitsvereinbarung.doc

10. Kontakt und Support

Vorarlberger Telekommunikations-GmbH
Weidachstraße 6, 6900 Bregenz
Tel.: +43/5574/601 74001
Fax: +43/5574/601 74010
Mail: office@vtg.at
http: www.vtg.at

Bitte beachten Sie, dass in den Preisen im Anmeldeformular die Installation und der Support für die Client-Software nicht enthalten sind. Ebensowenig ist eine Unterstützung bei lokalen oder Provider-Netzwerk- und Firewallproblemen enthalten. Wird Unterstützung benötigt, führen wir diese gerne zu unseren üblichen Stundensätzen durch.

11. Sicherheitsvereinbarung

Über den CNV-Teleworker-Zugang besteht die Möglichkeit, über Internet oder RAS authentifiziert und verschlüsselt auf definierte Ressourcen des CNV-Netzwerkes zugreifen zu können. Dies erfordert neben den technischen Gegebenheiten auch eine organisatorische Policy, die in jedem Fall eingehalten werden muss.

Jeglicher Verlust, Diebstahl oder sonstiges Abhandenkommen des Authentifizierungs-Token (iKey oder Soft-Zertifikat) muss umgehend der VTG-Hotline (siehe Kontakt) gemeldet werden. Die Meldung muss auch bereits bei reinen Verdachtsmomenten erfolgen.

Authentifizierungs-Accounts haben eine Gültigkeit von maximal 2 Jahren und dürfen in keinem Fall an Dritte weitergegeben werden. Mitarbeiterwechsel müssen der VTG-Hotline gemeldet werden, so dass der alte Account gesperrt und ein neuer eingerichtet werden kann.

Bei SecureClient-Anbindungen ist es nicht erlaubt, die Desktop-Policy zu deaktivieren und somit die "Personal-Firewall" abzuschalten.

Wird seitens des Teleworkers keine Desktop-Security gewünscht (das sind z.B. SecuRemote-Zugänge für Wartungsfirmen) müssen vom Teleworker andere geeignete Maßnahmen für die Desktop-Security des PCs ergriffen werden (z.B. Firmen-Firewall oder andere „Personal Firewall“).

Jede Anmeldung und jeder Datentransfer wird protokolliert und im Bedarfsfall ausgewertet.

Besteht keine andere Vereinbarung, behalten wir uns das Recht vor, Zugänge, die länger als 2 Monate nicht benutzt werden, zu deaktivieren.

Vor der Einrichtung eines Teleworker-Accounts wird der Antrag durch die VTG-Security-Administration geprüft. Bei Sicherheitsbedenken behalten wir uns das Recht vor, die Einrichtung von Zugängen nicht durchzuführen.

Ansonsten gelten die Sicherheitsvorschriften für Behördennetze. Der Teleworker muss alles unterlassen, was eine Gefährdung der IT-Sicherheit bedeuten könnte.

Diese Vereinbarung ersetzt weder bestehende arbeitsrechtliche Vereinbarungen, noch anderweitige Sicherheitsvorschriften. Im Zweifelsfall und bei Unklarheiten muss immer die VTG kontaktiert werden.

Kontakt: Vorarlberger Telekommunikations-GmbH
Weidachstraße 6, 6900 Bregenz
Tel.: +43/5574/601 74040
Mail: hotline@vtg.at

.....	.....
(Datum)	(Firma / Organisation)
.....	.....
(Benutzer)	(Unterschrift)

12. Anmeldeformular[1]

Der CNV-Kunde: .....

beauftragt die Einrichtung eines Teleworker-Zuganges für:

Firma/Organisation: .....

Anschrift: .....

Für den Benutzer:
Vor- /Zuname: .....

e-Mail: .....

Tel. .....

Zugangsart (bitte ankreuzen)

	VPN-Client	Authentifizierung	Bemerkung	Einmalig[2]	Monatlich
☐	SecuRemote	iKey (HW-Token)	von VTG empfohlen	€ 185,--	€ 12,--
☐	SecuRemote	Soft-Zertifikat		€ 105,--	€ 12,--
☐	SecureClient	iKey (HW-Token)	von VTG empfohlen	€ 300,--	€ 15,--
☐	SecureClient	Soft-Zertifikat		€ 220,--	€ 15,--

Lizenzkosten und iKey(optional) im Preis enthalten. Preise exkl. USt, inkl. Einrichtung des Zuganges, exkl. Clientinstallation und Support. Freischaltungen an CNV-Kundennetzen, Installationshilfe und Support sowie die Änderung von Accounts werden zu den üblichen Stundensätzen der VTG verrechnet.

Beschreibung der erforderlichen Freischaltungen:

Server	Dienst	Port	Begründung

Gewünschte Inbetriebnahme: .....

Der Zugang wird eingerichtet für die Zeitdauer (bitte ankreuzen):

☐ unbefristet (z.B. Telearbeiter)
☐ temporär (z.B. Wartungsfirma) von-bis: .....

Die Sicherheitsvereinbarungen sind bekannt und wurden/werden vom Benutzer unterschrieben.

....
(Datum) (Stempel, Unterschrift des CNV-Kunden)

1 Sollen mehrere Benutzer Zugriff erhalten, muss diese Anmeldung mehrfach ausgestellt werden. Formular auch im Internet verfügbar: http://www.vtg.at/dl/tw-anmeldeformular.doc
2 Die Rechnungslegung erfolgt immer an den CNV-Kunden.