

## Success Story: Kreisverwaltung Cochem-Zell



# Erweiterung der Zugriffsoptionen: Citrix Access Gateway mit Advanced Access Control Options ermöglicht sicheren Zugriff auch für unbekannte Clients

Die Verwaltungen in Rheinland-Pfalz ermöglichen seit 2004 Außenstellen und Mitarbeitern einen geschützten, sicheren Zugang über das Internet ins Netz der eigentlichen Verwaltung. Eine konsequente Überwachung und Pflege der externen Clients ist allerdings nur für Geräte möglich, die der Administrationsverantwortung der Verwaltung unterliegen. Ein gehärteter Client kann zwar vorgeschrieben, aber im Augenblick des Zugriffs nicht überprüft werden. Deshalb sollte in der Kreisverwaltung Cochem-Zell die vorhandene Zugangslösung durch den Einsatz des Citrix Access Gateway mit Advanced Control Options erweitert werden. Darüber hinaus sollen Secure ThinClients zum Einsatz kommen. Mit der Analyse, Konzeption und Umsetzung des Projekts wurde die net on Netzwerktechnologien Online GmbH aus Mainz beauftragt, Spezialist für Application Delivery-Lösungen.

*„Da wir bei der Realisierung einer Citrix-Umgebung mit net on bereits sehr gute Erfahrungen gemacht haben, lag es für uns nahe, auch diese Citrix-Lösung mit net on zu realisieren. Die Zugriffsszenarien auf das Verwaltungsnetzwerk konnten erweitert werden, ohne die Sicherheit zu gefährden. Die Kompetenz und Erfahrung von net on im Citrix-Umfeld ist beeindruckend.“*

Gerhard Richter,  
Leiter IT Kreisverwaltung Cochem-Zell

### Ausgangslage

Seit 2004 können die Verwaltungen in Rheinland-Pfalz Außenstellen und Mitarbeitern einen sicheren Zugang zum LAN der jeweiligen Verwaltung ermöglichen. Dies geschieht mit Hilfe des so genannten Kommunalbundles der Firma ecos und dem Einsatz von Kobil SmartCard-Lesern. Das ecos Kommunalbundle besteht aus einem VPN-Gateway und einer Firewall mit Zertifikatsserver der BB-5000® Produktlinie. Der Nutzer benötigt einen gehärteten Client, der einen SmartCard-Kartenleser und eine

gültige Signaturkarte erfordert. Die Verarbeitung der Daten bei der Kreisverwaltung Cochem-Zell erfolgt über Citrix Terminalserver ausschließlich im Verwaltungszentrum. Über das VPN werden lediglich die Bildschirmausgaben in komprimierter und verschlüsselter Form zum Nutzer übertragen. Bei der Anmeldung am VPN-Gateway überprüft dieses das vom Nutzer übermittelte Zertifikat und baut eine verschlüsselte Verbindung vom LAN der Verwaltung zum Client auf. Dieser hat dann Zugriff auf alle Anwendungen und Daten, die ihm auf Basis der Nutzerauthentifizierung durch Citrix bereitgestellt werden.

### Nachteile der bisherigen Lösung

Eine konsequente Überwachung und Pflege der externen Clients ist nur für Geräte möglich, die der Administrationsverantwortung der Verwaltung unterliegen. Die Härtung der Clients war zwar vorgeschrieben, aber im Augenblick des Zugriffs nicht überprüfbar. Dies betraf z.B. die Aktualität der Personal Firewall, des Virenschanners oder des Windows Patchlevels.

### Projektanforderung

Um diese Nachteile auszugleichen, sollten die bisherigen Zugriffsszenarien erweitert werden ohne die Sicherheit des Verwaltungsnetzwerkes zu gefährden. Nach eingehender Analyse schlug net on der Kreisverwaltung Cochem-Zell den Einsatz des Citrix Access Gateway mit Advanced Access Control Options sowie den Einsatz von Secure ThinClients vor.

### Secure ThinClients

Secure ThinClients ermöglichen hochsichere, externe Verbindungen auf Terminalserver (z.B. Citrix, Windows u.a.) oder Webserver im Firmennetzwerk über das Internet oder über WLAN. Sie sind speziell für den Einsatz außerhalb des lokalen Netzes in einer unsicheren Umgebung konzipiert und erlauben die hochsichere VPN-Anbindung von Außenstellen und mobilen Mitarbeitern. Secure ThinClients sind spezielle ThinClients mit integrierten Optionen für den Anschluss an das Internet über ISDN, DSL oder UMTS sowie einem integrierten Smart-Card-Kartenleser. Sie fungieren ausschließlich als Terminals, denn die Verarbeitung der Daten findet im Verwaltungsnetzwerk statt. Damit ist Sicherheit und Wartungsfreiheit garantiert.

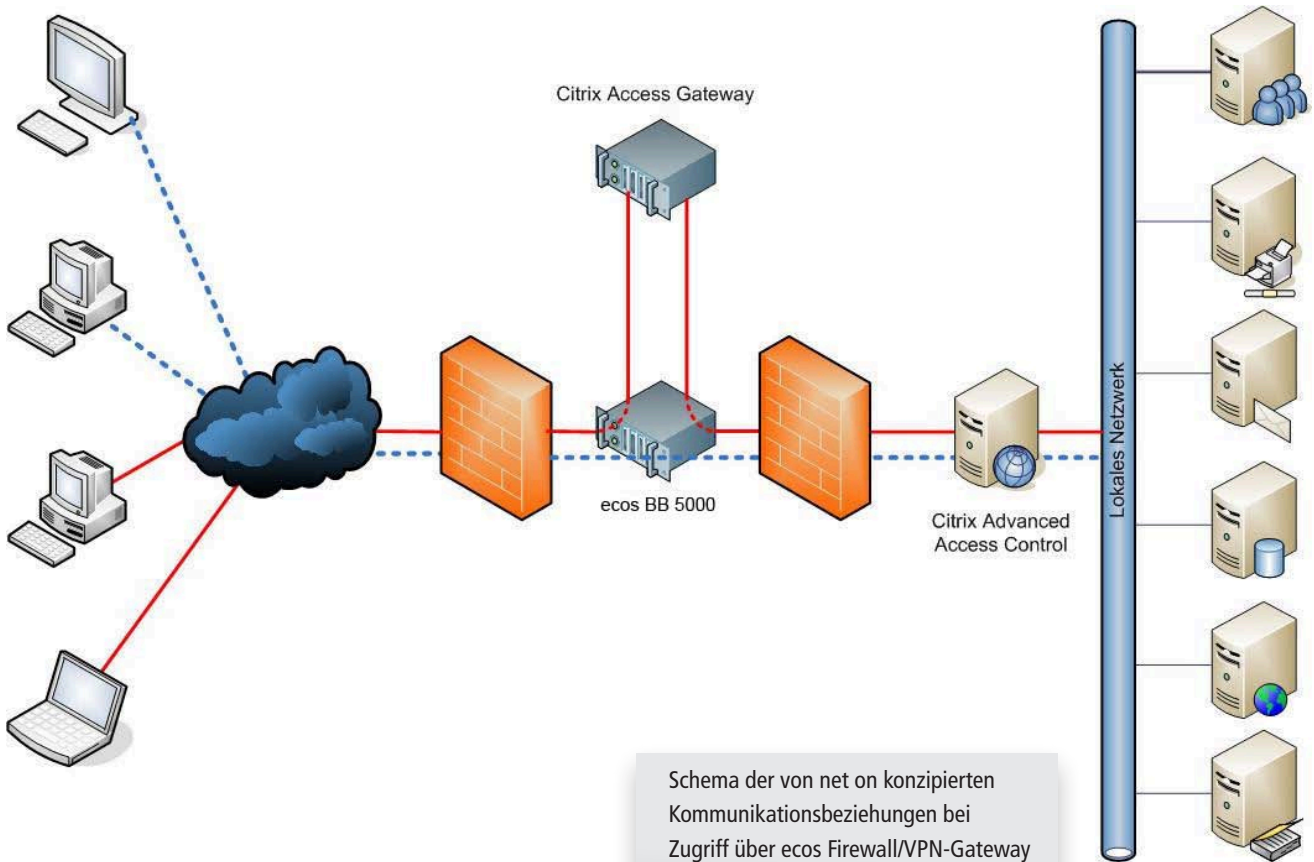
### Citrix Access Gateway

Citrix Access Gateway ist eine SSL-VPN fähige Appliance. Sie sichert den Remote-Zugriff auf sensible Unternehmensinformationen und Anwendungen jeder Art. Access Gateway ermöglicht die Erstellung von Richtlinien, die dynamisch auf das jeweilige Zugriffsszenario des Benutzers reagieren und die Nutzungsrechte entsprechend anpassen. Durch kontinuierliches Endpoint-Scanning mit Advanced Access Control Options wird darüber hinaus sichergestellt, dass Endgeräte die nötigen Sicherheitsanforderungen für Verbindungen in das Unternehmensnetzwerk erfüllen, also z.B. mit aktueller Anti-Virus-Software und einer aktiven Firewall versehen sind. Über frei definierbare Regeln werden das zugreifende Endgerät und die Art des Zugriffs analysiert. Abhängig vom Ergebnis werden exakt abgestimmte Zugriffsberechtigungen erteilt. Verschiedene Zugriffsszenarien sind somit eindeutig definierbar. Der Nutzer identifiziert sich über ein OTP (One Time Password). Das OTP wird über ein Token generiert, welches die Verwaltung zur Verfügung stellt.

### Neue Lösung

Als sicher eingestufte Clients werden wie bisher durch das Kommunalbundle von ecos authentifiziert und der entsprechende Zugriff konfiguriert bzw. gewährleistet. Dabei werden diese Clients an einen dedizierten LogonPoint im sicheren Netz weitergeleitet, der nicht aus dem unsicheren Netz erreichbar ist. Als nicht sicher eingestufte Clients werden durch das VPN-Gateway und der Firewall zum Access Gateway weiter geleitet. Dieses führt die Analyse des Endgeräts durch, bei positiver Prüfung gewährleistet Access Gateway granularen Zugriff auf Anwendungen und Verzeichnis des Verwaltungsnetzwerkes. Die Verschlüsselung des SSL-Datenverkehrs zum Access Gateway wird durch Zertifikate abgesichert. Sämtliche Verbindungen zum ecos Kommunalbundle und zum Citrix Access Gateway sowie die Ergebnisse der Endpoint-Analyse können zur späteren Auswertung an zentraler Stelle protokolliert werden.

# Success Story: Kreisverwaltung Cochem-Zell



Schema der von net on konzipierten Kommunikationsbeziehungen bei Zugriff über ecos Firewall/VPN-Gateway und Citrix Access Gateway mit Advanced Control Options

## Der Kunde

Der Landkreis Cochem-Zell gehört zur Region Mittelrhein mit Koblenz als Oberzentrum. Der Tourismus ist eine der Haupterwerbsgrundlagen im Landkreis. Die Fremdenverkehrsstatistik weist jährlich etwa 1,8 Millionen Übernachtungen aus.

## Die Lösung

Erweiterung der bisherigen Zugangslösung zu den Verwaltungsnetzwerken bestehend aus Smart Card und IPSec-/SSL-Verschlüsselung. Ziel: unbekannten Clients eingeschränkten Zugriff auf nicht kritische Anwendungen zu ermöglichen, ohne die Sicherheit des Verwaltungsnetzes zu gefährden. Maßnahmen: Implementierung von Citrix Access Gateway mit Advanced Access Control Options sowie Einsatz von Secure ThinClients. Das bisherige Zugangsszenario bleibt weiter bestehen.

## Der Nutzen

Konsequente Überwachung und Pflege der externen Clients. Erweiterung der sicheren Zugriffsoptionen auf das Verwaltungsnetz.

Die net on Netzwerktechnologien Online GmbH ist Spezialist für Application Delivery-Lösungen. Mit dem Ziel „IT so einfach wie Fernsehen“ und als Partner führender Hersteller, wie z.B. Citrix, sucht net on für seine Kunden passende Lösungen zur Bereitstellung und Verwaltung von IT-Anwendungen, Desktops, Servern und SaaS-Dienstleistungen.

net on wurde 1997 in Mainz gegründet und ist seither stetig gewachsen. Neben dem Hauptsitz Mainz unterhält net on Filialen in Koblenz, Wetzlar und St. Augustin. net on arbeitet auf der Basis von Virtualisierungstechnologien, Software as a Service (SaaS) und Cloud Computing an der Vision von IT als reiner Dienstleistung „aus der Steckdose“ – einschalten und loslegen.

Zentrale Rhein/Main  
Robert-Koch-Straße 41  
D-55129 Mainz  
fon +49 (6131) 914-300  
fax +49 (6131) 914-390

Filiale Köln/Bonn  
Grantham-Allee 2-8  
D-53757 Sankt Augustin  
fon +49 (2241) 166-552  
fax +49 (6131) 914-390

Filiale Mittelhessen  
Karl-Kellner-Ring 41  
D-35578 Wetzlar  
fon +49 (6441) 210-4295  
fax +49 (6131) 914-390

Filiale Koblenz  
Löhrstraße 113  
D-56068 Koblenz  
fon +49 (261) 88964-54  
fax +49 (261) 9215300