TRISEC
YOUR WAY INTO SECURITY

SUCCESS STORY

Remote Access SSL-VPN-Lösung für Main-Kinzig-Kliniken gGmbH

Executive summary

Die Main-Kinzig-Kliniken gGmbH suchten eine Lösung, Mitarbeiter mit Heimarbeitsverträgen, Belegärzten und Mitarbeitern im Bereitschaftsdienst an das Unternehmensnetzwerk anzubinden. Aufgrund der steigenden Zahl entsprechender Benutzer stellte die bisherige RAS-Lösung mit Rückruf keine adäquate Möglichkeit mehr dar. Da bisher schon die Einbindung über Citrix Terminalserver erfolgte, wurde nach einer Citrix-basierten VPN-Lösung gesucht.
Nach Gesprächen und Erfahrungsberichten mit verschiedenen Dienstleistern wurde eine SSL-VPN Lösung favorisiert.
Die Authentifizierung der Benutzer sollte zur zusätzliche Sicherheit mittels Tokencode und PIN-Eingabe erfolgen.

Kunde

Die Main-Kinzig-Kliniken gGmbH sind im Jahr 1997 aus dem Eigenbetrieb der drei Kreiskrankenhäuser mit Standorten in Gelnhausen, Schlüchtern und Bad Soden-Salmünster in der Rechtsform einer gemeinnützigen GmbH entstanden.
Alleiniger Eigentümer ist der Main-Kinzig-Kreis. Heute bieten sie als eine Klinik an drei Standorten auf allen Gebieten der Grund- und Regelversorgung stationäre und ambulante Behandlungen an.

Gelnhausen

Die Main-Kinzig-Klinken behandeln in 12 Fachrichtungen und bieten auf die drei Standorte verteilt 689 Betten.
Sie sind Träger einer Schule für Pflege-berufe und nehmen als akademisches Lehrkrankenhaus an der studentischen Ausbildung in der Medizin und in den Pflegewissenschaften teil.

Main-Kinzig-Kliniken gGmbH
Gelnhausen Schlüchtern Bad Soden-Salmünster

Aufgabenstellung

Durch die steigenden Anzahl von mobilen Benutzern im Unternehmen und der Zunahme von Breitbandzugängen eben dieser Benutzer, sollte eine Lösung gefunden werden, diese einfach administrierbar, mit verschlüsseltem Datenverkehr und mittels starker Authentifizierung, an das Unternehmensnetzwerk anzubinden. Es wurde über die Verwendung von dedizierten Laptops, software- und hardwarebasierten VPN-Lösungen und die Citrix-eigenen Lösungen (Citrix Secure Gateway, Citrix Presentation Server) nachgedacht. Die Benutzer sollten Zugriff auf ihre gewohnte Citrix-Terminalserverumgebung erlangen können.
Im Laufe der Überlegungen kristallisierte sich als großer Wunsch heraus, dass der Zugang ohne zusätzliche Software auf den Mitarbeiter-PCs möglich sein sollte und somit der administrativen Aufwand weiter minimiert und zentralisiert werden kann.
Aufgrund der Möglichkeiten einer SSL-VPN Lösung entstanden schnell weitere Anforderungen an ein solches System. Direkte Zugriffe auf interne Webseiten sollten ermöglicht werden um dort auf Groupwaresysteme oder Intranetseiten zugreifen zu können. Ebenfalls sollte die Möglichkeit geschaffen werden, auf Freigaben Zugriff erlangen zu können und Daten, zur Bearbeitung, erreichen zu können. Eine eigene Gruppe für die Mitarbeiter der Datenverarbeitung mit zusätzlichen Rechten und Zugriff auf die Managementsysteme musste geschaffen werden.

Wichtigste Punkte der Aufgabenstellung

- Browser-basierende Lösung
- Authentifizierung mittels Tokencode und PIN
- Citrix-Terminalserverumgebung muss für Benutzer verfügbar sein
- Kommunikation muss verschlüsselt erfolgen
- Zugang soll unabhängig von der Art der Internetverbindung möglich sein

TRISEC
YOUR WAY INTO SECURITY

SUCCESS STORY

Remote Access SSL-VPN-Lösung für Main-Kinzig-Kliniken gGmbH

Lösung

Während der Konzeptionsphase stellte sich sehr schnell heraus, dass diese Hauptanforderungen am besten von einer SSL-VPN-Appliance oder der Citrix-eigenen Lösung erfüllt werden konnten. Die Kosten und Features für beide Varianten wurden verglichen und die Vor- und Nachteile einander gegenüber gestellt.

Als Ergebnis dieses Vergleichs hat man sich dazu entschlossen die SSL-VPN Lösung umzusetzen. Für die Auswahl einer SSL-VPN-Appliance wurden Angebote der Hersteller F5 Networks, Netscreen und Aventail einbezogen und letztendlich F5 Networks als umzusetzende Lösung gewählt.
Wegen der Anforderungen, nicht mehr als 100 gleichzeitige Benutzer bedienen zu müssen, wurde ein Produkt aus der Firepass-Serie 1000 ausgewählt. Diese sind von 25 Usern in ebenfalls 25 User-Schritten aufrüstbar, bis hin zu 100 gleichzeitigen Benutzerverbindungen. Zur Authentifizierung wurde auf die weltweit bewährte Lösung von RSA zurückgegriffen und RSA SecurID als Authentifizierungsmechanismus gewählt. In dem Projekt vorangegangenen Tests wurde das Zusammenspiel der Komponenten geprüft und bestätigt.

Die genannte F5/RSA Produktkombination erfordert beim Benutzer keine zusätzliche Software und entspricht somit den Anforderungen des Kunden voll und ganz. Durch ein zusätzlich erworbenes F5 Firepass Webifyer-Modul für Terminalverbindungen, kann man durch die von der Firepass über das Web zur Verfügung gestellten Oberfläche Zugriff auf Citrix-, VNC- und Windows Terminalverbindungen erlangen.

Die installierte Lösung befreit den Kunden von den typischen Remote Access Problematiken, wie Support von Einwahlsystemen und des Endbenutzers. Sofern der Benutzer eine Internetverbindung und einen SSL fähigen Browser besitzt, kann auf das System, unabhängig von der Art der Internetanbindung zugegriffen werden. Sei sie nun mittels analogem Modem, ISDN oder DSL hergestellt worden.
Die F5/RSA Lösung ist sehr kosteneffizient, da sie den administrativen Aufwand auf einem Minimum hält und keine Änderung an der bestehenden Netzwerkinfrastruktur beim Kunden als auch beim Benutzer erfordert.

Die Firepass wurde in die bestehende demilitarisierte Zone der Firewall installiert und im Regelwerk entsprechend bedacht. Es sollen keine Verbindungen zu dem Gerät möglich sein, außer dem SSL-Zugriff der Benutzer. Zur Authentifizierung wird der mit Radius-Support versehene RSA ACE Server verwendet. Die ausschließliche Form der Benutzeranmeldung an der Firepass- wurde mittels Radiusabfrage zum ACE Server konfiguriert, welcher den aktuellen Tokencode, sowie eine benutzereigene PIN erfordert.

Nur bei Gültigkeit von Tokencode und PIN wird dem Benutzer der Zugriff auf die Firepass gewährt. Zugriff auf die Citrixumgebung wurde für die entsprechenden Benutzer erlaubt. Darüber hinaus ist es den Benutzern möglich, auf E-Mails, das Intranet und freigegebene Dateien zuzugreifen. Die Zugriffsberechtigungen für Dateifreigaben übernimmt weiterhin der Windows Domain Controller.

Für die Gruppe der Administratoren wurden Möglichkeiten geschaffen, für Fernwartung zusätzlich Zugriff auf Windows Terminal Services und VNC Verbindungen zu erlangen. Ebenso sind sie in der Lage, die Firepass zu administrieren und können das interne Überwachungssystem Nagios benutzen, um Netzwerkprobleme jederzeit remote erkennen und einkreisen zu können.

Zukunftsideen / Planungen

- Durch das modulare System können weitere Benutzer hinzugefügt werden.
- Drahtlose Benutzer, wie zum Beispiel Ärzte, können sicher ans Netzwerk angebunden werden.
- Belegärzte könnten von der Praxis aus Zugriff erhalten

TriSec GmbH - Senefelderstrasse 1 / T1 - 63110 Rodgau - email: info@trisec.de, url: http://www.trisec.de
Tel. : +49 (0) 6106 70 79 180 Fax : +49 (0) 6106 70 79 189

SUCCESS STORY

Remote Access SSL-VPN-Lösung für Main-Kinzig-Kliniken gGmbH

Kurzübersicht Lösungsumsetzung

- Unterschiedliche Benutzerrechtevergabe
- Zwei Wege Authentifizierung
- Kommunikation ist verschlüsselt und Leitungs- sowie Betriebssystem unabhängig
- Einfache und zentrale Administration
- Keine Veränderung der bestehenden Netzstrukturen

Warum SSL-VPN mit F5 und RSA?

Die F5 Firepass Komponente wurden den Mitbewerbern aufgrund ihres entscheidenden Preis-/Leistungsvorteil vorgezogen.

Als Punkte für die Wahl RSA SecurID waren das gute Zusammenspiel der Komponenten von RSA und F5 entscheidend, darüber hinaus hat der Erfahrungsaustausch mit anderen Nutzern dieser Systeme gerade in Verbindung mit Citrix den Ausschlag gegeben. Die Lösungen der beiden Hersteller fügen sich problemlos in die bestehende Netz- und Firewallstruktur ein und haben in der vorangegangenen Testphase mit ihren Funktionen überzeugen können. Ein weiterer wichtiger Punkt zum Entschluss für eine SSL-VPN Lösung war die Zukunftssicherheit und die Erweiterbarkeit. Unabhängig von den zukünftigen Entwicklungen ist davon uszugehen dass IP-basierte Netzwerke weiterhin als Transportplattform für das Internet genutzt werden. Da die Verbindungen über eine SSL-Browserverbindung hergestellt werden, ist das zugrunde liegende, Betriebssystem nicht relevant. Dies stellt sicher, dass jeder bestehende und in Zukunft hinzukommende Benutzer, eventuell auch kooperierende Ärzte, an das System angebunden werden können.

Kundenzitat

„Die umgesetzte Lösung ermöglicht uns den vollen Zugriff auf die gewünschten Systeme bei einfacher Administration und bietet unseren Benutzern eine komfortable Lösung ohne auf höchste Sicherheit zu verzichten.“, berichtet Bernd Bischof, EDV Leiter

Umgesetzt durch

TriSec GmbH – Your Way Into Security
Senefelderstr. 1 / T1
D – 63100 Rodgau

Tel.: +49 (0) 6106 - 7079 – 180
Fax.: +49 (0) 6106 – 7079 – 189
http://www.trisec.de
eMail : info@trisec.de

Ansprechpartner
Main-Kinzig-Kliniken gGmbH
B. Bischof

TRISEC
YOUR WAY INTO SECURITY