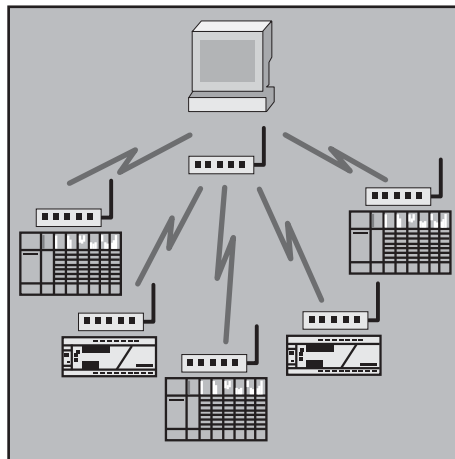


Schwerpunktthema

SCADA und IT-Security: Informations-Sicherheit in Automatisierungs- und Prozesskontrollsystemen

von Dipl.-Phys. Stephan Beirer

Die moderne IT-Technologie hat in den letzten Jahren auch ihren Weg in die klassische Automatisierungs- und Prozessleittechnik gefunden. Damit kommen die bekannten Hardware- und Software-Komponenten mit all ihren Tücken und Sicherheitsproblemen nun auch in sehr sensiblen Produktionsumgebungen und kritischen Infrastrukturen (KRITIS) zum Einsatz. Darüber hinaus wird auch die Vernetzung von einstmalig weitgehend isoliert betriebenen Systemen mit anderen IT-Bereichen immer weiter voran getrieben. Diese unaufhaltsame Entwicklung verlangt dringend nach erweiterten Sicherheitskonzepten, um solch wichtige Ressourcen gegen die neu auftretenden Bedrohungen angemessen abzusichern.



Bei der Steuerung und Überwachung von komplexen industriellen Fertigungsprozessen spielt die elektronische Automatisierungs- und Messtechnik eine wichtige Rolle. Gleiches gilt für die Kontroll- und Leittechnik von räumlich verteilten Systemen wie zum Beispiel Gas- und Ölpipelines, Kommunikations- und Stromnetzen oder Verkehrstelematik-Systemen. Die in diesen Bereichen verwendeten Technologien werden meist unter den Oberbegriffen DCS (Distributed Control Systems) und SCADA (Supervisory Control and Data Acquisition) zusammengefasst.

weiter auf Seite 22

Zweitthema

RAS via VPN - Leitfaden anhand eines Projektbeispiels

von Dipl.-Inform. Andres Meder

Die Nutzung Virtueller Privater Netze (Virtual Private Networks, VPN) hat sich in der jüngeren Vergangenheit insbesondere im Bereich des Remote Zugriffs mobiler oder auch stationärer Anwender (Stichwort: Telearbeit) auf zentrale Ressourcen als mehr oder weniger Standard-Lösungsansatz etabliert.

Wer als Hersteller von Netzwerktechnik - sei es auf dem Infrastruktur- oder auch auf dem Sicherheitssektor - etwas auf sich hält, bietet entsprechende Lösungen mit teilweise üppigem Funktionsumfang an. Gerade dieses umfangreiche Angebot stellt den Netzwerkverantwortlichen, der mit dem Aufbau einer geeigneten Lö-

sung für die jeweiligen Rahmenbedingungen betraut ist, jedoch vor mitunter nicht einfach zu treffende Entscheidungen. Schlagworte sind hier unter anderem: IP-Sec oder SSL, Security Token oder Smart Cards, transparenter Netzzugriff: ja oder nein, ...

weiter auf Seite 9

Top Veranstaltung

**ComConsult
IT-Sicherheits-
Forum 2007**

auf Seite 6

Zum Geleit

**Asterisk:
OpenSource-
Telefonie wirklich
reif für die
Nutzung in
Unternehmen?**

auf Seite 2

Report des Monats

**VPN-Technologien:
Alternativen und
Bausteine
einer erfolgrei-
chen Lösung**

auf Seite 20

Zweitthema

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Fortsetzung von Seite 1



Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Dieser Artikel versucht, auf Basis aktueller Projekterfahrungen einen Leitfaden für den oben erwähnten Verantwortlichen zu erstellen, mit dessen Hilfe für die allermeisten Szenarien eine sinnvolle Lösung aufgebaut werden kann. Dazu werden diverse grundsätzliche Fragestellungen, die in derartigen Realisierungsprojekten häufig auftauchen, diskutiert und - hoffentlich - hinreichend beantwortet. Den Abschluss bildet ein kurzer Blick auf ein beispielhaftes auf der Basis dieses Leitfadens abgewickelter Planungsprojekt, das in ähnlicher Ausprägung tatsächlich realisiert worden ist.

Zusätzlich zu den diskutierten Aspekten ist natürlich - auch wenn auf diesen Bereich hier nicht im Detail eingegangen wird - wie bei jedem Konzept zunächst eine Analyse des Status Quo und der Vorstellungen bzw. Wünsche hinsichtlich der zu entwickelnden Lösung voranzustellen. Diese Ist- und Anforderungsanalyse ist wesentlicher Eckpfeiler jedweder Konzeption und Planung und sollte daher keinesfalls als unangenehme „langweilige“ Begleiterscheinung des ansonsten „spannenden“ Projekts angesehen werden. Andernfalls ist die Gefahr groß, dass man mit der neu konzipierten Lösung nicht allzu lange wirklich glücklich wird...

Wie können die Sicherheitsziele erreicht werden?

Für die Konzipierung von Kommunikationslösungen sind regelmäßig folgende Sicherheitsziele zu unterstellen:

- Vertraulichkeit (von übertragenen bzw. gespeicherten Informationen)
- Integrität (von Systemen bzw. übertragenen oder gespeicherten Informationen)
- Verfügbarkeit (von Systemen bzw. nachgefragten Informationen)

Eine zu konzipierende VPN-Lösung trägt diesen Sicherheitszielen sinnvollerweise wie folgt Rechnung:

Sichere VPN-Lösungen basieren auf dem Aufbau von Kommunikationstunneln zwischen den beteiligten Partnern (Einzelplatz-Client bzw. Remote Netz sowie internes Netz des zentralen Standorts) über das Internet. Für diese Tunnel wird ein Mechanismus verwendet, der durch Anwendung hinreichend starker kryptografischer Methoden sowohl die Vertraulichkeit der übertragenen Informationen als auch deren Integrität sicherstellt. Hierfür finden Verschlüsselungsalgorithmen sowie Prüfsummenverfahren Verwendung.

Zur Sicherstellung der Vertraulichkeit und Integrität gespeicherter Informationen und von Systemen (innerhalb des internen Netzes) verwendet eine solche VPN-Lösung üblicherweise Filtertechniken, die Zugriffe auf das interne Netz ohne Verwendung der zugelassenen VPN-Tunnel verhindern. Hierfür werden klassische Paketfilter (z.B. Access Control Lists) eingesetzt, die jegliche Kommunikation verwerfen, die nicht zu bestehenden VPN-Tunneln gehört oder für den Aufbau solcher Tunnel notwendig ist. Zur Prüfung, inwieweit VPN-Tunnel zulässig sind, werden als hinreichend stark eingeschätzte Methoden zur Authentifizierung der jeweiligen Kommunikationspartner eingesetzt - hierunter können durchaus unterschiedene Methoden verstanden werden:

Im Falle von Client-PCs, die einen Tunnel zum internen Netz aufbauen (Client-to-Site-Szenario) kommen hierzu grundsätzlich SmartCards oder Security-Token in Frage - von der Nutzung einfacher „Nutzername / Kennwort“-Kombinationen ist in der Regel abzuraten, da eine sichere Wahl

derartiger Passwörter für sämtliche Konten in der Praxis unmöglich zu gewährleisten ist. Die Vorgabe komplexer Regeln zur Generierung solcher Passwörter ist hier eher kontraproduktiv, da die Neigung der Anwender, die Passwörter niederzuschreiben, umso größer ist, je komplexer und damit schwerer im Gedächtnis zu behalten diese sind. Mindestens in Szenarien, in denen davon auszugehen ist, dass auch Zugriffe von beliebigen Client-Systemen aus erfolgen müssen (z.B. aus Internet-Cafés), ist dem Ansatz des Security-Tokens jedoch eindeutig der Vorzug gegenüber der SmartCard zu geben. Bei diesen Token handelt es sich um tragbare Passwortgeneratoren, mit deren Hilfe sich der Besitzer beim Aufbau des VPN-Tunnels durch Eingabe des generierten Einmal-Passwortes - in der Regel in Verbindung mit einer nur ihm bekannten PIN - eindeutig ausweisen kann. Über den Einsatz im Rahmen der VPN-Lösung hinaus lassen sich Security-Token praktisch überall einsetzen, wo eine Kennwort-basierte Benutzerauthentifizierung vorgesehen ist, und bieten somit erweitertes Nutzungspotenzial.

Zusätzlich zur Authentifizierung des jeweiligen Benutzers sollte ggfs. eine hinreichend sichere Identifizierung von Clients auf Basis von Managed PCs (s.u.) möglich sein, dies kann durch eine Systemauthentifizierung beispielsweise auf Basis von Zertifikaten erfolgen.

Wird der Tunnel zum internen Netz nicht vom Client-PC des Anwenders, sondern von einem vorgelagerten System (VPN-Gateway) aufgebaut, kommt der Einsatz von Security-Token aus technischen Gründen i.d.R. nicht in Frage, da diese das Ablesen und Eingeben des Einmal-Passworts durch einen Nutzer erfordern. Hier reicht

RAS via VPN - Leitfaden anhand eines Projektbeispiels

jedoch die Verwendung hinreichend langer und komplex aufgebauter statischer Passwörter zur Authentifizierung aus, da die Nachteile statischer Passwörter (zu geringe Länge und Komplexität, absichtliche oder fahrlässige Preisgabe durch den Anwender) nicht zum Tragen kommen. Solche Passwörter sollten „zufällig“ generiert werden; ihre Länge sollte dabei mindestens 12 Zeichen betragen. Eine regelmäßige Änderung in kurzen Intervallen ist normalerweise nicht erforderlich, da etwaige Versuche, das Passwort durch Raten in Erfahrung zu bringen, durch zu lange Zeitdauer und zwangsläufige Entdeckung zum Scheitern verursacht sind.

Die dargestellten Maßnahmen werden sinnvoll ergänzt durch eine Kanalisierung der Zugriffsrechte. Hierzu lässt sich ein zusätzlicher Filter einsetzen, der je nach Identität des Anwenders den Zugriff auf bestimmte interne Ressourcen freigibt oder sperrt (Firewallfunktionalität; s.u.).

Maßnahmen zur Sicherstellung der Verfügbarkeit von Systemen oder Informationen im internen Netz durch die VPN-Lösung müssen sich naturgemäß auf den Kommunikationspfad beschränken; die Systeme und Informationen selbst können hier nicht berücksichtigt werden. Die Verfügbarkeit des VPN-basierten Zugriffs hängt von vielen Faktoren ab; zu den wesentlichen hier zu berücksichtigenden zentralen Faktoren zählen:

- das zentrale VPN-Gateway,
- die Anbindung dieses VPN-Gateways an das interne Netz,
- die Anbindung des VPN-Gateways an das Internet.

Die beiden letzten Faktoren sollen hier nicht weiter betrachtet werden. In den meisten Fällen muss hier bei der Konzipierung einer VPN-Lösung auf die bereits vorhandenen Rahmenbedingungen Rücksicht genommen werden; eine komplette Neuplanung der besagten Schnittstellen kommt eher selten in Betracht.

Je nach den zu berücksichtigenden infrastrukturellen Gegebenheiten kommen für das VPN-Gateway - in Abhängigkeit von der konkreten Lösung - verschiedene Ansätze zur Verfügbarkeitssicherung in Betracht. Zu den gängigsten zählen:

- Einsatz einer Cluster-Lösung
- Einsatz einer Hot-Standby-Lösung
- Einsatz von Load-Balancern
- Einsatz dynamischer Routing-Mechanismen
- Definition alternativer Peers in den jeweiligen Gegenstellen

- Bereithaltung eines identischen Reserve-Systems (Cold Standby)

Je nach konkreten Anforderungen reicht häufig zunächst ein Cold Standby-Ansatz aus. Die konzipierte Lösung sollte jedoch grundsätzlich zumindest die Option auf einen höherwertigen Ansatz bieten; insofern ist bei der Evaluierung von Produkten auf entsprechende Möglichkeiten zu achten.

Wie lassen sich bei Bedarf Hersteller- und Produktneutralität sicherstellen?

Eine strikte Neutralität hinsichtlich der beim Aufbau der Lösung einzusetzenden Produkte bzw. deren Hersteller ist üblicherweise nur im Bereich der Ausschreibung durch öffentliche Auftraggeber zu wahren. Ist ein entsprechender Bedarf - aus welchem Grund auch immer - gegeben, so sollte folgendes beachtet werden:

Alle durch das Konzept an eine konkrete Lösung gestellten Anforderungen sind grundsätzlich produkt- und herstellernerutral zu formulieren. Wird in Einzelfällen dennoch auf bestimmte Hersteller oder deren Lösungen Bezug genommen, so sollte darauf hingewiesen werden, dass dies stets als beispielhafte Nennung einer denkbaren Lösung zu verstehen ist. Im Bereich öffentlicher Ausschreibungen ist diese Vorgehensweise übrigens - spätestens bei Formulierung der Leistungsbeschreibung - als ultima ratio zu verstehen, d.h. dergleichen ist nur dann vergaberechtlich zulässig, wenn auf andere Weise (also durch allgemeine Begriffe) eine hinreichend genaue

Beschreibung der gewünschten Leistung nicht möglich erscheint.

Derartige beispielhafte Lösungsansätze können im Übrigen während der Konzipierungsphase gleichzeitig dem Nachweis dienen, dass die jeweils konzipierte abstrakte Lösung auch tatsächlich auf der Basis marktverfügbarer Produkte realisierbar ist.

Wie kann ein sicherer Remote-Zugriff sowohl durch eigene Mitarbeiter als auch durch Fremdfirmen erfolgen?

Ein geeignetes VPN-Konzept, wie es das Ziel dieses Leitfadens ist, sollte den Remote-Zugriff durch unterschiedliche Nutzergruppen unterstützen; hier sind insbesondere eigene Mitarbeiter und Fremdfirmen zu unterscheiden. Dazu bieten sich folgende Mechanismen bzw. Ansätze an:

- Einsatz eines Filtermechanismus zur Steuerung des Zugriffs auf interne Ressourcen (s.o.)
- Ermöglichung unterschiedlicher Zugriffsszenarien je nach Nutzergruppe und Nutzungsverhalten

Ansatz 1: Steuerung des Zugriffs

Der Zugriff auf interne Ressourcen wird üblicherweise mittels Firewalltechnik gesteuert: ein geeignetes Filterelement - typischerweise auf Basis eines Paketfilters - lässt Zugriffe auf interne Systeme über bestimmte Dienste je nach Nutzergruppe zu oder sperrt diese.

Report

VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung



Der komplett überarbeitete und neu aufgelegte Technologie-Report von ComConsult Research zeigt alle wichtigen Meilensteine bei Aufbau, Organisation und Betrieb einer VPN-Lösung. Die einzelnen Bausteine typischer Installationen werden anhand praxisnaher Vorgaben bewertet und ein umfangreiches Projekt- und Konfigurationsbeispiel detailliert besprochen. Insgesamt werden Sie somit in die Lage versetzt, Ihre eigene technisch und wirtschaftlich optimale VPN-Lösung zu entwerfen, in Ihr Gesamtkonzept einzubinden und zu betreiben.

Autor: Dipl.-Inform. Andreas Meder
Preis: € 398,- zzgl. 7% MwSt. und Versand



Bestellen Sie über unsere Web-Seite www.comconsult-research.de

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Für diese Aufgabe kann prinzipiell eine vorhandene Internet-Firewall verwendet werden; günstiger ist es jedoch zu meist, diese Aufgabe dem zentralen VPN-Gateway zu übertragen. Hierdurch ist u.a. eine bessere benutzerbezogene Steuerung möglich (s.u.). Die Lösung (d.h. das als VPN-Gateway einzusetzende Produkt) sollte daher eine derartige Steuerungs-möglichkeit bieten.

Zu beachten ist, dass sich die Steuerung in Abhängigkeit von der Art des Zugriffs (s.u.) unterschiedlich darstellt:

- Bei Client-to-Site-Zugriffen werden die Zugriffsregeln an den jeweiligen Benutzer (bzw. die jeweilige Benutzergruppe) gebunden - nur einem entsprechend berechtigten und authentifizierten Benutzer wird der Zugriff auf die gewünschten Ressourcen gestattet.
- Bei Site-to-Site-Zugriffen werden die Zugriffsregeln an das jeweilige Remote-Netz gebunden - jedem aus diesem Netz zugreifenden Benutzer wird der Zugriff im Rahmen der für das Remote-Netz geltenden Berechtigungen gestattet. Es sind daher bei Fremdzugriffen entsprechende organisatorische Maßnahmen in Form vertraglicher Regelungen zu ergreifen, um einen Missbrauch der so geschaffenen Netzverbindung hinreichend unwahrscheinlich zu machen. Dies gilt im Übrigen stets bei Site-to-Site-Zugriffen, unabhängig von deren technischer Realisierung; insofern ist diese Problematik auch dann gegeben, wenn etwa für derartige Zugriffe eigenständige Lösungen (z.B. eine Dial-In-Lösung) eingesetzt werden.

Grundsätzlich ist eine benutzerbezogene Filterung für solche Szenarien zwar denkbar - dazu ist eine Authentifizierung des Anwenders gegenüber dem Filter erforderlich - wird in der Praxis jedoch ohnehin meist „unterlaufen“, indem die notwendigen Identitätsausweise (Security Token) innerhalb von Nutzergruppen weitergegeben werden. Dies ist gerade bei Wartungsfirmen gängige Praxis, da eine feste Bindung einer oder weniger Personen des Service-Teams an den Kunden weder machbar noch in dessen Sinne. Üblicherweise erhalte daher schon aus Gründen der Minimierung von Kosten und Administrationsaufwand die Wartungsfirma ein für jeden Techniker frei zugängliches Gemeinschaftstoken; damit ist aber gegenüber der skizzierten Lösung einer Authentifizierung des gesamten Netzes durch das Remote-Gateway kein nennenswerter Sicher-

heitsgewinn mehr erzielbar. Es ist daher üblicherweise zur Minimierung des Gesamtaufwands von einem solchen Ansatz eher abzuraten.

Ansatz 2: Zugriffsszenarien

Für interne Mitarbeiter empfiehlt sich in der Regel ein Zugriff über einen direkten Tunnel zwischen Client und VPN-Gateway. Diese Form des Zugriffs ermöglicht die präziseste Form der Zugriffssteuerung (s.o.) und bestmögliche Abschottung der jeweiligen Kommunikationsbeziehung von der Umgebung. Als Methode der Wahl haben sich hier in der Vergangenheit IPSec-basierte Client-to-Site-VPNs bewährt.

Aufgrund der relativen Freizügigkeit der Kommunikation, insbesondere der Möglichkeit, Daten mit dem internen Netz auszutauschen, sind an derart ausgestattete Client-Systeme gewisse Anforderungen hinsichtlich des Sicherheitsstatus zu stellen. Konkret sollte ein remote-Client systemtechnisch mindestens dem Sicherheitsstatus eines internen Clients entsprechen. Zusätzlich muss er sich über entsprechende clientseitige Firewallfunktionen gegenüber etwaigen Bedrohungen aus dem VPN-Trägernetz (also üblicherweise dem Internet) schützen können.

Es existieren VPN-Lösungen am Markt, die Mechanismen zur weitgehenden Sicherstellung eines adäquaten Client-Status bieten. Nach Möglichkeit sollte für die konkrete Realisierung einer solchen Lösung der Vorzug gegeben werden.

Produktabhängig kann alternativ der Einsatz eines SSL-basierten VPNs hierfür in Frage kommen. Dazu muss die Lösung sicherstellen, dass ein transparenter Zugang wie beschrieben nur auf der Basis eines vom Betreiber des internen Netzes gestellten Clients mit hinreichendem Sicherheitsstatus (s.o.) erfolgen kann, beispielsweise durch Einsatz eines dedizierten SSL-Clients als Lösungsbestandteil.

Es gibt jedoch auch Nutzergruppen oder Einsatzszenarien, die mit IPSec-basierten Lösungen generell nicht sinnvoll bedient werden können:

- Nicht in allen Fällen kann ein eigener Mitarbeiter einen durch seinen Arbeitgeber bzw. dessen Netzbetreiber bereitgestellten und administrierten Client („Managed PC“) für den VPN-Zugriff nutzen - nur solche kommen jedoch üblicherweise für den oben dargestellten Ansatz in Frage. Nutzt der Mitarbeiter ein „fremdes“ System, so ist mit an Sicherheit grenzender Wahrscheinlichkeit davon auszugehen, dass dieses nicht für

die Nutzung des IPSec-VPN ausgestattet ist; Standard-Gründe sind fehlende Client-Software bzw. fehlendes Systemzertifikat. Sollen auch in solchen Fällen die Mitarbeiter mit einem VPN-Zugang versorgt werden, so kommt sinnvoll nur ein „clientless VPN“ auf Basis von SSL unter Nutzung eines Web-Browsers als Client in Frage. Auf dieser Basis ist ein Zugriff technisch von praktisch jedem Endgerät mit Internetzugang möglich, beispielsweise auch aus Internet-Cafés.

Aufgrund der vielfältigen Risiken für das interne Netz, die von fremden Clients ausgehen - an dieser Stelle sei exemplarisch die Verbreitung von Viren oder Würmern genannt - , kann ein solcher Zugriff allerdings nur sehr restriktiv zugelassen werden. Konkret bedeutet dies:

- Zugriff nur Terminalserver-basiert
- Kein Dateitransfer zwischen Client und Server

Da diese Form des Zugriffs sowohl sicherheitstechnisch als auch vom Administrationsaufwand her als optimal anzusehen ist, kann sie generell auch als Standardlösung für interne Mitarbeiter vorgesehen werden, die keinen Bedarf an transparenter Netzkopplung haben (solcher Bedarf kann z.B. aufgrund notwendiger Datenaustausche entstehen oder weil die genutzten Anwendungen nicht zur Bereitstellung via Terminalserver geeignet sind).

- Mitarbeiter von Wartungsfirmen greifen typischerweise von ihren eigenen Clients aus auf die gewarteten Systeme im internen Netz zu. Eine Installation des für einen IPSec-basierten VPN-Zugriff notwendigen VPN-Clients wirft sowohl technische als auch organisatorische Probleme auf:

- In der Regel wird ein solcher Techniker mehr als nur einen Kunden betreuen. Die Installation mehrerer IPSec-VPN-Clients auf einem Endgerät führt jedoch in vielen Fällen zu Schwierigkeiten.
- Es wäre zu klären, wer ggfs. für den Support solcherart ausgestatteter Clients verantwortlich ist.

Die Bereitstellung eines entsprechenden Client-Systems durch den internen Netzbetreiber würde die beschriebenen Probleme lösen, ist aber mit Blick auf die potenziellen weiteren Kunden aus Sicht der Wartungsfirma in der Regel nicht praktikabel. Außerdem wäre ein solcher Ansatz mit zusätzlichen Kosten verbunden und die Frage des (Vor-

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Ort-)Supports für diese Systeme wäre ebenfalls ein nicht trivial zu klärendes Problem.

Eine Verwendung eines clientless-Ansatzes auf Basis von SSL (s.o.) kommt ebenfalls nicht in Frage, da für solche Zugriffe aufgrund des hohen Risikopotenzials nur eingeschränkte Funktionalität vorgesehen werden sollte, die für Wartungszwecke im Allgemeinen bei weitem nicht ausreicht.

Für Zugriffe der beschriebenen Art eignet sich deutlich besser der Einsatz von Site-to-Site-Tunneln zwischen dem Netz der Wartungsfirma und dem internen Netz.

- Neben den oben angesprochenen Wartungsfirmen kommen häufig auch andere Fremdfirmen als Nutzer der VPN-Lösung in Betracht, z.B. Ingenieurbüros oder externe Berater, die in die Abwicklung von Projekten involviert sind. Für derartige Nutzergruppen reicht in den meisten Fällen ein clientless-Zugriff analog zu oben vollkommen aus.

Kann die VPN-Infrastruktur auch für sicheren Zugriff auf externe Ressourcen genutzt werden?

Neben dem klassischen Fall des Remote-Zugriffs im Rahmen der VPN-Nutzung kann auf der Basis von VPN-Technik grundsätzlich auch ein Zugriff aus dem internen Netz auf extern bereitgestellte Ressourcen erfolgen. Dies ist allerdings aus technischen Gründen nur auf Basis von Site-to-Site-VPN-Tunneln möglich.

Werden aus anderen Gründen ohnehin Site-to-Site-Szenarien durch das VPN-Konzept vorgesehen, lassen sich ohne Mehraufwand auch die beschriebenen Zugriffe realisieren.

Ist die VPN-Lösung skalierbar?

Unter Skalierbarkeit wird die Möglichkeit verstanden, eine konzipierte Lösung an unterschiedliche Mengengerüste anzupassen. Dies bedeutet, dass eine Erweiterung der Leistungsfähigkeit ohne grundsätzliche Änderungen des Konzepts möglich sein muss.

Für VPN-Lösungen sind hier vorrangig folgende Leistungsparameter relevant:

- Verschlüsselter Datendurchsatz
- Maximale Anzahl konfigurierbarer VPN-Peers (Clients oder Remote-Gateways)
- Maximale Anzahl simultan kommunizierender VPN-Peers

Grundsätzlich kommt eine Skalierung eines einzelnen VPN-Systems in der Regel nur im Bereich der unterstützten Peers in Betracht; hier lassen sich - produktabhängig - durch Speicherausbau im Rahmen der vorgesehenen Möglichkeiten entsprechende Erweiterungen der Leistungsfähigkeit realisieren. Bezüglich des Durchsatzes ist eine Skalierung nur dann möglich, wenn durch Austausch vorhandener Hardware gegen leistungsfähigere oder durch Einbau zusätzlicher Hardware der Durchsatz erhöht werden kann; dies betrifft vor allem spezielle Verschlüsselungshardware, die in allen Systemen gehobener Leistungsstufen regelmäßig verbaut wird.

Neben der systeminternen Skalierung kommt grundsätzlich auch eine externe Skalierung durch Hinzunahme weiterer VPN-Systeme hinzu; hierzu sind allerdings mehr oder weniger aufwändige Cluster-Lösungen erforderlich, die nicht nur die Kosten erhöhen, sondern darüber hinaus aufgrund der Komplexität von Loadsharing-Mechanismen im sicherheitssensiblen Verschlüsselungsumfeld nicht immer zu verbesserter Systemstabilität beitragen. Ein Verzicht auf derartige Zusatzmechanismen ist allerdings grundsätzlich möglich und im Sinne obiger Bedenken auch zu empfehlen; vorausgesetzt, eine statische Zuteilung von Peers an die unterschiedlichen VPN-Gateways ist akzeptabel.

Grundsätzlich sollte bei der Planung die Möglichkeit zukünftig steigender Bedarfe geeignet berücksichtigt werden und ggfs. bei der konkreten Produkt- bzw. Mo-

dellauswahl die Einstiegsvariante nicht zu knapp kalkuliert werden. Dann ist zumindest innerhalb eines planerisch überschaubaren Zeitraums die Notwendigkeit einer Skalierbarkeit im obigen Sinne in der Regel nicht gegeben. Muss dennoch eine Erweiterung der Leistungsfähigkeit vorgenommen werden, kann aus Kosten- sowie Praktikabilitätsgründen in den meisten Fällen ohne weiteres ein Aufbau zusätzlicher Gateways, jedoch ohne Cluster- oder Loadbalancer-Lösung erfolgen; die zu bedienenden Verbindungen werden bei diesem Ansatz im Bedarfsfalle basierend auf den bis dahin gemachten Erfahrungen statisch auf die verschiedenen Gateways aufgeteilt.

Wie sehen Maßnahmen zur Gefährdungsabwehr aus?

Jedwedes VPN-Konzept sollte auf einen möglichst sicheren Einsatz der zu schaffenden Lösung ausgelegt sein. Dabei ist vor allem den grundlegenden Sicherheitszielen entsprechend Rechnung zu tragen.

Neben den unmittelbar durch das VPN (bzw. die zu seiner Realisierung genutzten Techniken) verursachten Gefährdungen kommen zusätzlich alle bei jedweder Remote-Kommunikation anfallenden Gefährdungen in Betracht, hierzu zählen insbesondere ein Missbrauch der erteilten Zugriffsrechte durch den Anwender selbst, ein Missbrauch des VPN-Clients als Relay zum Eindringen in das interne Netz (etwa auf der Basis von so genannten Remote Access Trojanern, RAT), eine Verseu-

Seminar



VPN Virtuelle Private Netze: Planung, Konfiguration, Betrieb 05.03. - 07.03.07 in Bonn

VPN-Technologie ist ein unverzichtbarer Teil jeder Netzwerk-Sicherheits-Lösung. Ebenso vielfältig wie die Nutzungsformen sind die Realisierungs-Alternativen und die Integration in bestehende Netzwerk-Infrastrukturen. Dieses 3-tägige Seminar bewertet die bestehenden Alternativen und gibt direkt in der Praxis umsetzbare Empfehlungen zur optimalen Nutzung von VPN-Technologien.

Referent: Dipl.-Inform. Andreas Meder
Preis: € 1.690,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

RAS via VPN - Leitfaden anhand eines Projektbeispiels

chung mit Viren oder ähnlichen Schadprogrammen sowie die Preisgabe interner Informationen.

Setzt man voraus, dass ein akzeptabler Grundschutz innerhalb des internen Netzes gegeben ist, der u.a. einen funktionsfähigen Virenschutz, Sicherheitsvereinbarungen mit den internen Mitarbeitern hinsichtlich der Nutzung von IT-Ressourcen und eine sinnvolle Steuerung von Benutzerrechten umfasst - die Bereitstellung eines solchen Grundschutzes sprengt naturgemäß den Rahmen eines VPN-Projekts -, so ist den genannten Gefährdungen unter dieser Prämisse mit folgenden Maßnahmen zu begegnen:

- Sicherstellung eines funktionierenden Virenschutzes entsprechend dem Virenschutzkonzept für das interne Netz auf allen Client-Systemen, die mit dem internen Netz Daten austauschen können

Dies impliziert:

- Die Ausstattung aller durch den internen Netzbetreiber gestellten VPN-Clientsysteme mit einem Virenschutzmechanismus gemäß gültigem Standard
- Nach Möglichkeit (produktabhängig) eine Überprüfung der Aktualität der jeweiligen Virendefinitionsdateien und Beschränkung der Kommunikation auf unkritische Ziele bzw. mit dem Update-Server bei Bedarf
- Vereinbarung mit allen Fremdfirmen hinsichtlich des Einsatzes eines adäquaten Virenschutzprodukts auf deren Client-Systemen - immerhin sind diese womöglich (s.o.) per Site-to-Site-VPN mit dem internen Netz verbunden...
- Einsatz von Virenschutzprogrammen auf allen Systemen, auf die durch externe Firmen zugegriffen wird, soweit dies technisch möglich ist - insbesondere in Produktionsbereichen und/oder bei Systemen mit Echtzeitanforderungen können sich hier leicht Probleme ergeben
- Vereinbarungen mit allen Fremdfirmen hinsichtlich der Nutzung der zum Zugriff freigegebenen Ressourcen; hierunter fällt insbesondere eine technische Beschränkung (z.B. durch einen Paketfilter) der Clients, die über das VPN auf das interne Netz zugreifen können
- Steuerung des Zugriffs interner und externer Nutzer auf interne Ressourcen

durch Einsatz von Firewalltechnik (s.o.)

- Unterbindung der Kommunikation von VPN-Clients außerhalb des VPN-Tunnels (z.B. durch lokale Firewalltechnik)
- Vereinbarungen mit allen Fremdfirmen hinsichtlich deren sicherer Anbindung an weitere Netze Dritter
- Verhinderung des Datenaustauschs zwischen dem internen Netz und fremden VPN-Clients, mit deren Betreibern keine Sicherheitsvereinbarungen existieren (insbesondere Systeme in Internet-Cafés u.ä.)

Welche Standards sind bei der VPN-Kommunikation einzusetzen?

Diese Frage ist im Grunde zweigeteilt zu betrachten, nämlich hinsichtlich der technologischen Standards, denen eine Lösung sinnvollerweise folgen sollte, und hinsichtlich der organisatorischen Standards, an denen sich der Einsatz bzw. die Nutzung der Lösung zu orientieren hat.

Als technologische Standards sind hier für die beiden grundlegenden Ansätze zum einen IPSec und zu anderen HTTPS (für SSL-basierte Lösungen) zu nennen. Da beide Standards im Internet weit verbreitet sind - ja, im Grunde den Defacto-Standard repräsentieren, sollte die Forderung nach Einhaltung der Standards den Nutzern keine unangemessenen Hürden auferlegen...

In organisatorischer Hinsicht ist zwischen internen und externen Nutzern zu unterscheiden:

Interne Nutzer des VPNs müssen sich an die durch ihren „Dienstherren“ bzw. dessen Netzbetreiber festgelegten Standards halten; dies impliziert insbesondere eine entsprechende Ausstattung der VPN-Clientsysteme mit Kommunikations- und Sicherheitssoftware, soweit diese der administrativen Hoheit des besagten Netzbetreibers unterliegen.

Externe Nutzer des VPNs müssen sich an die abzuschließende (s.o.) gegenseitige Vereinbarung zur Nutzung des VPNs halten; dies sollte tunlichst mindestens die Gewährleistung eines hinreichenden Sicherheitsniveaus in Fremdnetzen beinhalten, die per Site-to-Site-Kopplung an das eigene Netz angeschlossen werden.

Welche VPN-Mechanismen kommen sinnvoll in Frage?

Aktuell kommen zwei Varianten von VPN-Mechanismen grundsätzlich in Betracht:

- IPSec
- HTTPS (SSL)

Beide Ansätze weisen prinzipbedingt sowohl Vor- als auch Nachteile auf.

- IPSec bindet VPN-Clients und Remote-Sites transparent an die zentrale Site an, d.h. - soweit nicht Einschränkungen durch zusätzliche Filterelemente vorgenommen werden - jegliche IP-basierten Kommunikationsformen werden unterstützt. Allerdings ist der Einrichtungs- und Administrationsaufwand für ein IPSec-basiertes Client-to-Site-VPN infolge der speziellen Client-Software vergleichsweise hoch.

- HTTPS-basierte VPNs (so genannte SSL-VPNs) benötigen im Prinzip keinen speziellen Client, da sie aus einem handelsüblichen Browser heraus genutzt werden. Insofern ist ein Zugriff von jedem beliebigen System aus möglich und der operative Aufwand ist vergleichsweise gering. Allerdings sind bei diesem Einsatzszenario (Nutzung von beliebigen Systemen aus) die Kommunikationsmöglichkeiten teilweise eingeschränkt. Beispielsweise wird für den technisch auch hier grundsätzlich möglichen transparenten Netzzugriff in der Regel zur Laufzeit ein Applet auf den Client geladen, zu dessen Ausführung häufig erweiterte Benutzerrechte erforderlich sind. Außerdem führt der bei diesem Konzept technisch nicht zu verhindernde Zugriff von beliebigen Systemen aus zu einem deutlich erweiterten Risikopotenzial, das sinnvoll nur durch Beschränkung auf Terminalserver-basierte Kommunikation beherrschbar ist.

In Fällen, wo sowohl der transparente Netzzugriff von Managed PCs aus als auch der (eingeschränkte) Zugriff von Fremdsystemen aus anzubieten ist, sollte das Konzept eine Kombination beider Mechanismen vorsehen (s.o.). Dabei ist es jedoch nicht zwingend erforderlich, beide Verfahren auf der Basis eines einheitlichen Produkts zu realisieren; eine diesbezügliche Diversifikation würde im Gegenteil sogar automatisch eine Redundanz bieten und damit die Verfügbarkeit der Gesamtlösung erhöhen. Allerdings steigen dabei der administrative Aufwand und die Komplexität einer redundanten LAN-Anbindung.

Wie ist mit Authentifizierung und PKI umzugehen?

Eine möglichst zuverlässige Identifizierung des jeweiligen Kommunikationspartners ist bei VPN-Lösungen unabdingbar.

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Insofern sollte jedes Konzept an dieser Stelle besonderen Wert auf Einsatz als hinreichend sicher geltender Methoden zur Authentifizierung des jeweiligen Users bzw. Remote-VPN-Gateways legen.

Zur Authentifizierung von Anwendern, die von einem VPN-Client aus zugreifen, können grundsätzlich wahlweise Security-Token oder SmartCards eingesetzt werden. SmartCards kommen allerdings, wie schon dargelegt, nur dann sinnvoll in Betracht, wenn ein Zugriff von Fremdsystemen aus nicht vorgesehen ist. In entsprechend flexibel auszurichtenden Szenarien stellen daher die Security-Token nach wie vor die Methode der Wahl dar.

Die eigentliche Authentifizierung, d.h. die Überprüfung des vom Token gelieferten Passcodes auf Korrektheit, wird dabei von einem speziellen Server vorgenommen. Mit diesem Server kann das jeweilige VPN-Gateway (produktabhängig) wahlweise direkt oder über einen RADIUS-Server kommunizieren. Grundsätzlich bietet die RADIUS-basierte Variante Vorteile, da diese einen universellen Einsatz der Token-Lösung auch in anderen Bereichen grundsätzlich ermöglicht. Als RADIUS-Server kann dabei in Windows-dominierten Umgebungen prinzipiell auch ein Microsoft IAS fungieren; da in der Vergangenheit hier mitunter Kompatibilitätsprobleme auftraten, sollte dies bei Bedarf als Anforderungskriterium in einer Ausschreibung ausdrücklich formuliert werden. Über diesen Ansatz ist prinzipiell auch eine Einbindung in eine ActiveDirectory-Struktur, allerdings ist in jedem Fall derzeit noch eine separate Administration der Security Token auf dem Token-Server erforderlich (jedes Token muss in der Datenbank des Servers parametrisiert werden; derzeit ist dies nach Kenntnis des Autors über das AD nicht möglich).

Da für Remote-VPN-Gateways, d.h. bei Einsatz von Site-to-Site-Tunneln, eine Token-Lösung aus technischen Gründen in den allermeisten Fällen nicht eingesetzt werden kann (Ausnahme: Verwendung so genannter VPN Hardware Clients, z.B. Cisco VPN 3002), muss eine Ausweichlösung gefunden werden. Anders als bei der Authentifizierung von Anwendern kann hier - ohne erhöhtes Sicherheitsrisiko - die Verwendung zufällig generierter statischer Kennwörter ausreichender Länge (mindestens 12 Zeichen) vorgesehen werden. Schließlich muss sich bei diesem Szenario niemand diese Kennwörter merken, so dass die üblichen Gefahren der Kennwortpreisgabe nicht bestehen (sinnvoller Umgang mit der Thematik durch die jeweiligen Administratoren unterstellt...).

Wird auf eine Verwendung von SmartCards verzichtet, sind aufwändige PKI-Mechanismen nicht erforderlich. Aufgrund der technischen und insbesondere auch organisatorischen Komplexität einer sinnvollen PKI ist dies ein weiterer Vorteil der Token-basierten Lösung. Zur (zusätzlichen) Systemauthentifizierung bei IPSec sowie für den Aufbau der SSL-Kommunikationsbeziehung bei SSL-VPNs werden zwar u.U. Zertifikate benötigt, die jedoch typischerweise auf der Basis produktintegrierter Mechanismen erzeugt werden können. Demzufolge sollte das VPN-Konzept hier eine entsprechende Fähigkeit der jeweiligen Produkte vorsehen sowie optional eine Unterstützung der Windows-PKI (die Unterstützung weiterer Schnittstellen wäre in diesem Zusammenhang sicherlich wünschenswert).

Welche Schutzvorkehrungen sind bei bereichsübergreifender Kommunikation einzuplanen?

Erfolgt über die VPN-Lösung eine Kommunikation zwischen unterschiedlichen Verantwortungsbereichen, beispielsweise in Extranet-Szenarien, sind Vorkehrungen zum Schutz eigenen internen Netzes erforderlich. Hierzu wurden bereits geeignete Maßnahmen angesprochen und diskutiert:

- Beschränkung der zulässigen Kommunikation (weitestgehend vergleichbar einer Anbindung an das Internet)
- Vereinbarungen mit den jeweiligen Verantwortlichen des „fremden“ Verantwortungsbereichs

Gateway-Position, Architektur, Firewall-Integration

Da als Trägermedium für die VPN-Kommunikation das Internet genutzt wird, liegt grundsätzlich eine Positionierung des zentralen VPN-Gateways im Umfeld des in der Regel vorhandenen Internetzugangs nahe. Theoretisch kann das Gateway auch „weiter innen“ oder - im Fall größerer Netze mit mehreren per klassischer WAN-Technik verbundenen Standorten - sogar an einem

anderen Standort positioniert werden. Dabei sollte man jedoch bedenken, dass dies potenziell Umwege im Pakettransport nach sich ziehen könnte, die insbesondere hinsichtlich der meist teuren und daher typischerweise hinsichtlich der Bandbreitenauslegung eher knapp kalkulierten WAN-Leitungen zwischen den Standorten vermieden werden sollten.

Hinsichtlich der Integration der VPN-Lösung in eine vorhandene Firewall-Infrastruktur existieren zwei grundlegende strategische Ansätze:

- Integration des VPN in die vorhandene Struktur
Bei diesem Ansatz wird die VPN-Kommunikation grundsätzlich durch die Firewall(s) geschleust, wobei prinzipiell verschiedene Positionierungen des Gateways denkbar sind.
- Unabhängige Realisierung des VPN
Bei diesem Ansatz erfolgt eine Kopplung des VPN-Gateways an die vorhandene Firewall nur bei Bedarf.

In der Praxis hat sich der zweite Ansatz als der sinnvollere erwiesen - es sei denn, es existieren entsprechend anders lautende Vorgaben, etwa im Rahmen einer übergreifenden Security Policy.

Für das Konzept empfiehlt sich auf dieser Basis typischerweise eine direkte Verbindung des VPN-Gateways mit dem Internet (Abbildung 1). Die erforderliche Steuerung der zulässigen Kommunikation innerhalb des VPN erfolgt dabei durch das VPN-Gateway. Dieser Ansatz generiert zwangsläufig Anforderungen an die Funktionalität des Gateways:

- Eine (benutzerbezogene) Filterung des VPN-Datenverkehrs muss möglich sein
- Ausreichende Schutzfunktionen gegenüber dem Internet als Trägermedium müssen zur Verfügung stehen.

Gründe für diese Empfehlung sind vor allem die nachfolgend aufgeführten:

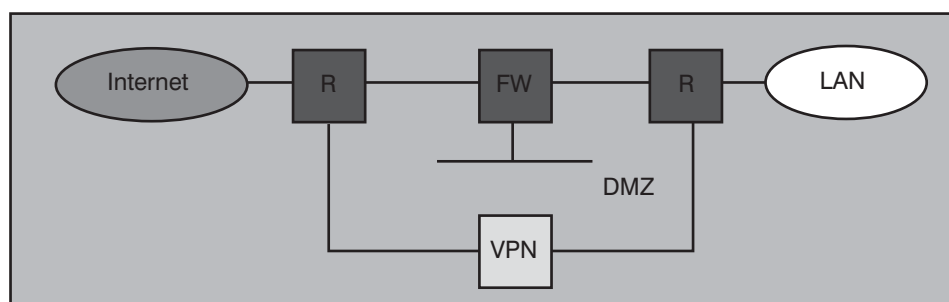


Abbildung 1: VPN-Realisierung ohne Einbindung der Firewall

RAS via VPN - Leitfaden anhand eines Projektbeispiels

- Eine Kommunikationskontrolle über eine vorhandene Internet-Firewall bedingt erhöhten Verwaltungsaufwand, da die zulässigen Kommunikationsformen benutzerabhängig zu steuern sein sollen; dazu sind aber ein entsprechendes Regelwerk und eine Korrelation zum VPN-Gateway bzw. RADIUS-Server notwendig, damit die Firewall aus dem Datenstrom den jeweiligen User ermitteln kann (z.B. über die genutzte Client-IP-Adresse). Alternativ käme eine (zusätzliche) Benutzerauthentifizierung an der Firewall in Betracht, die aber das Handling für den User erschwert und die Fehlerhäufigkeit und damit den Supportbedarf erhöht.
- Bei einem integrierten Ansatz beeinflusst die Verfügbarkeit der Firewall die des VPN; durch die Verkettung der Komponenten steigt die Fehlerwahrscheinlichkeit für das VPN an, insbesondere falls die Firewall nicht hochverfügbar ausgelegt ist.
- Der Ende-zu-Ende-Delay der über das VPN abgewickelten Kommunikationsbeziehungen steigt durch die zusätzliche Informationsverarbeitung in der Firewall an; dies kann sich auf diesbezüglich sensible Anwendungen nachteilig auswirken.
- Gleichzeitig ist der Sicherheitsgewinn einer solchen integrierten Architektur bestenfalls marginal - den Einsatz eines VPN-Gateways mit ausreichender Schutzfunktionalität vorausgesetzt. Grundsätzlich ist das Risikopotenzial

eines VPN-Gateways (sofern es keinerlei sonstigen Datenverkehr bedienen muss) deutlich geringer als das einer Firewall. Dies liegt daran, dass die zulässigen Pakete aus Sicht eines VPN-Gateways meist erheblich stärker - zumindest jedoch in gleichem Maße wie durch eine vorgeschaltete Firewall (Abbildung 2 zeigt eine beliebige Architekturvariante) - eingeschränkt werden können.

Für eine Lösung mit IPSec und SSL-VPN werden nur die Protokolle IKE (UDP500 und ggfs. UDP4500), HTTPS (TCP443) und ESP (IP50) benötigt; alle übrigen Datenpakete können prinzipiell verworfen werden. Hinzu kommt, dass zumindest bei IPSec weitere Mechanismen wie z.B. die Systemauthentifizierung zum Einsatz kommen, die den Missbrauch der zulässigen Protokolle durch Fremde bei sorgfältiger Konfiguration praktisch ausschließen.

Die zusätzliche Verwendung von Firewalls bei der Anbindung des VPN-Gateways ließe sich somit lediglich mit einer ggfs. notwendigen zentralen Steuerungsfunktion begründen - etwa wenn über eine solche Firewall die Kommunikation von ebenfalls auf dem Campus ansässigen Fremdfirmen von den eigenen Datenströmen getrennt werden muss. Aus Sicht der möglichst frühzeitigen Auskopplung derartiger mehr oder minder unkontrollierbarer Kommunikationsströme ist in solchen Fällen eine entsprechende Anbindung an die besagte Firewall sinnvoll (Abbildung 3). Die Steuerung des sonstigen VPN-Verkehrs hin-

gegen kann von einem geeigneten VPN-Gateway deutlich besser und mit weniger Administrationsaufwand wahrgenommen werden (s.o.).

Welche VPN-Komponenten werden benötigt?

Rein funktional kann ein VPN Gateway-seitig wahlweise auf Basis einer Appliance oder einer Software-Lösung realisiert werden. Erfahrungsgemäß neigen allerdings Appliances zu insgesamt stabileren Betriebsergebnissen und reduzieren in Summe den operativen Aufwand.

Client-seitig ist in den allermeisten Fällen eine Software-Lösung vorzusehen. Üblicherweise bietet der Hersteller des VPN-Gateways eine passende Client-Komponente mit an. Theoretisch kann auch ein alternativer Client eingesetzt werden; dies führt jedoch in der Praxis häufig zu technischen Schwierigkeiten und sollte daher nur in Verbindung mit ausgiebigen Tests erwogen werden. Hinzu kommt, dass proprietäre Zusatzmechanismen (z.B. in den Bereichen Benutzer-Authentifizierung, Client-Update, Client-Policy, etc.) in aller Regel nur auf Basis einer homogenen Lösung nutzbar sind.

Es sind auch so genannte Hardware-Clients am Markt verfügbar (s.o.); eine Festlegung auf einen solchen Ansatz würde jedoch die Produktauswahl stark einschränken. Zudem kommen solche Systeme aus Gründen der Praktikabilität nur sinnvoll bei stationären Clients in Betracht - es wäre dem Anwender sicher-

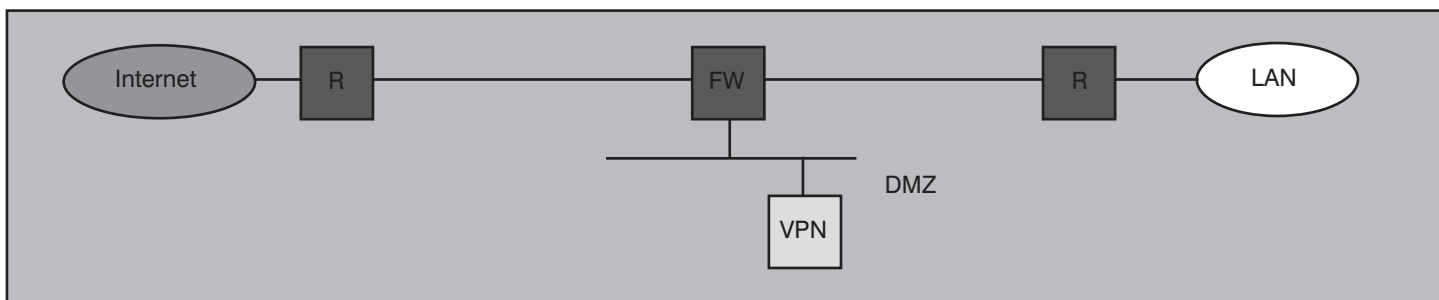


Abbildung 2: VPN-Realisierung mit vor- (und nach-)geschalteter Firewall

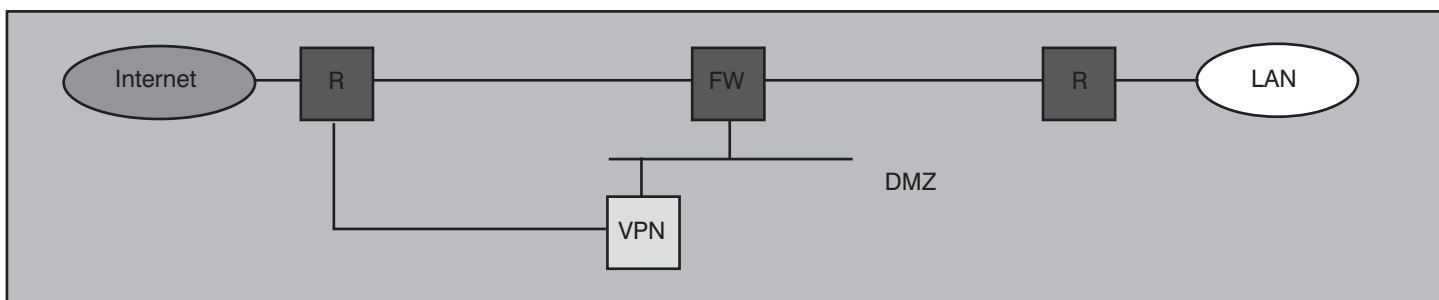


Abbildung 3: VPN-Realisierung mit Filterung der entschlüsselten Datenströme

RAS via VPN - Leitfaden anhand eines Projektbeispiels

lich kaum zu vermitteln, dass sein neues Notebook zwar erneut kleiner und leichter als das alte ausfallen wird, er jedoch zum Ausgleich ein weiteres Gerät inklusive Netzteil etc. zwecks VPN-Nutzung bei sich tragen muss...

Sollte bei der Auswahl einer Lösung die Entscheidung für einen Hersteller fallen, der derartige Hardware-Clients im Portfolio hat, könnten diese jedoch durchaus eine Alternative für die Realisierung von Site-to-Site-Kopplungen darstellen.

Auf die Anordnung der Komponenten wurde bereits eingegangen. Zur Authentifizierung sind zusätzlich weitere Komponenten, typischerweise ein RADIUS-Server und ein Token-Server vorgesehen. Diese können prinzipiell an beliebiger Stelle im internen Netz positioniert sein, wobei etwaige Empfehlungen der jeweiligen Hersteller zum Schutz dieser Server zu beachten sind; eine Positionierung in einem besonders geschützten Netzsegment ist unter Sicherheitsaspekten sicherlich zu bevorzugen.

Es ist von Vorteil, wenn das VPN-Gateway auf einer speziell gehärteten Firmware bzw. OS-Plattform basiert. Vor diesem Hintergrund ist Lösungen, die eine eigene geeignete Firmware bzw. OS bereits mitliefern, gegenüber Lösungen, die auf einer Standard-Plattform aufsetzen, der Vorzug zu geben.

VPN-Client-Software sollte über eine geeignete lokale Firewall-Funktionalität zum Schutz des Clientsystems gegen das VPN-Trägermedium verfügen. Als Mindestanforderung gilt eine Möglichkeit, einen so genannten „Split Tunnel“, d.h. die Möglichkeit gleichzeitig mit dem Internet und per VPN mit dem internen Netz zu kommunizieren, administrativ zu unterbinden. Alle Schutzfunktionen („Client-Policy“) sollten zentral administrierbar sein. Andernfalls ist ein nicht unerheblicher Pflegeaufwand, je nach Größe der Nutzerpopulation, zu kalkulieren. Bietet die Software zusätzlich eine Prüfung des Client-Status (etwa hinsichtlich des Release-Stands der VPN-Software oder des Virenschutzes, s.o.), so ist dies eindeutig positiv zu bewerten, da es die verbleibenden Restriktionen der VPN-Nutzung deutlich reduziert.

Welche grundlegenden Konfigurationsvorgaben sind zu machen?

Allgemein sollte die Regel „Sicherheit vor Funktionalität“ gelten. Das bedeutet, dass alle Komponenten des VPN so zu konfigurieren sind, dass ein als hinreichend betrachtetes Sicherheitsniveau erreicht wird - notfalls unter Verzicht auf bestimmte nicht

unbedingt notwendige Funktionalitäten. Diesem Grundsatz sollte das gesamte Konzept Rechnung tragen, als Beispiel wären hier die zuvor empfohlenen Beschränkungen bei SSL-VPNs zu nennen.

Über diese konzeptionellen Aspekte hinaus sind alle Systeme mindestens entsprechend dem im jeweiligen internen Netz etablierten Sicherheitsstandard zu konfigurieren; ggfs. kann eine Orientierung an den Vorgaben des Grundschutzkatalogs des BSI erfolgen. Zu den Standardmaßnahmen zählen hier:

- Beschränkung des administrativen Zugriffs auf das verantwortliche Personal
- Deaktivierung von Default-Konten; Einrichtung spezifischer Administratorkonten
- Verwendung hinreichend starker Kennwörter - alternativ kann eine zur Authentifizierung der VPN-Anwender eingesetzte Token-Lösung auch für die Administration der VPN-Komponenten verwendet werden.

Analog ist hinsichtlich der Backup- und Recovery-Thematik zu verfahren.

Wie können Redundanzen geschaffen werden?

Für VPNs sind verschiedene Redundanz-Mechanismen realisierbar. Ergibt sich auf Basis der Ist- und Anforderungsanalyse keine zwingende Notwendigkeit für eine automatisch aktiv werdende Redundanzlösung, so kann beispielsweise schon die Bevorratung eines zum primären zentra-

len VPN-Gateway identisch konfigurierten sekundären Gateways als prinzipiell ausreichend angesehen werden.

Soll das auszuwählende Produkt andererseits jedoch eine entsprechende Option aufweisen, empfiehlt sich - je nach konkreter Lösung - die Nutzung entsprechender Failover-Mechanismen, soweit diese ohne nennenswerten Mehraufwand realisierbar sind. Dies ist bei diversen Produkten der Fall.

Externe Lösungen (z.B. Load-Balancer) allein können in der Regel ein automatisiertes Failover oder gar eine Lastverteilung nicht bewerkstelligen (zumindest im Fall von IPSec-basierten VPNs). Insofern ist praktisch immer eine entsprechende Funktionalität innerhalb des VPN-Produkts vonnöten. Damit ergibt sich unmittelbar, dass Redundanz- bzw. Lastverteilungsmöglichkeiten stark produktabhängig sind - allgemeine konzeptionelle Vorgaben ohne Produktbezug sind daher kaum möglich.

Soll bzw. muss die Beschaffung der Lösung auf dem Ausschreibungswege erfolgen, so sind entsprechende funktionale Optionen produktneutral in die Leistungsbeschreibung aufzunehmen, damit die Produktauswahl entsprechende potenzielle Anforderungen berücksichtigen kann. Ähnliches gilt für die Authentifizierungslösung: auch hier sind die jeweiligen Möglichkeiten produktabhängig und sollten über entsprechende funktionale Anforderungen im Rahmen der Ausschreibung sichergestellt werden.

Seminar



Sicherheit 1: Kernbausteine einer erfolgreichen Sicherheits-Lösung 12.02. - 16.02.07 in Aachen

Dieses 5-Tages-Seminar identifiziert die herausragenden Gefahrenbereiche für Firewalls, Webserver, Clienten, Mailsysteme und Netzwerke und zeigt detailliert effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. An vielen typischen Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Inform. Andreas Meder, Sven Ossendorf
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

RAS via VPN - Leitfaden anhand eines Projektbeispiels

Was ist bei der Migration zu berücksichtigen?

Im Zuge der Migration auf die konzipierte VPN-Lösung sind folgende Aktivitäten notwendig:

- Inbetriebnahme der VPN-Lösung einschließlich aller flankierenden Systeme (z.B. Token-Server, Terminalserver für SSL-VPN, etc.)
- Festlegung der zukünftigen Nutzerkreise

Achtung: der Umstieg von klassischen RAS-Lösungen auf eine VPN-basierte Zugriffsform kann gewisse potenziell unerwünschte Nebenwirkungen mit sich bringen. So können beispielsweise bei einer Dial-In-basierenden RAS-Nutzung mit Hilfe des Callback-Verfahrens die Zugriffskosten zentral übernommen werden; diese Möglichkeit der Kostenübernahme ist bei einer VPN-gestützten Lösung nicht gegeben. Derartige Auswirkungen sind bei der Entscheidung, welche Nutzer migriert werden, ggfs. zu berücksichtigen.

- Erstellung von Prozessbeschreibungen für die mit der VPN-Lösung verbundenen administrativen Vorgänge (z.B.: Ausstellung Token, Anlegen VPN-Nutzer, etc.)
- Erstellung von Richtlinien für die Nutzer; dazu zählen insbesondere die notwendigen Aspekte von Vereinbarungen mit Fremdfirmen
- Erstellung eines Vorschlags für ein Rollen- und Berechtigungskonzept für die Nutzung des VPN
- Einrichtung der Nutzer und Nutzergruppen und ihrer Zugriffsrechte
- Installation der IPSec-Client-Software auf den Managed PCs und Vergabe der jeweiligen Security Tokens
- Bei Bedarf: Schulung der Anwender
- Bei Bedarf: Sukzessive Deaktivierung der Dial-In-Accounts bereits auf VPN migrierter Nutzer
- Planung und Einrichtung der Site-to-Site-VPN-Verbindungen (hierfür wird je Fall die Aufstellung eines gesonderten Migrationsplans empfohlen)
- Sukzessive Deaktivierung der Dial-In-Accounts bereits auf VPN migrierter Remote Sites
- Abbau aller vollständig abgelösten Di-

al-In-Lösungen nach Ablauf einer festzulegenden Übergangsfrist

Bei einigen der aufgezählten Aktivitäten kann es sinnvoll sein, diese als Leistung vom Lieferanten der VPN-Lösung einzufordern. Dies gilt insbesondere dann, wenn ein starker Produktbezug gegeben ist, etwa bei der Aufstellung der Prozessbeschreibungen.

Welche Vorgaben sind für Clients zu spezifizieren?

Die Vorgaben für die Ausstattung der VPN-Teilnehmer mit Sicherheitsfunktionalitäten hängen nicht zuletzt von der jeweiligen Sicherheitspolitik und dem darauf basierenden Sicherheitskonzept ab. Im Folgenden werden wir daher lediglich einige grundlegende empfehlenswerte Maßnahmen betrachten, die speziell bei Nutzung VPN-basierter Remote-Zugriffe zu berücksichtigen sind.

- Managed PCs

Managed PCs erhalten in jedem Fall zusätzlich zu ihrer Standard-Ausstattung eine Personal/Desktop Firewall-Funktionalität. Diese dient dem Schutz sowohl des Clients als auch des internen Netzes gegenüber dem Internet (u.a. durch Verhinderung so genannter Split Tunnels).

Idealerweise sollte diese Funktionalität Bestandteil der VPN-Client-Software sein. In diesem Fall wird keine zusätzliche Software benötigt, und es kann von einem optimalen Zusammenspiel von IPSec-Client und Desktop Firewall ausgegangen werden. Die meisten für den Enterprise-Einsatz ausgelegten Produkte bieten darüber hinaus ein zentrales Management der Policies dieser Firewalls. Auf diese Weise lässt sich eine einheitliche Sicherheitsstrategie besonders effizient umsetzen.

Der Einsatz von Intrusion Detection oder Sicherheitsagenten ist prinzipiell möglich, sollte aber nicht zuletzt aus Kostengründen nicht zur generellen Vorgabe gemacht werden. Bei hinreichend restriktiver, d.h. sicherer Firewall-Policy ist das Risiko eines netzbasierten Einbruchs als gering einzustufen. Sicherheitsagenten können erwogen werden, um einen adäquaten Sicherheitsstatus des Clients auch hinsichtlich installierter Software, eventuellen Virenbefalls, Aktualität des Virenschanners etc. sicherzustellen. Allerdings sind derartige Funktionen je nach Produkt teilweise bereits Bestandteil der VPN-Lösung.

Daher sollte hier eine Entscheidung frühestens nach Auswahl eines konkreten Produkts getroffen werden.

- Fremd-PCs im Rahmen von Site-to-Site-Zugriffen

Vorgaben für derartige Fremd-PCs können in der Regel nur in geringem Umfang gemacht werden.

Im Rahmen des Konzepts sollte jedoch, wie schon angesprochen, mindestens der Einsatz eines hinreichend aktuellen Virenschutzes verlangt werden. Darüber hinaus sollte im Rahmen gegenseitiger Vereinbarungen auf weitergehende Maßnahmen gedrungen werden, die zumindest einen akzeptablen Grundschutz der jeweiligen Client-Systeme gewährleisten.

- Fremd-PCs im Rahmen von SSL-VPN-Zugriffen

Da derartige Zugriffe von beliebigen Systemen aus technisch möglich und in der Regel auch gewollt sind (Stichwort: Flexibilität), sind hier keinerlei Vorgaben möglich. Das Konzept sollte dies durch die strikte Beschränkung derartiger Zugriffe auf per Terminalserver bereitgestellte Applikationen ohne Möglichkeit zum Datentransfer berücksichtigen.

Es existieren auch SSL-VPN-Lösungen, die eine Remote-Überprüfung des jeweiligen Clients durch das Gateway ermöglichen sollen. Der ggfs. eingeschränkte Zugriff wird dabei vom Ergebnis dieser Überprüfung abhängig gemacht. Hier waren die Produkte aber nach Ansicht des Autors in der jüngeren Vergangenheit noch nicht so ausgereift, dass man diese Strategie grundsätzlich empfehlen könnte. Je nach Funktionalität des ins Auge gefassten konkreten Produkts kann dies im Einzelfall jedoch eine Alternative darstellen; bei erfolgreichem Verlauf entsprechender Tests kann in solchen Fällen von der Beschränkung auf Terminalserver eventuell abgesehen werden.

Welche organisatorischen Maßnahmen sind zur Einführung des VPN nötig?

Da durch Umstieg auf VPN-Technologie - sorgfältige Planung und Umsetzung unterstellt - keine zusätzlichen Gefahrenpotenziale gegenüber klassischen Lösungen (Dial-In) entstehen, sind im Grunde keine weiter gehenden organisatorischen Maßnahmen vonnöten. Dabei wird unterstellt, dass eine vorhandene Dial-In-Lösung die-

RAS via VPN - Leitfaden anhand eines Projektbeispiels

sen Gefahrenpotenzialen bereits durch entsprechende technische Maßnahmen begegnet.

Ist dies nicht der Fall oder sieht das Konzept die Einführung zusätzlicher - bisher nicht vorhandener - Schutzmechanismen vor, so sind für deren sinnvollen und effizienten Einsatz die notwendigen organisatorischen Strukturen zu schaffen.

Dies betrifft häufig vor allem den Einsatz von Security Token zur starken Authentifizierung, da viele bestehende Dial-Szenarien auf Basis herkömmlicher Kennwort-Authentifizierung realisiert wurden. Neben der Benennung des verantwortlichen Systemadministrators bedarf es hier vor allem der Etablierung eines Verfahrens zur Beantragung, ggfs. Generierung und Zuteilung der Token und der benutzerbezogenen, geheimen PIN.

Von der Theorie zur Praxis: Ein beispielhaftes Projekt

Im Folgenden soll kurz ein reales Projekt beispielhaft dargestellt werden, das auf Basis der vorstehenden grundsätzlichen konzeptionellen Überlegungen und Empfehlungen realisiert wurde.

Ausgangslage war ein MAN basiertes Netz, das unterschiedliche technische Lösungen (u.a. Internet-basierte VPNs sowie verschiedene Dial-In- und Dial-Out-Konstrukte) für den Remote-Zugriff auf interne Ressourcen bzw. den Zugriff aus dem Intranet auf externe Ressourcen nutzte. Diese Vielfalt sollte im Sinne einer weitgehenden Harmonisierung durch eine möglichst einheitliche Lösung auf VPN-Basis abgelöst werden. Insofern musste die zu schaffende Lösung sowohl hinreichend flexibel sein als auch geeignete Skalierungsoptionen bieten. Dabei wurde die Lösung so gestaltet, dass sie unter Abwägung von Sicherheitsanforderungen, Praktikabilität und Kostenaspekten weitgehend optimal ist. Insbesondere die beiden letzten Aspekte bedingten wie so oft auch in diesem Fall punktuell Kompromisse hinsichtlich der Sicherheitsmaßnahmen; die gefundene Lösung konnte aber auf der Basis von „Best Current Practice“-Lösungen sicherstellen, dass das zu tragende Restrisiko überschaubar und insbesondere deutlich geringer war als auf Basis des Status Quo.

Als technischer Lösungsansatz für das VPN wurde der Einsatz dedizierter VPN-Appliances als VPN-Gateways vorgesehen, die sowohl Clients als auch Remote-Standorte über einen stark verschlüsselten VPN-Tunnel an das interne Netz anbinden können.

Für den Aufbau der VPN-Tunnel wurden die beiden Standard-Mechanismen

- IPSec
- SSL (HTTPS)

vorgesehen, um eine möglichst breite Palette von remote-Systemen unterstützen zu können. Aus Gründen der einheitlichen Administration und der einfacheren Architektur wurden dabei Lösungen bevorzugt, die beide Techniken innerhalb einer gemeinsamen Plattform anbieten.

Da bei SSL-VPNs im Allgemeinen von einem sehr hohen Gefährdungspotenzial durch den zugreifenden Client ausgegangen werden muss, wurde bei dieser Zugriffsform die Kommunikation auf die Nutzung von Applikationen auf Terminalserver-Basis beschränkt. Insbesondere wurde jeglicher Dateitransfer zwischen Client und internem Netz unterbunden – eine Funktionalität, die mit Blick auf die geforderte Flexibilität der Lösung dennoch durch die Implementierung nicht grundsätzlich ausgeschlossen wird.

IPSec-Clients und Clients aus Remote-Sites greifen über transparenten IPSec-Tunnel auf das interne Netz zu. Innerhalb dieses Tunnels wird die zulässige Kommunikation durch Einsatz von Firewall-Technik gesteuert. Diese Steuerung wird insbesondere zur Trennung der unterschiedlichen Nutzerkreise

- Eigene Mitarbeiter,
- Wartungsfirmen bzw. Kunden sowie

- Ingenieurbüros, die an der Neugestaltung der Liegenschaften arbeiten,

eingesetzt.

Das Konzept sah nicht zwingend eine hochverfügbare Ausrichtung der Lösung vor, da seitens des Auftraggebers ein Cold-Standby-Ansatz als ausreichend angesehen wurde. Soweit jedoch im Rahmen der Realisierung Produkte zum Einsatz kämen, die ohne Mehrkosten mindestens einen Hot-Standby realisieren könnten, sollte diese Option auch genutzt werden.

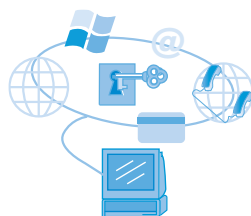
Im Folgenden wird daher der Begriff „VPN-Gateway“ synonym sowohl für ein einzelnes System als auch für ein entsprechendes Cluster gebraucht.

Über ein solches Cluster ließ sich auch - wiederum produktabhängig - eine Skalierung der Lösung durch Hinzunahme weiterer Gateways mit Lastverteilung erreichen.

Aus architektonischer Sicht war vorgesehen, das VPN-Gateway in die bestehende Firewall-Architektur am zentralen Standort zu integrieren. Dazu wurde sein externes Interface mit einem internen Interface der äußeren Firewall und sein internes Interface mit dem externen Interface der inneren Firewall verbunden (Abbildung 4).

Durch diese Architektur wird das VPN-Gateway gegenüber dem Internet durch die vorhandene Firewalltechnik geschützt.

Kongress



ComConsult IT-Sicherheits-Forum 2007 07. - 10.05.07 in Königswinter

Das IT-Sicherheits-Forum 2007 hat sich in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt. An insgesamt vier Tagen wird mit einführenden Tutorien, technischen Workshops und Fachvorträgen zu aktuellen und zukünftigen Entwicklungen für jeden Interessierten etwas geboten. Dabei wird äußerst hoher Wert auf Praxisnähe gelegt, die Teilnehmer sollen die gewonnenen Erkenntnisse möglichst sofort in der eigenen Umgebung anwenden können.

Fachliche Leitung: Dipl.-Inform. Detlef Weidenhammer
Preis: € 1.990,-* zzgl. MwSt. mit Tutorium am ersten Tag
€ 1.590,-* zzgl. MwSt. ohne Tutorium am ersten Tag
* gültig bis 15.02.07



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

RAS via VPN - Leitfaden anhand eines Projektbeispiels

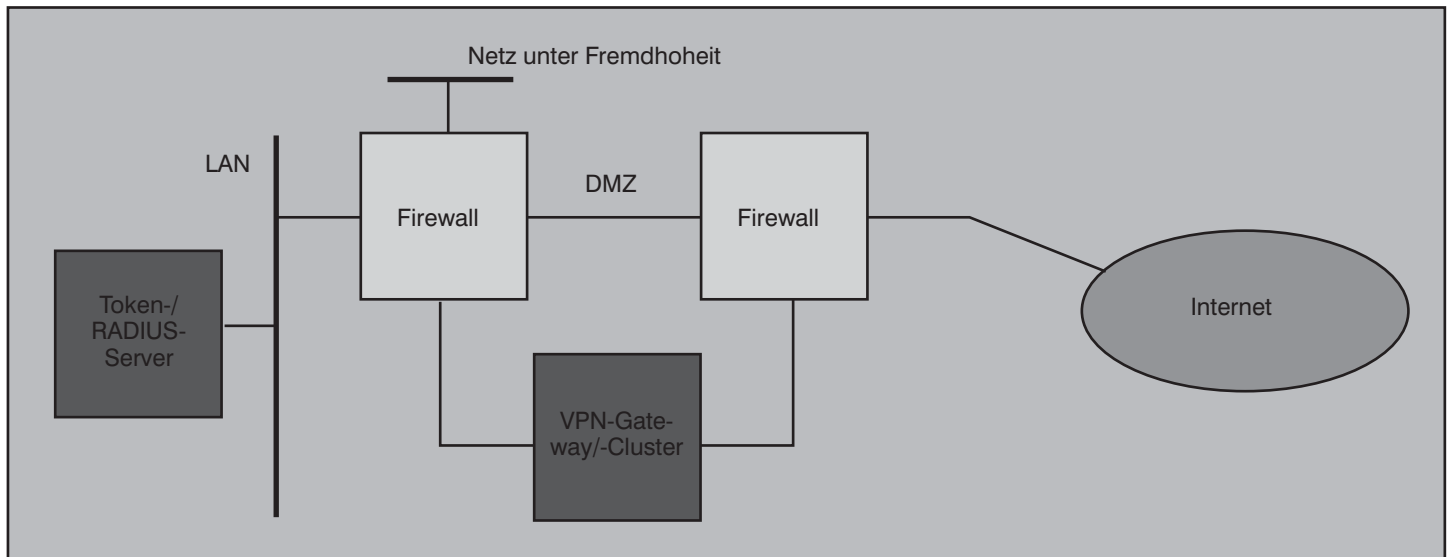


Abbildung 4: VPN-Architektur; Integration in Firewall-Architektur

Es ist jedoch eine direkte Verbindung des VPN-Gateways mit dem Internet nicht zwingend ausgeschlossen; eine derartige Architektur könnte zu einem späteren Zeitpunkt problemlos realisiert werden (Abbildung 5). Gleichzeitig erlaubt die Architektur eine Auskopplung jenes VPN-internen Datenverkehrs, der für - über die interne Firewall angebundene - Netze unter Fremdhoheit bestimmt ist. Eine weitergehende Filterung des VPN-Verkehrs durch die interne Firewall wurde nicht vorgesehen; diese erfolgt durch das VPN-Gateway.

Das Gateway musste zur sicheren Realisierung dieses Ansatzes mindestens folgende Eigenschaften aufweisen:

- Ausreichender Eigenschutz (durch Paketfilter o.ä.) gegen Gefahren aus dem

- Internet
 - Benutzerbezogene Filterung des VPN-Datenstroms zur Steuerung der VPN-internen Kommunikation

Die Authentifizierung der Remote-User ist, wie schon angesprochen, eine der wesentlichsten Aufgaben einer sicheren RAS-Lösung - unabhängig davon, ob per Dial-In oder per VPN. Demzufolge wurde hier mit dem Einsatz einer Token-basierten Zwei-Faktoren-Authentifizierung eine besonders sichere Lösung konzipiert.

Aus Gründen der Flexibilität sollte die Anbindung dieser Authentifizierungslösung an das VPN-Gateway über einen vorgeschalteten RADIUS-Server erfolgen (der allerdings in aller Regel auf demselben System wie der Token-Server arbeitet).

Dieser sollte gleichzeitig auch die Authentifizierung der Remote-Sites übernehmen, die typischerweise nur über Passwörter erfolgen kann; allerdings können diese so lang und komplex gewählt werden, dass hierdurch kein Sicherheitsrisiko entsteht.

Zusätzlich zur Authentifizierung der Nutzer erfolgt eine Identifizierung der Clients interner Mitarbeiter, z.B. zertifikatsbasiert.

Die Verwaltung der Benutzer ist aus technischer Sicht bei dem vorgelegten Konzept eine Verwaltung der Security-Token: je ein Token ist je einem Benutzer fest zugeordnet, und aus Sicht des VPN sind der Benutzer und sein Token identisch. Die Verwaltung der so definierten „Benutzer“ erfolgt damit zwangsläufig durch den Token-Server in einer speziellen Datenbank.

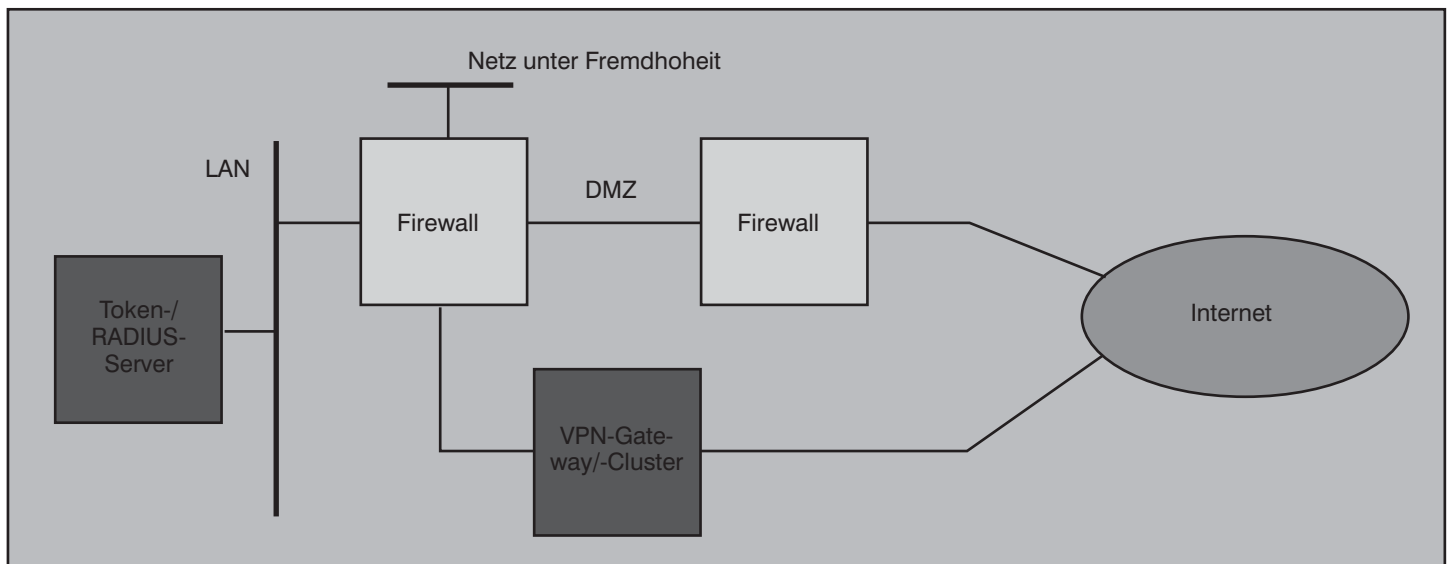


Abbildung 5: VPN-Architektur; unabhängig von Firewall-Architektur