VPN im heterogenen Netz

Anwenderbericht aus der Max-Planck-Gesellschaft

Angesichts eines stark heterogenen und verteilt administrierten Netzwerks hat sich die Max-Planck-Gesellschaft bei der Einrichtung ihres VPN für eine unabhängige Verschlüsselungslösung per Hardware entschieden.

Von Tim Fickert, Gerd Richter und Rainer W. Gerling, München

Die Max-Planck-Gesellschaft hat circa 80 Institute und Einrichtungen, die alle mehr oder weniger direkt am Deutschen Forschungsnetz (DFN) angeschlossen sind. Im Zusammenhang mit der Einführung von Standard-Anwendungen im Verwaltungsbereich (SAP R/3) ergab sich die Notwendigkeit des Aufbaus eines verschlüsselten Virtual Private Networks (VPN), um sensitive Daten vor unberechtigter Kenntnisnahme bei der Übertragung im öffentlichen Netz zu schützen.

Eine besondere Herausforderung dabei war die extreme Heterogenität der Netz-Infrastruktur. In den Instituten sind nicht nur Router unterschiedlicher Hersteller, sondern auch sehr unterschiedliche Firewalls installiert (Cisco PIX, Firewall 1, IP-Tables usw.). Da etliche Max-Planck-Institute an den Netzwerk-Infrastrukturen des Campus, auf dem sie sich befinden, partizipieren, ist nicht einmal sichergestellt, dass überhaupt ein administrativer Zugriff auf die Router- und Firewall-Konfiguration besteht. Es war deshalb unmöglich, die konkrete Umgebung im Zusammenspiel mit dem VPN vorab auszutesten.

Um Performance-, Konfigurations- und Kompatibilitätsprobleme auszuschließen, fiel die Entscheidung früh auf separate Verschlüsselungsboxen, die jeweils vor den zu schützenden Netzwerksegmenten eingebaut werden sollten. Auf die Installation von Verschlüsselungs-Clients auf den Arbeitsplatzrechnern (bei Einführung Microsoft Windows NT 4, heute Windows XP) wurde verzichtet, da auf allen Maschinen das Echtzeit-Dateiverschlüsslungssystem Utimaco LanCrypt eingesetzt wird. Da das VPN für alle Institute zentral gemanagt und überwacht werden sollte, war zudem eine einfache zentrale Konfigurations- und Administrationsfunktion gefordert.

Bild 1: Die Max-Planck-Gesellschaft nutzt für ihr VPN CryptoGuard VPN 3000 (Bild: unten im 19"-Rack); zum Entscheidungszeitpunkt von Utimaco vertrieben, werden die Boxen heute von Compumatica weiterentwickelt.

Krypto-Hardware

Nachdem eine erste Vorentscheidung aus Preis-/Leistungsgründen für die CryptoGuard-VPN-3000-Boxen gefallen war, wurde zunächst eine Testinstallation in drei Einrichtungen im Raum München eingerichtet. Installation und Testbetrieb verliefen unproblematisch und ohne Ausfälle. Die genutzten Boxen wurden ursprünglich von der KryptoKom GmbH entwickelt, liefen zum Entscheidungszeitpunkt im Vertrieb der Utimaco Safeware AG und werden mittlerweile von der Compumatica secure networks GmbH hergestellt (www.compumatica.de). Bild 1 zeigt die ursprüngliche Box im eingebauten Zustand; neue Modelle sind zudem nur noch eine Höheneinheit (HE) hoch.

Da diese Boxen auch im Informationsverbund Bonn-Berlin zum Einsatz kommen, sind sie vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im Jahr 2002 sorgfältig evaluiert und in der Version 2.2.20 mit E3/hoch zertifiziert (BSI-DSZ-ITSEC-0106-2002, vgl. www.bsi.bund.de/zertifiz/zert/reporte/0106.pdf); die zertifizierte Version war jedoch noch DOS-basiert.

Die aktuellen Kryptoboxen verwenden als Betriebssystem ein gehärtetes FreeBSD mit dem Paketfilter Drawbridge (www.net.tamu.edu/drawbridge/). Für den – neben einem proprietären CryptoGuard VPN Mode (s. u.) – ebenfalls möglichen IPsec-Betrieb dient das SSH IPSEC Express Toolkit der Firma SSH Communications Security (www.ssh.com/products/developer/ipsec_express/); derzeit arbeitet Compumatica am Einsatz eines alternativen IPsec-Protokoll-Stacks.

Die verwendeten Schlüssel kapseln die Boxen unauslesbar in einem Hardware-Sicherheitsmodul, das auch

zur Verschlüsselung verwendet wird. Der proprietäre CryptoGuard-(CG-)VPN-Modus nutzt hierzu ADES mit 112 Bit Schlüssellänge. Ursprünglich wurde das Kryptoboard mit zwei CE Infosys SuperCrypt Chips realisiert (www.ceinfosys.com.sg/technologies/SuperCrypt1.htm), die durch Teilparallelisierung einen Verschlüsselungsdurchsatz von 20 MByte/s erreichen; mittlerweile wird zur Hardwarebeschleunigung das Compumatica CryptOn1 Board eingesetzt.

Die Schlüsselgenerierung geschieht auf der zentralen CryptoGuard Security Management (CGCM) – vormals: Security Management Station (SMS). Die Personalisierung der Boxen und das Laden der Preshared Keys sind dabei ausschließlich über ein serielles Kabel möglich. Hierzu muss die Box zum zentralen CGCM-Arbeitsplatz gebracht werden. Nach der Personalisierung lässt sich die Box jedoch auch über das Netz administrieren.

IPsec? Nein, danke!

Beim Betriebsmodus fiel die Entscheidung gegen IPsec und für den CGVPN-Modus. Der Verschlüsselungsmodus wurde so konfiguriert, dass die Maschinen nur den eigentlichen Datenteil eines Datagramms verschlüsseln. IP- und TCP/UDP-Header verbleiben im Klartext. Damit war es nicht erforderlich Firewall-Regelwerke anzupassen, da die Header nach wie vor sichtbar sind.

Die Kryptoboxen benötigen zwar eine IP-Adresse zur Administration; im Netzverkehr verhalten sie sich jedoch ansonsten wie eine Bridge, sodass keine Umkonfiguration existierender Netzwerkkomponenten erforderlich war. IPsec-Gateways benötigen hingegen eine eigene IP-Adresse, da sie als Router arbeiten, und verlangen daher eventuell eine Umkonfiguration des Netzes.

Auch die Geschwindigkeit der Boxen hat bei der Auwahl des Verfahrens eine Rolle gespielt: Der proprietäre CGVPN-Modus arbeitet deutlich schneller als der IPsec-Modus. Der Hersteller gibt folgende Durchsatzraten an: unverschlüsselt 31–94 Mbit/s, verschlüsselt 25–99 Mbit/s. In der Praxis zeigt sich eine für Verwaltungsanwendungen ausreichende Performance.

In der Konfiguration mit rund 80 Boxen finden zudem häufige Schlüsselwechsel statt, da für jede Verbindung zwischen zwei Boxen ein separater Verbindungsschlüssel verwendet wird. Die Krypto-Hardwaremodule haben jedoch nur einen begrenzten Speicherplatz für Schlüssel, sodass sie Schlüssel öfter neu laden müssen.

Konfigurationskonzept

Die Authentifizierung der Boxen gegenüber der CGCM-Workstation basiert auf Preshared Keys. Jede Box hat einen Masterkey zur Kommunikation mit der Konfigurations-Workstation (vgl. [2]); diese Schlüssel werden im CGCM generiert und über eine serielle Verbindung zur Kryptobox übertragen. Nach dieser Personalisierung ist ein Remote-Management über das Netz möglich.

Die Verwaltung des Netzes basiert auf Netzwerkobjekten, die über definierte Verbindungen miteinander kommunizieren. Hierzu sind diese Netzwerkobjekte – sowohl einzelne Rechner als auch Subnetze – zunächst zu definieren. Anschließend erstellt man Verbindungen ähnlich einem Satz von Paketfilterregeln. Sie regeln im Detail, welche Kommunikation erlaubt ist. Hier bietet es sich zuerst einmal an, eine verschlüsselte Verbindung festzulegen: Für den Anfang könnte man verschlüsselt alle Protokolle erlauben. Es wäre aber auch denkbar, ein „verschlüsseltes SAP"-Kommunikations-Profil anzulegen; dann wäre über diese Verbindung ausschließlich eine SAP-Sitzung möglich.

Auch für die unverschlüsselte Kommunikation wird festgelegt, welche Protokolle und Dienste über eine Verbindung laufen. Gibt es sehr viele unterschiedliche Kommunikationsarten, so müssen entsprechend viele Verbindungen definiert werden. Dabei ist zu berücksichtigen, dass zwischen zwei Objekten nur jeweils eine Verbindung möglich ist.

Der letzte Konfigurationsschritt ist der Aufbau der Netzwerktopologie mit dem Topology Editor, einem leicht zu bedienenden grafischen Editor, mit dem man festlegt, wie Kryptoboxen und Netzwerkobjekte angeordnet sind. Ist dieser Schritt vollzogen, können abschließend die Konfigurationsregeln für die einzelnen Boxen generiert und verteilt werden. Dies wird manuell angestoßen, funktioniert aber automatisch. Ist eine erste Konfiguration erfolgt, modifiziert das Managementsystem bei Änderungen nur das Regelwerk der jeweils betroffenen Boxen.

Rollout

Die Boxen sind im frisch personalisierten Modus so geschaltet, dass sie allen Datenverkehr unverschlüsselt durchlassen. Obwohl sie mit einer IP-Adresse personalisiert werden, ist diese nur für das Management von der CGCM-Station erforderlich, die eine Verbindung über Port 57/UDP zur Box nutzt – die Box wiederum baut Verbindungen zu Port 87/UDP zum CGCM auf.

Ansonsten verhalten sich die Krypto-Boxen wie eine Bridge. Der Einbau geschieht durch Einschleifen in das Netzwerkkabel vor dem Gateway des entsprechenden Netzwerksegments. Hierzu ist keine Änderung der Konfiguration dahinter liegender Rechner notwendig. Erst wenn alle Boxen eingebaut sind, werden zentral vom CGCM die Verschlüsselungs- und Paketfilterregeln akti-

Literatur

[1] Tim Fickert, Gerd Richter und R.W. Gerling, VPN: auch ohne IPsec!, Folien zum Vortrag auf dem 10. DFN-Workshop, www.dfncert.de/events/ws/2003/dfncertws2003-f7.pdf

[2] Compumatica Aachen, Whitepaper „Security Management Station“, www.compumatica.de/products/WP_SMS_02_03.pdf

viert. Dadurch ist es möglich in aller Ruhe die Boxen zu installieren, ohne dass es zu Netzunterbrechungen kommt (außer während des Umsteckens der Kabel).

Beim Rollout kam es zu diversen, aber nur kleineren Problemen. Hierzu zählten neben vertauschten Kabeln (die beiden Netzwerkanschlüsse der Boxen, mit Plain und Cypher bezeichnet, sind nicht equivalent) auch fehlende Freischaltungen in den Firewalls für die Management-Verbindungen – da die Firewalls der Max-Planck-Institute, wie bereits angesprochen, dezentral administriert werden, war eine entsprechende Abstimmung erforderlich.

Aktuelle kleine HUBs oder Switches für den SOHO-Bereich mit Autosensing für gekreuzte RJ-45-Kabel (Auto MDI/MDI-X) machten zudem in Einzelfällen Probleme im Zusammenspiel mit dem 10/100-MBit-Autosensing der Boxen. Sie wurden an einigen Stellen als Konverter von der damals noch teilweise vorhandenen BNC-Verkabelung auf die RJ-45 Buchsen der Kryptoboxen eingesetzt. Ein Wechsel auf weniger „intelligente“ HUBs und Switches löste das Problem jedoch.

Betriebsprobleme

Im Betrieb sind einige kleinere Schwierigkeiten aufgetreten. Hervorzuheben ist lediglich ein Problem, das sich durch Verbindungsabbrüche, jeweils nach einer kurzen Zeit, äußerte. Um die Header der Datagramme nicht ändern zu müssen, wird kein Padding vor dem Verschlüsseln durchgeführt. Wenn der letzte Datenblock weniger als acht Bytes enthält, erfährt er daher eine Sonderbehandlung unter Verwendung des verschlüsselten vorhergehenden Blocks: Hierzu wird der bereits verschlüsselte vorletzte Block ein weiteres Mal verschlüsselt, und dieses Ergebnis mit dem Klartext des „unvollständigen“ letzten Blocks XOR-verknüpft. Besteht das gesamte Datagramm insgesamt nur aus maximal sieben Bytes Payload (d. h. es gibt keinen vorhergehenden Block), so wird ersatzweise Information aus dem Header verschlüsselt (vor allem die Sequenz-Nummer), um den Schlüssel für die XOR-Operation zu erhalten.

Im so genannten NAT-Modus ändern jedoch Cisco PIX Firewalls als Sicherheitsfeature diese Sequence-Nummer, sodass man ein derart kleines Paket nicht mehr entschlüsseln kann. Im Mittel dauert es etwa zehn bis zwanzig Minuten, bis eine Verbindung (z. B. eine SAP-Sitzung) durch das Auftreten solcher kleiner Pakete abbricht.

Um nicht von der Konfiguration der Firewalls abhängig zu sein, wurde mittlerweile die Firmware geändert (genauer: das Verschlüsselungsprotokoll). Hierbei zeigte sich, dass es auch im Alltagsbetrieb problemlos möglich ist, über das zentrale Management eine neue Firmware auch auf eine größere Anzahl von Boxen einzuspielen.

Ausblick

Eine zusätzliche Schwierigkeit hat sich im Falle einer lediglich logischen Trennung von Wissenschafts- und Verwaltungsnetz mittels VLANs gezeigt: Dabei ist es deutlich schwieriger einen geeigneten Aufstellungspunkt „vor dem Verwaltungsnetzsegment“ zu finden.

Als Fazit lässt sich festhalten, dass der Rollout der 80 Boxen erstaunlich unkompliziert war. Die Heterogenität der Netzstrukturen erschwerte zwar ein vorbereitendes ausführliches Testen. Die Boxen laufen aber seit rund zweieinhalb Jahren ohne nennenswerte Störungen und sind performant.

Eine gewisse Einschränkung stellt das 10/100-MBit-RJ45-Netzwerk-Interface dar: Für Gigabit-Ethernet muss man bei den im Einsatz befindlichen Boxen mit Protokollkonvertern eine Anpassung vornehmen. Mittlerweile sind jedoch vom Hersteller auch Varianten mit Gigabit-Interface verfügbar. ■

Tim Fickert und Gerd Richter sind Mitarbeiter der Sicherheitsadministration bei der Max-Planck-Gesellschaft, Rainer W. Gerling ist Datenschutzbeauftragter der Max-Planck-Gesellschaft (www.mpg.de).