VPN-Performance

Aktuelle Lösungen virtueller privater Netze im Leistungstest

Kai-Oliver Detken

Der Standard IPsec stellt heute die Grundlage für den einheitlichen Aufbau von Extranets dar. Eine ganze Reihe von Herstellern implementiert inzwischen IPsec, so daß die Anwender nicht mehr auf proprietäre Lösungen angewiesen sind. Allerdings ergeben sich durchaus noch Probleme in der Interoperabilität, da die Spezifikationen mitunter unterschiedlich interpretiert werden bzw. IPsec auf unterschiedlichen Layern (oberhalb, unterhalb und innerhalb der IP-Schicht) implementiert wird sowie etwaige proprietäre Funktionen der Hersteller hinzukommen.

Kai-Oliver Detken ist Senior IT-Consultant der DECOIT sowie freier Autor und Berater in Grasberg/Bremen

Die Gründe für die noch vorhandenen Probleme mit dem Standard IPsec liegen darin, daß IPsec noch eine sehr junge Spezifikation ist. IPsec-Tunnel werden durch zwei Endpunkte bzw. Subnetze definiert.
Es müssen aber auch zusätzliche Angaben wie Festlegung der Algorithmen für Authentifizierung und Verschlüsselung festgelegt werden. Manche Hersteller haben dabei eigene Datenkompression in die Softwarelösung integriert, wodurch es zu Problemen beim Einrichten der Tunnel kommen kann.

Beeinträchtigungen der Performance

Die Performance im eigenen Intranet wird nicht ausschließlich von den Sicherheitsmechanismen von IPsec beeinträchtigt. Das liegt daran, daß diese nur am Netzrand in der Firewall oder dem Router angewendet werden.
Allerdings kommt es natürlich zu Einschränkungen zwischen den Teilnehmern eines Extranet. Das liegt u.a. an dem deutlichen Overhead durch Verschlüsselung und Authentisierung der IP-Pakete. Es ist daher immer wichtig, einen Performance-Test durchzuführen, wenn man ein Extranet oder VPN aufbauen möchte. Ansonsten könnte man unliebsame Überraschungen erleben, wie beispielsweise einen schlechten Datendurchsatz.
Kryptographische Algorithmen, die auf Hardware implementiert werden, können die Performance erheblich steigern. Hier muß letztendlich zwischen Kosten/Nutzen bzw. Leistung/Sicherheit entschieden werden. Wenn man eine höhere Sicherheit, sprich Verschlüsselung, erhalten will, sind Einschränkungen in der Performance hinzunehmen [1].
Bei IPsec wird zwischen Tunnel- und Transportmodus unterschieden. Der Transportmodus schützt dabei vorrangig höhere Schichtenprotokolle, was für den Einsatz von End-to-end-Kommunikation zwischen zwei Segmenten spricht.
Dem Einsatz des Tunnelmodus wird allerdings momentan eine höhere Bedeutung zukommen, da hier unabhängig von der Infrastruktur eine Punkt-zu-Punkt-Verbindung aufgebaut werden kann.
Um eine Nichtleugbarkeit auszuschließen, sind AH- Algorithmen (Authentication Header) oder ESP-Algorithmen (Encapsulating Security Payload) wie Triple-DES oder Blowfish zu verwenden. IPsec bietet ebenfalls nach RFC-2401 Schutz gegen Replay-Attacken, was in der Vorgängerversion nicht möglich war. Das heißt, ein altes Paket, welches in den Datenstrom wieder eingebracht wird, kann aufgrund der Sequenznummern nicht mehr als gültig erkannt werden und wird abgewiesen.
Um eine höchstmögliche Sicherheit bezüglich der eingesetzten Anwendungen erhalten zu können, müssen AH und ESP eingesetzt werden. Allerdings ist auch eine Authentisierung mittels ESP möglich, wodurch er auch ohne AH verwendet werden kann.

Das Thema in Kürze

Die Performance in Internet, Intranet oder Extranet bei Anwendung von Verschlüsselungen und Authentifizierung ist kein Produktproblem, sondern begründet in den abzuarbeitenden Algorithmen. Zu diesem Schluß kommt der Autor, der das Übertragungsverhalten unter verschiedenen Test-Bedingungen untersuchte, wobei insbesondere die VPN-Lösung von NCP und die Firewall-1 von Sun berücksichtigt wurden.

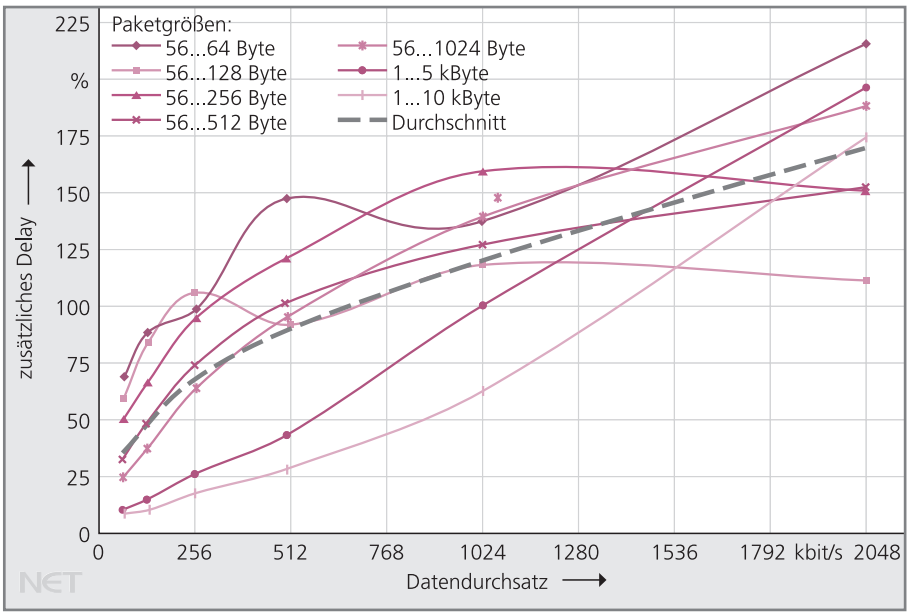

Bild 1: Zusätzliche Verzögerung durch IPsec-Verschlüsselung

Router-Performance bei IPsec

Eine Router-Messung wurde mit den Cisco-Routern 2600 und 3600 durchgeführt, um die Performance-Verluste herauszufinden.
Als vorteilhaft erwiesen sich dabei das Erkennen der Quelle, des Empfängers oder der Daten aus dem gesamten Datenstrom, weil die IP-Pakete gekapselt werden und die neuen IP-Pakete nur noch Source und Destination des IPsec-Knotens enthalten. Ebenfalls war ein bestimmter Sicherheitsgrad von einem Netzwerk zum anderen aufzubauen und aufrechtzuerhalten. Dabei konnte unabhängig von der Anwendung eine Verschlüsselung vorgenommen werden.
Das Einrichten eines neuen IPsec-Tunnels erzeugt weiterhin keine Verzögerungszeiten, da der neue Tunnel bereits aufgebaut wird, wenn die Lebenszeit des alten Tunnels abgelaufen ist. Aus Sicherheitsgründen muß der Tunnel in bestimmten Zeitintervallen gewechselt werden.
Nachteilig wirkte sich allerdings der erhebliche Performance-Verlust aus, der durch die Router-Verschlüsselung verursacht wurde. Obwohl im Back-to-back-Betrieb getestet wurde, lag der Leistungsverlust bei einer FTP-Anwendung bis 500 kbit/s bei nur 6 %, stieg dann aber auf 28 % bei 1 Mbit/s bzw. 62,9 % bei 2 Mbit/s an.
Bei der Übertragung einer Dialoganwendung, das heißt bei einem Austausch von Paketen geringer Größe, lag der Leistungsverlust bei 64 kbit/s bereits bei 22,2 % und stieg dann kontinuierlich auf 63,7 % bei 2 Mbit/s an.

Probleme mit Sicherheitsmechanismen

Bild 1 verdeutlicht diese Messungen auf anschauliche Weise. Hier wurden die Ereignisse der Verzögerungsmessungen einer Dialog-Anwendung mit Austausch von Datenpaketen unterschiedlicher Größe ermittelt. Die Prozentwerte beziehen sich dabei auf die Paketverzögerung ohne Verschlüsselung. Sind also beispielsweise IP-Pakete mit 56 bis 64 Byte bei einem Gesamtdurchsatz von 1 Mbit/s ohne Verschlüsselung mit 3,7 ms Verzögerungszeit ermittelt worden und mit Verschlüsselung 8,8 ms, so entspricht dies einem Zuwachs von 137 %.
Ein weiteres Problem besteht darin, daß bei mehreren Sicherheitsmechanismen, wie SSL auf der höchsten Schicht, die Sicherheit auf der IP-Ebene nicht mehr nötig ist. Es besteht dabei auch noch das Problem der Doppelverschlüsselung, wodurch Fehler bei der Entschlüsselung sowie weitere Performance-Einbußen entstehen können.
Bei dem Einsatz des Cisco-Routers der 3600er Serie fiel der Test etwas besser aus. Trotzdem konnte man das Fazit ziehen, daß IPsec bei heutigen Implementierungen nicht für Echtzeitanwendungen geeignet ist. Aus diesem Grund sollte man über geeignete Hardware-Lösungen nachdenken, wenn man eine Echtzeitverschlüsselung benötigt [4].

VPN-Messungen

Bei der VPN-Messung wurden zwei PCs (Pentium II/400 MHz/128 MByte) als Client verwendet (LWS/Sec-Pro1.2) und Server (AMD/500 MHz/128 MByte) als Gateway (MPR/GA VPN 4.05), um die Software von NCP zu installieren *(Bild 2)*.

Die Komponente LWS/Sec Client bestand im Detail aus:
- NT-Server (Pentium II/400 MHz/128 MByte RAM);
- NCP LWS/Sec Pro V.1.2;
- NIC: 10.129.1.232;

die Komponente MPR/GA Gateway aus:
- NT-Server (AMD/500 MHz/128 MByte RAM);
- NCP MPR/GA VPN 4.05 plus NCP Enterprise Manager 4.02;
- NIC: 3Com EtherLink 10/100 PCI NIC (3C905C-TX) und
- IP: 10.129.1.249.

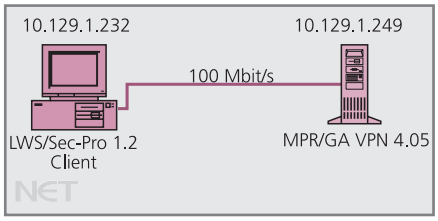

Bild 2: Meßaufbau für die VPN-Messungen

Die NCP Network Communications Products engineering GmbH mit Stammhaus in Nürnberg entwickelte eine Remote-Access-Lösung für unternehmensübergreifendes Enterprise Networking sowohl für Intranets als auch für Extranets.
Neben der Verbindung von verteilten LANs z.B. in Außenstellen und der Möglichkeit des Teleworking hat man auch die Integration mobiler Teilnehmer berücksichtigt. Zusätzlich bietet NCP den direkten Tunnelauf- und -abbau durch den Client zum firmeneige-

nen Network Access Server (NAS), unabhängig von der ISP-Infrastruktur, an. Auf diese Weise wird eine hochsichere End-to-end-Kommunikation auch ohne IPsec ermöglicht, so daß das gesamte Sicherheitsmanagement in den Händen des Unternehmens und nicht bei den jeweiligen ISPs liegt. Der Remote Client des Teilnehmers wird während des Bestehens der Verbin-dung vollständig in das Unternehmensnetz integriert. Connectivity besteht über alle öffentlichen Netze wie ISDN, PSTN (analoges Fernsprechnetz), X.25, GSM, HSCSD, GPRS, xDSL, xDSL Sat und Internet. Protokollseitig werden neben IP auch IPX, SNA und NetBIOS unterstützt und transparent im WAN übertragen. Als Tunnelverfahren kann Layer 2 Forwarding Protocol (L2F), Layer 2 Tunneling Protocol (L2TP) und IPsec eingesetzt werden. Das L2TP-Tunneling-Protokoll ist, so wie es NCP implementiert hat, in der RFC-2716 als L2sec dokumentiert. In der höchstmöglichen Sicherheitsstufe unterstützen die NCP-Komponenten PKI-Infrastrukturen nach X.509v3. Die Einbindung der Lösung in private oder öffentliche Trust-Center-Umgebungen (z.B. T-Telesec, Deutsche Post Signtrust) ist bereits in der Praxis erprobt worden [3].

Nach der LWS/Sec-Pro-Installation wurde zu dem physischen der virtuelle Netzwerkadapter (NCP LWS/Sec-Pro Adapter) installiert. Bei der Konfiguration der Netzadapter wurde ein Gateway-Eintrag lediglich beim physischen Adapter verwendet. Hierdurch werden nur die im LWS/Sec-Monitor angegebenen Netze über Tunnel erreicht. Die Konfiguration kann durch Einsicht in die Routing-Tabelle kontrolliert werden. Der restliche Datenverkehr wird über das Default-Gateway geroutet. Bei einer Verbindung zum Server (MPR/GA-Gateway) bedarf es jedoch eines weiteren Routing-Tabellen-Eintrags auf dem Server. Dieser Eintrag sorgt dafür, daß alle Daten mit virtuellem Zielnetz über das (virtuelle) Gateway geroutet werden.

Damit alle IP-Pakete mit Ziel 172.17.1.0 vom MPR/GA- zum LWS/Sec-Client durch den Tunnel übertragen werden, muß die Routing-Tabelle um den folgenden Eintrag ergänzt werden: route add -p 172.17.1.0 mask 255.255.255.0 10.1.1.1. Alle Pakete mit dem Zielnetz 172.17.1.0 werden dann über das VPN-Gateway gesendet. Zur Administration des Network Access Server (NAS) wurde der NCP Enterprise Manager benötigt. Dieser kann auf jedem PC, der in Verbindung mit dem NAS steht, installiert werden. Im Enterprise Manager wird neben dem WAN Link für Default User Tunnel-End-Point auch der für den User1 konfiguriert. Um nun Daten verschlüsselt zu übertragen, muß im LWS/Sec-Client und MPR/GA-Gateway der gleiche Verschlüsselungsalgorithmus und Schlüssel ausgewählt werden.

Bild 3 (s. S. 38) zeigt die Performance-Einbrüche bei verschiedenen Varianten der Verschlüsselung. Dabei werden die besten Ergebnisse erzielt, wenn ausschließlich L2TP eingestellt ist. Die größten Einbrüche sind mit L2TP+DES+Komprimierung festzustellen. IPsec konnte bei der NCP-Software nicht getestet werden, da diese zum Testzeitpunkt nicht zur Verfügung stand. Dies wird in Zukunft nachgeholt. Als Ergebnis läßt sich auch hier feststellen, daß die Performance auf unter 1/5 zurückgeht. Dies kann sich auch bei geringeren Datenraten negativ bemerkbar machen [2].

Firewall-1-Messung

Die FireWall-1 ist ein Produkt, das ursprünglich für Sun-Systeme unter Solaris entwickelt wurde und aktuell u.a. auch unter Windows NT verfügbar ist. FireWall-1 von CheckPoint hat sich inzwischen zum Marktführer entwickelt und ist weltweit die mit Abstand am häufigsten installierte kommerzielle Firewall-Software. FireWall-1 (Version 4.0) ist von der National Computer Security Association (NCSA) und IT-SEC E3 zertifiziert. Sie kontrolliert sämtliche Zugriffe auf das gesamte Netz, indem sie jedes Informationspaket mit verschiedensten Filtertechnologien durchsucht (Stateful Inspection). Individuell definierbare Sicherheitsstandards, auch für nicht standardisierte TCP/IP-Dienste, können jederzeit an die wechselnden Sicherheitsanforderungen angepaßt werden. Die Bildung von VPNs zur verschlüsselten Verbindung von Firmennetzen über mehrere FireWall-1-Systeme ist optional möglich. Die Lösung besteht dabei aus einem Softwarepaket, welches Zugriffskontrolle, Authentifizierung, Network Address Translation (NAT), Content Security, Auditing und unternehmensweites Policy-Management enthält [3].

Zur Messung wurden der SecuRemote Client und die Firewall-1 verwendet.

Nr.	Source	Destination	Service	Action	Track	Install On	Time
1	Remote-User@ any	Server	Any	Client Encrypt	Long	Gateways	Any
2	Any	Server	Any	Accept	Long	Gateways	Any
3	Server	Any	Any	Accept	Long	Gateways	Any

Tabelle: Firewall-1 Security Policy

Bei der Konfiguration der FireWall-1 wurde zuerst der Remote User 1 eingerichtet. Anschließend darf User 1 von jeder Lokation auf die Firewall zugreifen. Der SecuRemote-Zugriff ist dabei nicht an eine bestimmte IP-Adresse gebunden. Der Meßaufbau ist ähnlich einfach gehalten wie bei der vorherigen Messung, um möglichst alle Nebeneffekte ausschließen zu können.

Die Komponente SecuRemoteClient bestand aus:

- NT-Server (Pentium III/500 MHz);
- SecuRemote Client 4.0;
- NIC: 3Com EtherLink 10/100 PCI NIC (3C905C-TX);
- IP: 10.129.1.250;

die Komponente Firewall-1 aus:

- NT-Server;
- FireWall-1 4.0;
- NIC: 3Com EtherLink 10/100 PCI NIC (3C905C-TX);
- IP: 10.129.1.249.

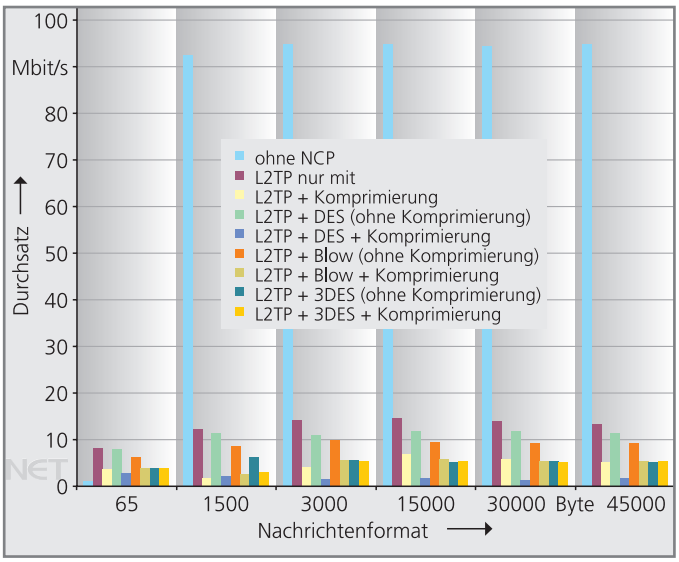

Bild 3: NCP-Performance-VPN-Test

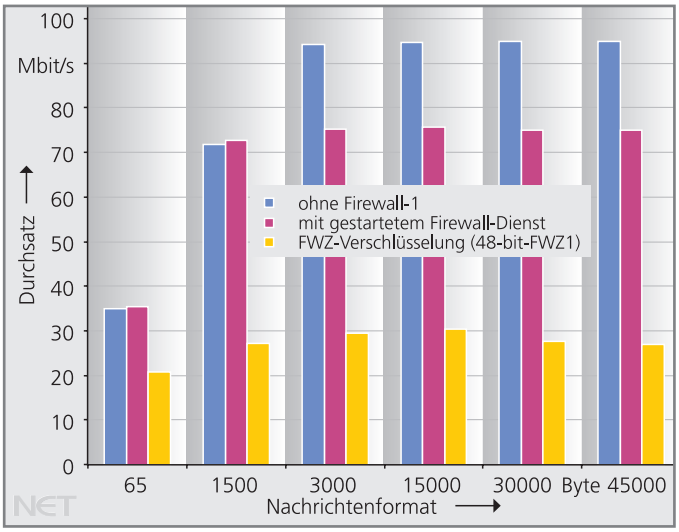

Bild 4: Firewall-1-Messungen

Bei der Einstellung der Security Policy sind wenig Regeln eingestellt worden, um die Leistungsfähigkeit so wenig wie möglich zu beeinträchtigen. In der *Tabelle* werden nur drei Regeln angezeigt, die im Grunde alles ermöglichen, aber zusätzlich eine 48-Bit-Verschlüsselung vornehmen [2].

Herstelleraussagen mit Vorsicht genießen

Bild 4 zeigt die Ergebnisse der FireWall-1-Messungen. Auch hier wird ein drastischer Performance-Abfall festgestellt, wenn Verschlüsselung hinzugenommen wird.
Allerdings macht die alleinige Anwesenheit der Firewall-Dienste – sprich der Security Policy – noch keinen Engpaß aus. Es sind auf der anderen Seite auch nicht viele Regeln eingestellt worden, weshalb dies noch in zukünftigen Mes-sungen überprüft werden sollte. Die Verschlüsselung mit 48 Bit führt hier auf der einen Seite zwar auf Werte um die 20 Mbit/s, ist allerdings auf der anderen Seite kein schlechtes Ergebnis, da heutige WAN-Verbindungen davon meist unbeeindruckt bleiben.
Anzumerken ist jedoch, daß keine starke Verschlüsselung mittels Blowfish oder Triple-DES eingesetzt worden ist, was sicherlich die Performance weiter nach unten setzen wird.
Die veröffentlichten Ergebnisse von Checkpoint bezüglich der Leistungsfähigkeit der FireWall-1 sind allerdings ohne Verschlüsselung und mit dem Aufsatz nur weniger Regeln ermittelt worden. Aus diesem Grund sind die Aussagen der Hersteller immer mit Vorsicht zu genießen, da hier doch erhebliche Unterschiede zu einer verschlüsselten Übertragung bestehen.

Resümee

Als Endresultat bleibt festzustellen, daß die Performance bei Verschlüsselung und Authentifizierung kein Produktproblem ist, sondern ein generelles Problem durch die abzuarbeitenden Algorithmen. Dies stellt Softwarelösungen auf eine harte Probe, sollen sie doch auf der einen Seite möglichst hohe Schlüssel für einen hohen Sicherheitsgrad verwenden, auf der anderen Seite aber die teuren WAN-Leitungen nicht beeinträchtigen.
Hier ist sicherlich ein Kompromiß zwischen Leistung und Sicherheit erforderlich. In Zukunft wird man aber nicht an der Implementierung von IPsec in Hardware vorbeikommen, um eine höhere Leistung zu erhalten. Dabei ist man aber wieder in der Bewegungsfreiheit eingeschränkt. Auch hier muß man also wieder einen Kompromiß finden, der auf die jeweiligen Anforderungen des Unternehmens abgestimmt sein muß.

Literatur

[1] Franken, Malte: Sicherheit auf der Netzwerkschicht (IPsec); Seminararbeit im Rahmen der Veranstaltung „Sicherheit in verteilten Systemen“; Fachbereich Informatik, Abteilung Rechnernetze; Prof. Dr. W. Kowalk; Universität Oldenburg; Oldenburg 2000.

[2] Müller, Merkus: Conception, planning and evaluation of Extranets for secure communication and cooperation between distributed enterprise locations: Protocols, Products and Security; Hochschule Bremen and South Bank University London; Computer and Information Engineering; Bremen 2000.

[3] Detken, Kai-Oliver; Eren, Evren: Extranet – VPN-Technik zum Aufbau sicherer Unternehmensnetze; Addison-Wesley-Verlag; Pearson Education Deutschland GmbH; ISBN 3-8273-1674-X; München 2001.

[4] Gorecki, Christian A.: Sichere Sprachübertragung über das Internet; Diplomarbeit an der Universität Bremen; Prof. Dr.-Ing. Rainer Laur; Fachbereich Physik/Elektrotechnik FB1; Bremen 2000.

(we)