Vergleichstest Security-Appliances – Für eine effektive Absicherung der Unternehmens-Kommunikation sollen spezialisierte Systeme mit Sicherheitsfunktionalität sorgen.

Schnell und sicher

Unified-Communcations bedeutet für viele Unternehmen, alle ITK-Datenströme zwischen den Unternehmensstandorten über eine technische Infrastruktur zu lenken. Um diese sensiblen Datenströme im unsicheren WAN zu schützen, werden VPN-Tunnel zwischen den Standorten etabliert. Durch diese Tunnel laufen alle Datenströme des Unternehmens, also auch Real-Time-Anwendungen wie VoIP oder Video-over-IP. Hierzu setzen die IT-Verantwortlichen in den Unternehmen Security-Appliances ein. Solche Systeme vereinen Firewall, VPN sowie diverse weitere Funktionalität auf einer Hardware-Plattform. Um den zuverlässigen Betrieb auch für echtzeitfähige Anwendungen wie die IP-Telefonie zu garantieren, müssen diese Systeme einige Voraussetzungen erfüllen. Dazu gehören die Datenpriorisierung sowie ein intelligentes Bandbreitenmanagement.

Eine Security-Appliance ist im Grunde eine aktive Netzwerkkomponente, wie ein Switch oder ein Router, die nicht nur die Kommunikation zwischen zwei Netzwerken oder Netzwerksegmenten ermöglicht, sondern zugleich eine Überwachungs-, Kontroll- und Schutzfunktion erfüllt, um die Unternehmenskommunikation beispielsweise vor unerwünschtem Datenverkehr oder Zugriffen zu schützen.

Auf der »internen« Seite handelt es sich zumeist um Ethernet-basierte Netze, »extern« können neben Ethernet-Netzen auch die unterschiedlichsten WAN-Verbindungen wie xDSL, Mietleitungen, Datendirektverbindungen, Standleitungen oder X.25 angeschlossen sein. Platziert werden Security-Appliances in der Regel zwischen dem abzusichernden Netz oder Netzsegment und einem entsprechenden Remote-Access-System oder einer anderen aktiven Komponente. Diese ermöglicht die WAN- oder LAN-Anbindung ins externe Netz oder ins benachbarte LAN-Segment. Hierfür bieten solche Appliances heute Fast-Ethernet- und häufig auch Gigabit-Ethernet-Ports an. Manche Systeme stellen darüber hinaus auch eigene WAN-Anschlüsse wie ISDN oder xDSL zur Verfügung.

Bei vielen Appliances lässt sich über einen der LAN-Ports zusätzlich eine »demilitarisierte Zone«, kurz DMZ, einrichten, in der beispielsweise Web-Server stehen, die von außen und innen erreichbar sein sollen.

Mit zunehmender Komplexität der heutigen Unternehmensnetze und in Anbetracht der Erkenntnis, dass das Gros der virtuellen Gefahren aus dem eigenen Unternehmensnetz und nicht aus dem Internet droht, gehen Netzwerkdesigner mehr und mehr dazu über, auch das interne Unternehmensnetz in einzelne Segmente zu parzellieren, die gegeneinander durch Security-Appliances gesichert werden. Durch die Integration dieser Systeme in das Unternehmensnetz muss nun aber nicht nur der Datenverkehr intern – extern, sondern auch ein Großteil des internen Datenverkehrs entsprechende Systeme passieren.

In Anbetracht der Datenmengen, der Qualitätsanforderungen in heutigen konvergenten Netzen mit ihren Voice- und Video-Applikationen und der Leistungsfähigkeit der übrigen Komponenten im Unternehmensnetz erhöht dieses Anwendungsszenario deutlich die Anforderungen an Security-Systeme im Hinblick auf Performance und Funktionalität. In Anbetracht dieser Situation machen Durchsatzraten auch im Gigabit-Bereich durchaus Sinn und die Implementierung der Gigabit-Ethernet-Technologie ist eine logische Konsequenz. Die Anforderungen an die Leistungsfähigkeit solcher Appliances entsprechen dann logischerweise denen, die auch an andere Komponenten des Unternehmensnetzes, wie LAN-Switches, gestellt werden.

VPN inklusive

Neben der klassischen Firewall-Funktionalität gehört der Aufbau von VPNs zur Standardfunktionalität von Security-Appliances. Virtuelle private Netzwerke, neudeutsch Virtual-Private-Networks oder kurz VPN, sollen einer geschlossenen Gruppe von Systemen eine geschützte Kommunikation über ein potentiell unsicheres Netz hinweg erlauben. Die logisch geschlossene Verbindung, auch VPN-Tunnel genannt, wird durch kryptografische Algorithmen realisiert, die die zu schützenden Datenströme verschlüsseln und an der Gegenstelle wieder entschlüsseln. Für diese Verschlüsselung gibt es eine ganze Reihe von Standards wie DES, 3DES oder AES. Über die Sicherheit solcher Verbindungen entscheidet – wie bei anderen kryptografischen Verfahren auch – nicht zuletzt die Länge der verwandten Schlüssel. Mechanismen wie Authentisierung oder Autorisierung sorgen zusätzlich dafür, dass keine unerwünschten User in das private Netz eindringen. Technisch realisieren Unternehmen ein solches VPN, indem sie an den Übergangsstellen zwischen sicherem und unsicherem Netzwerk ein VPN-System installieren.

Die wesentliche Verschlüsselungsfunktionalität ist zumeist in Software abgebildet, was bedeutet, dass die Funktionalität sehr rechenintensiv ist und eine gute Performance eine entsprechend leistungsfähige Hardware voraussetzt. Es gibt aber auch VPN-Lösungen, die Hardwarenäher realisiert sind und dann entsprechend leistungsfähiger sein können.

Auswirkungen von Datenverlusten

Für die Beurteilung des Verhaltens der Systeme im Testfeld, die wir mit Datenströmen bestehend aus den unterschiedlichsten Frame-Formaten belastet haben, ist es von besonderem Interesse, zu betrachten, welche Lasten und Frame-Größen in realen Netzen vorkommen. Bei klassischen Dateitransfers arbeitet das Netzwerk mit möglichst großen Datenrahmen. Bei Echtzeit-Applikationen teilt sich das Feld. Video-Übertragungen nutzen ähnlich den Dateitransfers relativ große Datenrahmen. Voice-over-IP bewegt sich dagegen im Feld der mittelgroßen und kleinen Frames. Messungen mit Ethernet-LAN-Phones der ersten Generation in unseren Real-World Labs haben beispielsweise ergeben, dass diese Voice-over-IP-Lösung die Sprache mit konstant großen Rahmen von 534 Byte überträgt, ein aktuelles SIP-Phone überträgt 214 Byte große Rahmen.

Aktuelle Lösungen überlassen es dem IT-Verantwortlichen selbst festzulegen, mit welchen Frame-Größen die Systeme arbeiten sollen. Dabei sollte der IT-Verantwortliche berücksichtigen, dass der Paketierungs-Delay mit kleiner werdenden Datenrahmen kleiner wird. Dagegen wächst der Overhead, der zu Lasten der Nutzdatenperformance geht, je kleiner die verwendeten Pakete sind. Generell kann man bei der IP-Sprachübertragung davon ausgehen, dass kleine Frames verwendet werden. Die meisten Web-Anwendungen nutzen mittelgroße Datenrahmen. Die kleinstmöglichen Frames von 64 Byte sind dagegen beispielsweise bei den TCP-Bestätigungspaketen oder interaktiven Anwendungen wie Terminalsitzungen zu messen.

Die Analyse der Verteilung der Framegrößen, die für das NCI-Backbone dokumentiert ist, sowie die Ergebnisse der Analyse typischer Business-DSL-Links haben ergeben, dass rund 50 Prozent aller Datenrahmen in realen Netzwerken 64 Byte groß sind. Die übrigen rund 50 Prozent der zu transportierenden Datenrahmen streuen über alle Rahmengrößen von 128 bis 1518 Byte. Für die Übertragung von Real-Time-Applikationen ist zunächst das Datenverlustverhalten von entscheidender Bedeutung. Für Voice-over-IP gilt beispielsweise: Ab 5 Prozent Verlust ist je nach Codec mit deutlicher Verschlechterung der Übertragungsqualität zu rechnen, 10 Prozent führen zu einer massiven Beeinträchtigung, ab 20 Prozent Datenverlust ist beispielsweise die Telefonie definitiv nicht mehr möglich. So verringert sich der R-Wert für die Sprachqualität gemäß E-Modell nach ITU G.107 schon bei zehn Prozent Datenverlust um je nach Codec 25 bis weit über 40 Punkte, also Werte, die massive Probleme im Telefoniebereich sehr wahrscheinlich machen.

Dafür, dass es zu spürbaren Datenverlusten im Netzwerk erst gar nicht kommt, sollen entsprechend gut funktionierende Priorisierungsmechanismen sorgen. Bei entsprechender Überlast im Netz sind Datenverluste unvermeidbar, jedoch sollen sie durch die Priorisierungsmechanismen in der Regel auf nicht echtzeitfähige Applikationen verlagert werden. Arbeitet diese Priorisierung nicht ausreichend, kommt es auch im Bereich der höher priorisierten Daten zu unerwünschten Verlusten. Dieses Priorisierungsverhalten ist daher auch für Security-Appliances, die in entsprechenden Netzen zum Einsatz kommen, wichtig.

Qualitätssicherung im Netz

Ethernet-basierte Netze ermöglichen eine kostengünstige durchgehende Netzwerk-Lösung vom Backbone-Bereich bis an die Endgeräte am Arbeitsplatz und sind nicht zuletzt aus diesem Grund weltweiter Standard in praktisch allen Unternehmen und Institutionen. Allerdings bietet das Ethernet auf Layer-2 und -3 nicht die selbe Übertragungsqualität wie von Hause aus echtzeitfähige Technologien, beispielsweise ATM. Das Ethernet-Protokoll ist zwar einfacher und arbeitet mit geringerem Overhead, die Übertragungen erfolgen aber ohne vorherigen Aufbau einer Verbindung oder die Aushandlung der Qualität der Übertragungsstrecke von Endpunkt zu Endpunkt. Für alle Applikationen wird nur eine Best-Effort-Behandlung – so gut, wie eben möglich – bereitgestellt. Dies geschieht unabhängig von deren tatsächlichen Anforderungen oder den Anforderungen der Nutzer. Die Absicherung einer Verbindung erfolgt – wenn überhaupt – erst in den Protokollen höherer Ebenen, wie dem TCP.

In Ethernet-Netzen und unter Verwendung des TCP/IP-Protokolls – und damit auch im Internet, Intranet oder Extranet – gibt es also keine garantierten Verbindungseigenschaften. Deshalb ist auch die Implementierung von Quality-of-Service oder kurz QoS, wie man es von ATM kennt, nicht möglich. Trotzdem versuchen die Ethernet-Produktentwickler seit einigen Jahren durch Priorisierung und Reservierung von Ressourcen auch in IP-Netzen verschiedene Serviceklassen, die Class-of-Service oder CoS, zu etablieren. Allgemein sind zwei Wege zu unterscheiden, Service-Qualitäten zu realisieren. Dies geschieht zum einen über die Reservierung von Netzwerkressourcen, die Resource-Reservation, und zum anderen über eine bevorzugte Behandlung bestimmter Pakete bei deren Weiterleitung, die Daten-Priorisierung.

Grundlage für letztere ist die Entscheidung, welches Paket welche Priorität besitzt. Diese Entscheidung kann auf Grundlage der generell zur Verfügung stehenden Informationen aus den Headern der Ebenen 2, 3 oder 4 erfolgen. So ist es möglich, den Verkehr beispielsweise hinsichtlich der Quell- und Zieladressen (MAC oder IP) oder der Protokoll- und Portnummern einzuteilen. Dies ist natürlich abhängig davon, bis in welche Ebene das Netzwerkgerät die Protokoll-Header analysieren kann. Geht man einen Schritt weiter, kann man in den Protokoll-Headern der verschiedenen Ebenen bestimmte Bits gezielt setzen und so die Zugehörigkeit eines Paketes zu einer Prioritätsklasse kennzeichnen.

Die Hierarchie der Prioritätsentscheidungen auf den verschiedenen Layern, die ja durchaus widersprüchlich sein kann, ist für jede aktive Netzwerkkomponente intern gelistet und entweder frei konfigurierbar oder fest vorgegeben. Zu beachten ist auch, dass Layer-2-Priorisierungen auf dem Weg durch ein Netzwerk in der Regel verloren gehen, sobald sie auf Layer-3 geswitched beziehungsweise geroutet werden. Die Konfiguration des aktiven Netzwerks, das intelligent die Priorisierungsmechanismen nutzen soll, ist daher gerade in heterogenen Umfeldern nicht gerade trivial. Häufig wird der IT-Verantwortliche gut beraten sein, wenn er sich schon aus Gründen einer vollständigen Kompatibilität für ein

Netzwerk aus einer Hand entscheidet. Bei größeren Netzen ist auch eine entsprechende CoS-Management-Software unerlässlich, um die zur Verfügung stehenden Priorisierungsmechanismen auch wirklich effizient nutzen zu können.

Qualitätssicherung auf Ebene 3

Eine Möglichkeit der Zuordnung eines IP-Paketes ist die Nutzung des Type-of-Service-Byte, kurz ToS, im IP-Header Version 4. Dazu sind zwei Varianten beschrieben. RFC 791 definiert mit den Bits 0 bis 2 acht Klassen, von »Routine« über »Immediate« bis zu »Network-Control«. Pakete mit einem höheren Octal-Wert in diesem 3-Bit-Feld werden vorrangig behandelt (IP-Precedence). Variante 2 verwendet die Bits 3 bis 6, um eine normale und vier um besondere Service-Klassen zu kennzeichnen. Festgehalten ist dies in RFC 1349. Ungünstigerweise wird dieses vier Bit große Teilfeld des ToS-Byte ebenfalls als Type-of-Service bezeichnet. Es gibt also im IP-Header ein ToS-Byte und darin enthalten ist ein ToS-Feld. Pakete können anhand des ToS-Feldes entsprechend der eingestellten Klasse Warteschlangen unterschiedlicher Priorität zugeordnet werden. Im IP-Header Version 6 ist ebenfalls ein Byte für eine Klasseneinteilung vorgesehen. Es wird treffend als »Class« bezeichnet und könnte ähnlich verwendet werden.

Eine Arbeitsgruppe der IETF stellte 1997 eine alternative Implementation des ToS-Byte vor. Auch bei den Differentiated-Services, kurz Diffserv, wird dieses Byte dazu verwendet, um Pakete mit Markierungen zu versehen, die dann auf den Netzwerkknotenpunkten eine bestimmte Behandlung bei der Weiterleitung zum nächsten Knoten bewirken (Per-Hop-Behavior). Dazu erhält dieses Byte im IP-Header per Definition eine neue Bedeutung und wird in diesem Anwendungsfall dann als Differentiated-Service-Byte oder kurz DS-Byte bezeichnet.

Die Diffserv-Spezifikation nach RFC 1349 definiert sechs Bits, die dazu dienen, den Differentiated-Services-Code-Point festzulegen. Diese sechs Bits werden genutzt, um verschiedene Service-Klassen zu definieren. Jede Netzwerkkomponente entscheidet anhand dieser Bits, wie die entsprechenden Pakete zu behandeln sind, und steuert das Per-Hop-Behavior. Die sechs Bits sind nochmals in zwei mal drei Bits unterteilt. Diese Struktur ist in RFC 1349 festgeschrieben, aber letztendlich ist es den Herstellern beziehungsweise den Netzwerkadministratoren freigestellt, wie sie diese Bits genau nutzen.

Eine sinnvolle Diffserv-Anwendung ist daher nur möglich, wenn ein Managementsystem durchgängig die notwendigen Service-Klassen-Zuordnungen steuert. Die insgesamt 64 Codierungs-Möglichkeiten müssen auf die vorhandenen Hardware-Queues beziehungsweise auf die zur Verfügung stehenden Links abgebildet werden und so dafür sorgen, dass die unterschiedlichen Dienste mit der gewünschten Qualität übertagen werden können. Diese Mechanismen müssen in einer Domäne konsistent arbeiten und zwischen verschiedenen Domänen durch Mapping gesichert werden.

Die Funktionsweise bei der Priorisierung ist im Grunde immer die gleiche. Pakete werden auf den Gateways und Knotenpunkten anhand dieser Unterscheidungsmerkmale in den Headern den Warteschlangen oder Queues unterschiedlicher Priorität zugeordnet. Die Queues höherer Priorität werden dann entsprechend der Policy der jeweiligen Queuing-Mechanismen bevorzugt weitergeleitet. Welches Prinzip dieser Bevorzugung zu Grunde liegt, ist unterschiedlich. In vielen Fällen sollte eine Priorisierung aber nicht ohne eine Festlegung einer gewissen Maximalbandbreite erfolgen. Diese könnte beispielsweise so aussehen, dass die Queue mit der höchsten Priorität nur eine bestimmte maximale Bandbreite erhält. Ohne diese Begrenzung kann es passieren, dass bei einer Überlast ausschließlich hoch eingestufte Pakete transportiert werden, während sich die Pakete in den unteren Queues stauen, bis sie verworfen werden. Ein solches Verhalten ist bei reinen Strict-Priority-Mechanismen typisch.

Das Festlegen einer minimalen Bandbreite für Pakete niedrigerer Priorität erfüllt den selben Zweck. Moderne Netzwerkkomponenten verschieben diese Grenzen dynamisch, abhängig vom momentanen Verkehr. Zu beachten ist jedoch, dass bei voller Ausreizung der entsprechenden Bandbreiten und der den Queues zugeordneten Buffern auch Pakete höherer Priorität keine Chance mehr haben, transportiert zu werden und ebenso verfallen können. Obwohl eigentlich alle aktuellen Netzwerkgeräte das ToS- beziehungsweise DS-Byte auswerten können, ist diese Funktion in den seltensten Fällen aktiviert und wird höchstens im In-House-Bereich oder anderen abgegrenzten und kontrollierbaren Umgebungen genutzt.

Port-Nummern-Klassifizierung

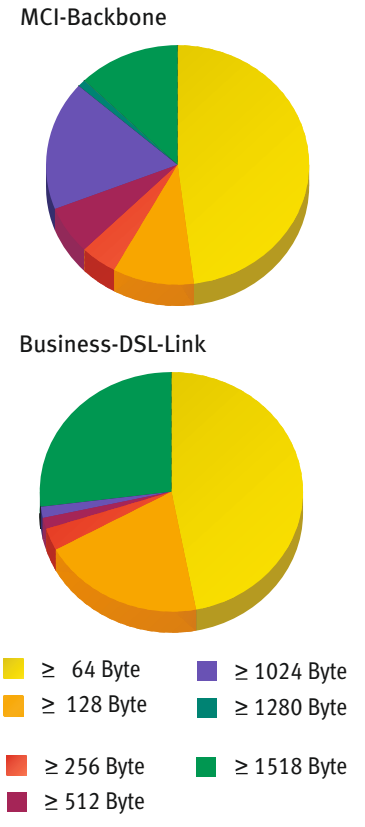
Die meisten Applikationen sowie Windows-Betriebssysteme beherrschen die Klassifizierung mit ToS und Diffserv nicht. Daher erfolgt zumeist eine erste Klassifizierung nach Diensten im Edge-Bereich sinnvoller Weise über die benutzten TCP- oder UDP-Port-Nummern. Hierbei weist der Edge-Switch anhand der erfolgten Klassifizierung den Paketen die entsprechende Hardware-Queue zu. Optional können die Klassifizierungen dann auch auf ToS- beziehungsweise Diffserv-Werte gemappt werden. Dabei werden die schon vorhandenen Werte überschrieben. Diese generierten ToS- und Diffserv-Werte können dann die Core-Switches weiter verwenden, ohne dass sie erneut ein Mapping durchführen müssten. Im vorliegenden Vergleichstest wurden zur Festlegung der Prioritäten die jeweiligen UDP-Portnummern gesetzt. Die Klassifizierung der einzelnen Datenströme erfolgte durch das jeweilige System, das die Datenströme empfing.

Fazit

Generell erfolgt das Routing von Datenströmen nach Merkmalen, die in den Headern der Datenpakete festgelegt sind. Hierfür werden in der Praxis beispielsweise Port-Nummern oder IP-Adressen verwendet. Diese Mechanismen sind bereits im Standard-Linux implementiert. Somit sind alle Systeme, die auf Linux basieren, von Hause aus bereits für den Einsatz in Unified-Communications-Umgebungen geeignet. Allerdings muss die Funktionalität auch vernünftig im GUI abgebildet sein. Voraussetzung ist dann noch, dass die erforderliche Rechenleistung für die entsprechende Funktionalität auch vorhanden ist. Alternativ ist es auch möglich, zur Verbesserung der Performance entsprechende Switch-Module zu integrieren, die eine Überlastung der Appliance vermeiden können. Dies ist möglich, indem das Switch-Modul dazu eingesetzt wird, um mittels Bandbreitenlimitierung eine Überlastung der Filterfunktionalität zu verhindern. Wie gut aktuelle Security-Appliances in der Praxis sind, musste eine Reihe von Systemen in unseren Real-World Labs an der FH Stralsund beweisen.

Dipl.-Ing. Thomas Rottenau,
Prof. Dr. Bernhard G. Stütz,
dg@networkcomputing.de

Verteilung der Framegrößen



Analysen der Verteilung der Framegrößen beispielsweise für das MCI-Backbone oder von den Applikationen her typischer Business-DSL-Links haben ergeben, dass rund 50 Prozent aller Datenrahmen in realen Netzwerken 64 Byte groß sind.