Onlinekapitel: Glossar

Dies ist die Liste der Fachbegriffe und Abkürzungen sowie deren Erklärung zum Buch:

Dr. Matthias Leu: Check Point Next Generation AI.
C&L-Verlag 2003,
1070 Seiten,
ISBN 3-936546-05-3.

Kursiv dargestellte Begriffe finden sich mit einer eigenen Definition wieder.

3DES

siehe *Triple-DES*.

Access Control List (ACL)

Regelbasis für *Paketfilter*, die auf einem Router, beispielsweise 3Com, Bay oder Cisco installiert werden kann, oft auch nur Access List genannt.

Accounting Log Entry

Einträge in eine spezielle Log-Datei früherer Versionen der FireWall-1, bei denen zusätzlich die Dauer der Verbindung und die Anzahl übertragener Pakete beziehungsweise Bytes erfaßt wird. Bei Next Generation befinden sich diese Einträge im normalen, datenbankbasierten Log.

Account Unit

auch kurz AU, *LDAP*-Server zur Authentisierung von Benutzern durch Next Generation.

Access-Control Rights

Bei Next Generation die Definition verschiedener Zugriffsrechte auf den *SmartCenter*.

Access Method

Zugriffsmethode auf das physikalische Netzwerkmedium (beispielsweise *CSMA/CD* oder Token Passing).

ACK

Acknowledgement, auch Flag im TCP-Header, durch das gekennzeichnet wird, daß im Feld *Acknowledgement Number* ein gültiger Eintrag vorhanden ist. Damit wird im *TCP* vom Absender der korrekte Empfang eines Paketes durch den Empfänger überprüft.

Active Directory

Mit Microsoft Windows 2000 eingeführte Domainstruktur zur Verwaltung von Benutzern. Sie ist kompatibel zu LDAP und wird, entsprechende Lizenzierung vorausgesetzt, auch von Next Generation unterstützt.

AD

siehe Microsoft *Active Directory*.

Address-Translation Modes

Anderer Name für Network Address Translation (*NAT*) und die Arten, wie sie durchführbar ist.

Address-Translation Rulebase

Regelbasis von Next Generation, in der die Regeln für eine Übersetzung der IP-Adressen eingetragen werden.

AES

Advanced Encryption Standard, der mit dem Rijndal-Algorithmus mit Schlüsseln einer Länge von 128, 192 oder 256 Bit arbeitet, in den USA offizieller Nachfolger von *DES* und *3DES*. Check Point Next Generation unterstützt diesen Algorithmus mit 128 Bit und 256 Bit.

AI

Application Intelligence, mit Next Generation Feature Pack 4 eingeführte Bezeichnung für eben diesen Feature Pack. Beschreibt, daß die Untersuchung von Inhalten nicht mehr grundsätzlich die Security Server erfordert.

ANSI

American National Standards Institute.

Anti-Spoofing

Mechanismus zur Sicherstellung, daß über ein Netzwerk-Interface nur Pakete mit einer IP-Absenderadresse akzeptiert werden, die nach den internen Routingtabellen auch auf diesem Interface den Rechner verlassen würden (Ausnahme: die eigene IP-Adresse dieses Interfaces).

Anti-Virus Inspection

Komponente von Next Generation, über die externe Anti-Virus-Server angesprochen werden können (siehe auch *CVP*).

API

Application Programming Interface, definierte und offengelegte Schnittstelle, über die von außen auf das Betriebssystem oder auch Module von Next Generation zugegriffen werden kann.

Application Level Gateway

oft auch verallgemeinernd *Proxy* genannt, Filtermechanismus für übertragene Daten, der auf Schicht 7 arbeitet und daher die eigentlichen Nutzdaten (beispielsweise auch Java oder Skripte) filtern kann.

ARP

Address Resolution Protocol, Umsetzung der logischen auf die physikalische Adresse innerhalb eines Netzsegments.

ARPA

Advanced Research Projects Agency.

ARPANET

Advanced Research Projects Agency Network, Vorläufer des Internet.

AS

Autonomous System, im Bereich dynamischen Routings eigenständiges, unabhängiges System.

ASM

Advanced Security Management, bei Check Point Dinge, welche SmartDefense betreffen.

Asymmetrische Verschlüsselung

Auch *Public-Key Verfahren* genannt. Verschlüsselungssystem mit einem privaten (geheimen) und einem öffentlichen Schlüssel. Notwendig sind lange Schlüssel, die Geschwindigkeit ist aufgrund des Rechenaufwands gering.

ATM

Asynchronous Transfer Mode, Netzwerkprotokoll.

Authentisierungs-Schema

Schema für die Abfrage von Benutzernamen und Paßwort, wodurch sichergestellt wird, daß es sich um einen berechtigten Benutzer handelt.

Autoritative Antwort

Diese liefert ein *Nameserver* auf eine Anfrage hin, wenn er sie als Master Server gibt. Als Master Server gilt hier sowohl der Master als auch der Slave. Die Antwort kommt direkt aus den Resource-Records (*RR*), die der Administrator von Hand angelegt hat. Sie ist endgültig und nicht von anderen Nameservern korrigierbar.

AXENT Defender

Server, mit dem eine tokenbasierte Authentisierung von Benutzern mittels Einmal-Paßworten möglich ist. Es handelt sich hierbei um ein Challenge-Response-Verfahren. Von früheren Versionen der Check Point unterstützt, seit Next Generation Feature Pack 3 nicht mehr.

Backbone

»Hauptstrecke« in einem Netzwerk oder hoch performant beziehungsweise hochverfügbar ausgelegte Verbindung zwischen verschiedenen Servern mit der Möglichkeit, Subnetze anzuschließen.

Bandbreite

Differenz zwischen unterer und oberer Frequenzgrenze. Im Netzwerkbereich wird hiermit auch oft die maximal übertragbare Datenmenge pro Zeiteinheit bezeichnet.

BGP

Border Gateway Protocol, im Internet verwendetes dynamisches Routing-Protokoll.

BIND

Berkeley Internet Name Daemon, Standard-Software zur Einrichtung des *Nameservice*, bestehend aus *Resolver*, *Nameserver* und Tools zur Administration.

BIOS

Basic Input/Output System, Basissystem eines Rechners, auf dem das Betriebssystem aufsetzt.

Blowfish

Frei verfügbarer, symmetrischer Verschlüsselungsalgorithmus von Bruce Schneier mit einer variablen Schlüssellänge von bis zu 448 Bit.

BOOTP

Boot Protocol, genutzt zur Übertragung von Daten über das Netzwerk, die Rechner zum Booten benötigen (beispielsweise IP-Adresse, Ort des Boot-Images).

Bridge

Vermittler zwischen mehreren physikalisch unterschiedlichen Netzen, die aber im gleichen logischen Netzwerk liegen. Arbeitet auf der Bitübertragungsschicht (Data Link Layer).

Broadcast

Rundsendeprinzip. Nachricht, die von einer Maschine an alle anderen im Netzwerk gesendet wird, gerichtet an die Broadcast-Adresse (die oberste Adresse im Netzwerk).

BSD

Berkeley Software Distribution, eine der beiden Unix-Familien, Anwendung beispielsweise in FreeBSD oder Nokia IPSO.

Bypass

Vorbeileiten von Daten an einem Host in einem Ringsystem.

CA

siehe *Certificate Authority*

Caching-Only Server

Nameserver ohne eigene Daten, der lediglich Informationen in seinem Zwischenspeicher (Cache) sammelt und diese an die anfragenden *Resolver* weitergibt.

CCITT

Comite Consultatif International Telegraphique et Telephonique.

Certificate Authority

Vertrauenswürdige Drittstelle, über die öffentliche Schlüssel sicher bezogen werden können. Die CA zertifiziert einen öffentlichen Schlüssel, in dem sie ihn digital signiert. Damit ist sichergestellt, daß der bezogene Schlüssel der richtigen Person zugeordnet ist. Eine Certificate Authority wird auch Trust Center genannt.

Cheapernet

10Base2, schwarzes RG-58-Kabel, oft auch als Thin Ethernet oder Koax bezeichnet.

Checksum

Prüfsumme

CIDR

Classless Interdomain Routing, Standard seit 1995, bei dem für das Routing nicht mehr Netzmasken, sondern mit der Prefix-Notation die Anzahl der Bit für das Netzwerk angegeben werden. Beispiel: 192.168.1.0 Netzmaske 255.255.255.0 entspricht 192.168.1/24.

Circuit Level Gateway

Als *Proxy* arbeitendes Gateway mit Filtermechanismus, das die über das Gateway übertragenen Daten auf den Schichten 4 bis 6 untersucht.

Classful Addressing

Nutzung der Aufteilung des IP-Adreßraums in verschiedene Klassen (bis Ende 1994 einzige Aufteilung: Class A, B, C).

Client

Computer, der von einem anderen Rechner oder *Server* Dienste in Anspruch nimmt und Antworten dieser Maschine akzeptiert.

Client Authentisierung

IP-basierte Authentisierung von Benutzern durch Next Generation für alle Dienste. Meist muß hierzu eine eigene Verbindung zum Gateway über 259/tcp oder 900/tcp aufgebaut werden.

Client Encryption

Bei Check Point VPN-1 Aufbau eines *VPN* vom SecuRemote beziehungsweise SecureClient zur Firewall mit Authentisierung des Benutzers.

CLM

Customer Log Module, „verkleinertes“ Management-Modul bei Check Point, das lediglich für die Entgegennahme und Auswertung von Logs zuständig ist.

CLNP

Connectionless Network Protocol.

CNAME

Canonical Host Name. Im DNS eingetragener Hauptname – im Gegensatz zu Alias-Namen.

Connect-Control Modul

Optionales Modul von Next Generation, mit der für HTTP- und andere Server Load-Balancing eingerichtet werden kann.

CRC

Cyclic Redundancy Check: Prüfsummenverfahren, das häufig für Dateien auf FTP Servern angewendet wird und nicht kollisionsfrei ist.

CSLIP

Compressed Serial Line IP.

CSMA/CD

Carrier Sense and Multiple Access with Collision Detection, bei Ethernet eingesetzter Mechanismus für den Transport von Paketen über das Netzwerk.

CVP

Content Vectoring Protocol, 18181/tcp, genutzt von Next Generation zur Kommunikation mit Anti-Virus-Servern. Wird von allen gängigen AV-Herstellern und inzwischen auch anderen Firewalls unterstützt.

Daemon

Prozeß auf einer Maschine, der auf eingehende Verbindungen wartet. Bei Next Generation wird diese die Kommunikation zwischen Modulen, Clients und Hosts vorgenommen.

DAIP

Dynamically Assigned IP-Address for Firewall, bei Check Point NG eine Bezeichnung für eine Firewall, die ihre IP-Adresse dynamisch bezieht.

Datagramm

Datenpaket in einem Netzwerk, das mit der Übertragung einzelner Pakete arbeitet (Paketvermittlungsnetz).

Datenpaket

Teil von elektronischen Daten, der ein Teil des *Datenstroms* darstellt, oft auch nur Paket oder *Datagramm* genannt.

Datenstrom

Bei der Übertragung von Daten über beispielsweise TCP werden diese in Form eines Stroms übertragen, der zur Übertragung über das Netzwerk in einzelne *Datenpakete* zerlegt wird.

DBMS

Database Management System

DC

Microsoft Windows Domain Controller

DDN

Defense Data Network

Denial-of-Service

DoS, Sabotieren eines Dienstes, Servers oder eines ganzen Netzwerkes, beispielsweise durch illegale Pakete (beispielsweise *Ping Of Death*) oder *SYN-Flooding*.

DENIC

Deutsches *NIC*, technischer Betrieb in Karlsruhe, zuständig für *Toplevel-Domain* de.

DENIC eG

In Frankfurt ansässige Genossenschaft, in der Provider Mitglied sind. Von der eG wird das technische *DENIC* betrieben.

DES

Data Encryption Standard aus den USA, Verschlüsselungsalgorithmus mit 56 Bit (40 Bit Länge), siehe auch *Triple-DES*.

DF

Don't Fragment Flag, Einstellung im IP-Header von Paketen, die Routern anzeigt, daß dieses Paket nicht fragmentiert werden darf.

DHCP

Dynamic Host Configuration Protocol für die dynamische Vergabe von IP-Adressen an beispielsweise Arbeitsplatzrechner.

Distinguished Name

Vollständiger Name nach X.500, in dem die Hierarchie bis zur Root enthalten ist. Notwendig z.B. bei *LDAP*.

Distributed Denial-of-Service

DDoS, konzentrierter *DoS*-Angriff unterschiedlicher Rechner auf ein Ziel.

DMA

Direct Memory Access.

DN

Distinguished Name

DNS

Domain Name System, im Internet der Standard für die Auflösung von Namen in IP-Adressen und umgekehrt. Nutzt meist 53/udp für Anfragen/Antworten und 53/tcp für Zonentransfers zwischen *Nameservern*. Meist implementiert durch den *BIND*.

DoD

Department of Defense, US-amerikanisches Verteidigungsministerium.

Domain

Namensraum, eigene Verantwortlichkeit für untergeordnete Teile. Unterscheidung zwischen Root Domain, *Top-Level Domains* und Second-Level Domains.

DoS

siehe *Denial-of-Service*

DDoS

siehe *Distributed Denial-of-Service*

Drop-Cable

Verbindung zwischen Daten-Endeinrichtung und dem Netzwerk-Kabel.

DSAP

Destination Service Access Point, im *SNAP* die Typenbezeichnung der Nutzdaten des verschickten *Frames* zum De-/Multiplexing im Schichtenmodell.

Dynamic NAT

Sofern viele IP-Adressen auf eine einzige abgebildet werden, handelt es sich um den sog. *Hide-Mode*, der inzwischen oft auch Dynamic NAT genannt wird.

E-Mail

Electronic Mail

EBONE

European IP Backbone, von verschiedenen Providern gemeinsam betriebener Internet-Backbone durch ganz Europa.

EGP

Exterior Gateway Protocol, im Internet verwendetes dynamisches Routing-Protokoll.

Eitherbound

Untersuchung übertragener Daten an einem Gateway in beiden Richtungen, das heißt, auf jedem Interface (*Inbound* und *Outbound*) wird die Untersuchung durchgeführt.

Encapsulation

siehe auch *Tunneling*, beispielsweise bei Verschlüsselungsverfahren wird das gesamte Paket verschlüsselt und mit neuen Headern versehen, Anwendung u.a. bei *IPsec*.

Encryption

Verschlüsselung von Daten.

Encryption Modul

Optionales Modul der FireWall-1, mit dem die Verschlüsselung von Daten vorgenommen werden kann – hierdurch wird dann die FireWall-1 zur VPN-1.

Enterprise Version

Lizenzierung einer Check Point FireWall-1/VPN-1 in unlimitierter Version, das heißt, die Anzahl der durch dieses Gateway geschützten IP-Adressen ist nicht beschränkt und die Trennung von Management-Modul und Firewall ist möglich.

Explizite Regel

Regel, die in Next Generation explizit über die Regelbasis eingegeben wird.

FCS

Frame Check Sequence.

FDDI

Fiber Distributed Data Interface, Verkabelungsstandard für Glasfaserkabel.

FIFO

First in, first out, eine Arbeitsmethode eines Rechners, die ersten Daten werden zuerst verarbeitet – also in der Reihenfolge, wie sie ankommen.

FIN

Finish Flag, ist beim regulären Verbindungsabbau von TCP-Verbindungen gesetzt.

Firewall-Modul

Version der *Inspect-Engine* einer FireWall-1/VPN-1, wodurch die Security Policy, Log-Ereignisse und die Kommunikation mit dem Management-Modul durchgeführt wird. Das Firewall-Modul ist die erweiterte Version des Inspektions-Moduls und unterstützt auch Benutzerauthentisierung, Synchronisation mehrerer Firewalls und Content Control.

FQDN

Fully Qualified Domain Name, vollständiger Name innerhalb des *DNS*, abschließend mit ».«.

FTP

File Transfer Protocol, 21/tcp für Kontrollverbindungen, 20/tcp für Datenverbindungen, sehr weit verbreitetes Protokoll zur Dateiübertragung, arbeitet mit mehreren Verbindungen.

FWD

Firewall-Daemon der Check Point FireWall-1/VPN-1, unter anderem zuständig für die Kommunikation zwischen dem *Management-Modul* und der *Inspect-Engine.*

FWM

Management Server der Check Point FireWall-1/VPN-1, zuständig für das Management der Datenbanken, Regelsätze, Netzwerkobjekte, Server, Benutzer etc.

FWZ

Proprietäres Verschlüsselungsprotokoll von Check Point. Benutzt entweder DES oder FWZ-1 als symmetrische Verschlüsselungsalgorithmen. Wird seit Next Generation Feature Pack 2 nicht mehr unterstützt.

FWZ-1

Proprietärer, symmetrischer Verschlüsselungsalgorithmus von Check Point, der bis Next Generation Feature Pack 1 unterstützt wurde.

FYI

For Your Information, englische »Kurzfloskel«, die »für Sie zur Information« bedeutet.

GOSIP

Government OSI Profile.

HDLC

High-Level Data Link Control, beim ISDN genutztes Protokoll.

HELLO

Dynamisches Distance/Vector-Routingprotokoll, heute nur noch sehr selten eingesetzt.

Hide-Mode

Übersetzung vieler IP-Adressen auf eine einzige (siehe auch *NAT*, *PAT*).

HTTP

Hypertext Transfer Protocol, (80/tcp) im Web verwendet.

Hub

Zentraler Verteiler in einem Sternnetz auf unterster Ebene (physikalisch), Unterscheidung zwischen passiven und aktiven Hubs.

Hz

Hertz, Einheit für Frequenzen.

IAB

Internet Architecture Board, Gremium im Internet.

IANA

Internet Assigned Number Authority, Gremium im Internet.

ICA

Internal *Certificate Authority*, seit Next Generation arbeitet das Management-Modul in der *SIC* grundsätzlich als CA, die entsprechend bezeichnet wird. Sie ist auch für die Authentisierung im *IKE* einsetzbar.

ICMP

Internet Control Message Protocol, Hilfsprotokoll für das *IP*.

IDEA

International Data Encryption Algorithm, symmetrischer Verschlüsselungsalgorithmus aus der Schweiz mit 128 Bit Länge, von Check Point Next Generation nicht unterstützt.

IEEE

Institute of Electrical and Electronics Engineers, Standardisierungsbehörde in den USA, deren Standards meist weltweit geltend sind.

IEEE 802

Ein Standard der IEEE.

802.2	Logical Link Control
802.3	Bustopologien (10Base2, 10Base5, 10BaseT, ...)
802.4	Token Passing, Bus-Topologie
802.5	Token-Ring
802.11(b)	WLAN

IEN

Internet Experiment Notes

IETF

Internet Engineering Task Force. Arbeitsgruppe, die unter anderem für Standardisierungen im Internet zuständig ist.

IKE

Internet Key Exchange, Verschlüsselungsstandard der IETF. Verwendung von *IPsec*, s.a. *ISAKMP/Oakley*.

IGMP

Internet Group Management Protocol, im Internet verwendetes Routing-Protokoll.

IMAP

Interactive Mail Access Protocol, Protokoll zum Abholen von E-Mail von unterschiedlichen Servern.

Implizite Regel

Regel der FireWall-1, die nicht über den Regelbasiseditor, sondern über dessen Grundeinstellungen (Properties) angelegt wird. Auch »Pseudo-Regel« genannt.

Implizite Drop-Regel

Regel der FireWall-1/VPN-1, die automatisch als abschließende Regel an den bestehenden Regelsatz angefügt ist. Durch diese Regel wird alles, was vorher durch die Regelbasis nicht explizit genannt wurde, fallengelassen.

In-Place Verschlüsselung

Verschlüsselungsmethode, bei der nur der Datenteil der Originalpakete verschlüsselt wird. Die Header der Pakete bleiben original. Siehe auch *FWZ*.

Inbound

Untersuchung von Paketen am ersten, eingehenden Interface der Firewall oder des Routers.

INSPECT

Skriptsprache von Check Point, in der beispielsweise sämtliche Regeln der FireWall-1/VPN-1 formuliert und abgesichert werden.

Inspect-Engine

Ein Teil der FireWall-1/VPN-1, der als Kernel-Attachment auf dem Gateway zwischen den Schichten 2 und 3 installiert wird. Durch sie wird hier die Sicherheit erreicht. Sie muß zusammen mit anderen Teilen der FireWall-1/VPN-1 installiert sein. Am Gateway ist entweder das *Firewall-Modul* oder das *Inspektions-Modul* installiert.

Inspektions-Modul

Teil der FireWall-1, durch den die Security Policy an einem Gateway umgesetzt wird. Es besteht aus der Inspect-Engine, dem *FWD* und den *Security Servern*. Unterstützt dazu die *Stateful Inspection*, *Client-* und *Session-Authentisierung*, *NAT* und Logging.

Inspection Script

ASCII-Datei, das von der Security Policy der FireWall-1 in der Sprache INSPECT generiert wird.

Interface

Allgemeine Bezeichnung für Schnittstelle, in diesem Buch oft als Netzwerk-Interface gemeint.

Internet

Weltweite Verknüpfung verschiedenster Netzwerke, bei denen überall *TCP/IP* als Netzwerkprotokoll eingesetzt wird.

InterNIC

Oberstes *NIC*, USA, Verwaltung der Toplevel-Domains com, edu, gov, mil, net, org und IP-Adressen, Delegation anderer Domains an nationale *NIC*. Noch vor nicht allzu langer Zeit wurde die Aufgabe lediglich von der Firma Networksolutions wahrgenommen. Inzwischen ist dieses Monopol abgeschafft und es gibt mehrere Registries für diese Toplevel-Domains.

IP

Internet Protocol, arbeitet auf Schicht 3 im ISO/OSI-Schichtenmodell und ist zuständig für die korrekte Auslieferung von Paketen an die richtige Zielmaschine.

IP-Adresse

Logische Adresse im IP. Verbreitet ist heute IP-Version 4 mit 32-Bit-Adressen. Version 6 hat eine Adreßlänge von 128 Bit. In V4 wird die IP-Adresse in vier punktseparierten Oktetten dargestellt, beispielsweise 192.168.154.15.

IP Address Translation

Übersetzung von IP-Adressen, genau genommen der Austausch von Absender- oder Zieladresse im IP-Header, oft auch NAT genannt.

IPsec

Oft auch als IPsec geschrieben. IP Security Protocol, standardisiert von der *IETF* in den *RFC*s 2401 und folgenden.

IPX

Internetworking Packet Exchange, unter Novell verwendetes Protokoll in der Netzwerkschicht, auf TCP/IP übertragen dem Internet-Protokoll IP entsprechend.

IRTF

Internet Research Task Force, Arbeitsgruppe der *IETF*.

IS-IS

Intermediate System to Intermediate System Protocol. Ein Routing-Protokoll auf Distance/Vector-Basis.

ISAKMP

Internet Security Association and Key Management Protocol, Anwendung dieses Protokolls im Verschlüsselungsstandard IPsec.

ISAKMP/Oakley

Verschlüsselungs-Standard zum Schlüsselmanagement zwischen zwei Servern, die *IPsec* benutzen. Dieser Standard ist durch die *RFC*s 2401 ff. standardisiert.

ISDN

Integrated Services Digital Network, in Deutschland weit verbreiteter Telekommunikationsstandard.

ISN

Initial Sequence Number, die erste, beim TCP-Verbindungsaufbau ausgetauschte Sequenznummer.

ISO

International Organization for Standardization, internationale Standardisierungsorganisation.

ISP

Internet Service Provider, Anbieter von Internet-Anbindungen und meist auch Mehrwertdiensten.

Kernel

Essentieller Teil von Unix und anderen Betriebssystemen, der für Ressourcen, Low-Level-Hardware-Interfaces und Sicherheit zuständig ist.

L2TP

Layer 2 Tunneling Protocol, Verschlüsselungsprotokoll für Schicht 2, eingesetzt bei Systemen unter Microsoft Windows. Hiermit kann ein VPN zu Check Point NG seit Feature Pack 3 aufgebaut werden.

LAN

Local Area Network, lokales Netzwerk, beispielsweise innerhalb einer Abteilung.

LCP

Link Control Protocol, Steuerprotokoll des *PPP*.

LDAP

Lightweight Directory Access Protocol zur zentralen Benutzerverwaltung auf LDAP-Servern, benutzt unverschlüsselt Port 389/tcp, mit *SSL*-Verschlüsselung Port 636/tcp.

LDAP Account Units

Integration von *LDAP*-kompatiblen Benutzerdatenbanken zur Authentisierung durch Next Generation.

LHTTPD

Load-Balancing Daemon der FireWall-1, der für das Verteilen von Anfragen beim *Load Balancing* zuständig ist.

LIFO

Last in, first out, eine Arbeitsmethode eines Rechners, die neuesten Daten werden zuerst bearbeitet.

LLC

Logical Link Control, obere Hälfte der Data Link Schicht im IEEE-Ethernet-Modell. Stellt eine einheitliche Schnittstelle der Data-Link-Ebene höheren Schichten zur Verfügung (IEEE 802.2).

Load Balancing

Mechanismus zum Verteilen von Anfragen auf mehrere gespiegelte Server.

Log Viewer

Teil der FireWall-1, in dem Ereignisse und Alarme der Regelbasis kontrollierbar sind. Seit Next Generation Feature Pack 3 SmartView Tracker genannt.

Logischer Server

Bei Next Generation eine Gruppe gespiegelter Maschinen, die nach außen wie ein *Server* erscheinen, wird eingesetzt beim *Load Balancing* durch die Firewall.

MAC

Media Access Control, medienabhängige untere Hälfte des Data Link Layers im IEEE Ethernet (gesamter Data Link Layer in anderen Ethernetstandards). Häufig auch als Bezeichnung für die physikalische Adresse eines Netzwerk-Interfaces verwendet.

Mail Transport Agent

Meist kurz *MTA* genanntes Programm, das für die Weiterleitung von E-Mail über das Internet per SMTP zu Port 25/tcp des nächsten Mail-Servers zuständig ist.

Management Modul

Teil der FireWall-1/VPN-1, der die »zentrale Verwaltung« der Firewall darstellt. Seit Next Generation Feature Pack 3 in der unlimitierten Version SmartCenter bzw. Smart Center Pro genannt.

Management Server

Teil der FireWall-1/VPN-1, FWM, ist zuständig für das Management von Next Generation: Datenbanken-Regelbasis, Netzwerkobjekte, Server, Benutzer, etc.

Manual IPsec

Standardisiertes Verschlüsselungs- und Authentisierungsschema, bei dem feste Schlüssel verwendet werden und die Verwaltung dieser Schlüssel grundsätzlich durch die Administratoren von Hand erfolgt. Dieses Verschlüsselungsprotokoll war bisher oft die Rettung, wenn andere Protokolle zwischen VPN-Endpunkten unterschiedlicher Hersteller nicht funktionierten – mit Einführung der Version Next Generation unterstützt Check Point dieses Protokoll nicht mehr.

Master

Für eine oder mehrere *Zonen* zuständiger *Nameserver*, dessen Zonendaten der Administrator selbst in Dateien pflegt. Ein Master Server ist also die »Schnittstelle« zwischen dem Administrator und dem Domain Name System.

MBONE

Multicast *Backbone*.

MAN

Metropolitan Area Network, Größenbeschreibung für ein Netzwerk in »Städtegröße«.

MAU

Multistation Access Unit, im Token-Ring (802.5) verwendeter Konzentrationspunkt (vgl. Hub), der mehrere Computer an den Ring der Netztopologie anbindet.

MHS

Message Handling System.

MIB

Management Information Base, für das Netzwerkmanagement genutzte Datenbasis mit den entsprechenden Parametern der überwachten Maschinen.

MILNET

Military Network, militärischer Teil des Vorgängers vom *Internet*.

MIME

Multipurpose Internet Mail Extensions, Standard zur Codierung von Binärcode, der durch E-Mail übertragen wird.

MSS

Maximum Segment Size, maximale Größe eines Segments.

MTA

Mail Transport Agent, für den Transport von E-Mail über das Internet, aber auch im Intranet, eingesetzte Mailprogramme. Sie nutzen das Protokoll *SMTP*. Beispiele hierfür sind sendmail, qmail oder aber auch andere, kommerzielle Anwendungen wie Exchange.

MTU

Maximum Transfer Unit, maximale Größe eines Pakets, das als ganzes über ein Netzwerk übertragbar ist. Diese Größe ist auch vom Netzwerktyp (beispielsweise Ethernet, Token Ring) abhängig.

Multicast

Gruppenadresse. Nachricht, die von einer Maschine an verschiedene andere ausgewählte Maschinen gesendet wird.

MX

Mail Exchanger, Eintrag von Mailservern im Nameservice für die Auslieferung von Mail an Benutzer in einer *Zone*, auch meist als Domain bezeichnet (beispielsweise an username@*aerasec.de*).

NACK

Mitteilung innerhalb des genutzten Protokolls, daß diese Aktion nicht gestattet ist.

NASL

Nessus Attack Scripting Language, Sprache zur Konfiguration und Einrichtung von Nessus zur Durchführung technischer Security Audits.

Nameserver

Server zur Umsetzung von Namen zu IP-Adressen und umgekehrt, im Internet hauptsächliche Nutzung des *BIND* im Domain Name System, *DNS*.

NAT

Network Address Translation, Austausch von IP-Adressen (Absender- oder Zieladresse) an einem Gateway oder Router.

NCP

Network Control Protocol, im PPP zwischen Authentisierung und Nutzprotokoll (beispielsweise IP) ansässige Klasse von Enkapsulations- und Steuerprotokollen (beispielsweise IPCP für IP).

NDIS

Network Driver Interface Specification, Verwendung meist in Novell-Netzwerken.

NetBEUI

NetBIOS Extended User Interface, genutzt von Microsoft Windows 9x und NT.

NetBIOS

Network Basic Input/Output System, genutzt von Microsoft Windows 9x und NT.

Netzwerkobjekt

Bei Next Generation Beschreibung von Elementen wie beispielsweise einzelner Rechner, Router, Netzwerke, Gateways, Switches, Domains, logische Server.

Netzwerkobjekt-Manager, NOM

Tool, mit dem bei Next Generation die *Netzwerkobjekte* deklariert und verwaltet werden.

NFS

Network File System, hauptsächlich unter Unix verbreitetes Protokoll für den Zugriff auf Laufwerke über das Netzwerk.

NG

Kurzform für Check Point Next Generation.

NIC

Network Information Center, zuständig für die Vergabe von Second-Level Domains unterhalb der jeweiligen Toplevel-Domain.

NIS

Network Information System, Protokoll zur Synchronisation von Benutzerdatenbanken und anderen Kontrollinformationen zwischen Unix-Servern.

NMS

Network Management System, Einsatz für das Management größerer Netzwerke. Beispiele für NMS sind HP OpenView oder Tivoli.

NNTP

Network News Transfer Protocol, im UseNet eingesetztes Protokoll des Internet, mit dem Postings von NewsGroups übertragen werden.

NSFNET

National Science Foundation Network, frühe Organisation zur Organisation des Internet.

NT

Network Terminator

New Technology

NTP

Network Time Protocol, auf UDP Port 123 basierendes, komplexes Protokoll zur Synchronisation der Systemzeit mit mehreren Referenzrechnern.

NVT

Network Virtual Terminal.

Oakley

Internet-Verschlüsselungsprotokoll, das zwei authentisierten Partnern sichere und geheime Übertragung gestattet. Die Verschlüsselung ist mit *ISAKMP* kompatibel und nach Hilarie Orman benannt.

Octet

Neben Byte auch oft genutzte Bezeichnung für eine 8-Bit-Einheit.

ODI

Open Datalink Interface, notwendig dann, wenn mehrere Netzwerk-Protokolle auf einem System parallel eingesetzt werden sollen.

OOB

Out of Band, Flag für wichtige Nachrichten an Systeme, auch genutzt für *DoS*-Angriffe gegen Systeme unter Windows NT, die SP3 nicht installiert haben: Durch den Empfang eines einzigen OOB-Paketes wird diesem die volle »Aufmerksamkeit des NT« geschenkt – und es kommen keine weiteren Informationen. Das Ergebnis: Windows NT ist nicht mehr ansprechbar.

OPSEC

Open Platform for Secure Enterprise Connectivity. Von Check Point gegründetes Forum, das die Kompatibilität von Drittthersteller-Produkten mit der FireWall-1 sicherstellt.

OSI

Open Systems Interconnections, 1983 von Day und Zimmermann entworfenes Referenzmodell für Kommunikation zwischen zwei Einheiten. Wird häufig als Modell für TCP/IP, aber auch für andere Protokollfamilien (beispielsweise IPX/SPX) verwendet.

OSPF

Open Shortest Path First, Protokoll für dynamisches Routing, das auf Link-State Basis funktioniert und eine schnelle Konvergenz bei minimaler Netzbenutzung zur Verfügung stellt.

Outbound

Untersuchung von Paketen am letzten, ausgehenden Interface der Firewall.

Paketfilter

Meist auf Routern vorgesehene Filterung der Pakete eines Datenstroms nach IP-Adressen und Ports. Paketfilter arbeiten auf Schicht 3.

PAT (Port Address Translation)

Austausch von Ports in Verbindung mit *NAT*, notwendig beispielsweise beim Hide-Mode der VPN-1/FireWall-1.

Persistent Server Mode

Beim Einsatz von *Load Balancing* wird hier nach dem Verbindungsaufbau des Clients zu einem Server innerhalb einer Session immer wieder der gleiche Server angesprochen, ohne weitere Berücksichtigung der Lastverteilungs-Regeln.

PFS

Perfect Forward Secrecy, unter anderem im IKE verwendete Option, daß bei einem Schlüsselwechsel in einem VPN aus der Vergangenheit nicht auf zukünftige Schlüssel geschlossen werden kann – Phase Eins wird immer parallel zu Phase Zwei durchlaufen.

Ping

Absenden eines *ICMP* Echo Requests, (ICMP Typ 8, Code 0), das angepingte System antwortet mit einem *ICMP* Echo Reply (ICMP Typ 0, Code 0).

Ping Of Death

Illegale Paketgröße für Ping-Pakete, der Empfang eines PoD kann einen Systemabsturz verursachen, sofern das System die resultierende Paketgröße nicht vor der Annahme überprüft.

PKI

Public-Key Infrastructure.

POP

Post Office Protocol, neben IMAP ein Protokoll zum Abholen von elektronischer Mail von Servern zur lokalen Ansicht beziehungsweise Bearbeitung (110/tcp).

PPP

Point-to-Point Protocol, speziell für die Einwahl in das Internet von PCs genutzt. Ersetzt SLIP und bietet die Möglichkeit, etliche Kommunikationsprotokolle (beispielsweise IP) zu enkapsulieren.

PPTP

Point-to-Point-Tunneling Protocol, Protokoll zur Verschlüsselung in Schicht 2, zum Teil stark vom Hersteller abhängig.

Primary Nameserver

Für eine oder mehrere *Zonen* zuständiger *Nameserver*, der seine Daten aus Konfigurationsdateien liest, eingesetzt in *BIND* 4.x.

Proxy

»Strohmannsystem«, Benutzer richten Anfragen an den Proxy und dieser holt dann für die Benutzer die gewünschten Daten aus dem externen Netzwerk.

Pseudo-Regel

Regel innerhalb von Next Generation, die nicht über den Regelbasiseditor, sondern über die Grundeinstellungen (Policy > Global Properties) angelegt wird. Auch *implizite Regel* genannt.

PSH

Push Flag, Flag im TCP-Header, durch das angekommene Pakete direkt ohne Rücksicht auf die Reihenfolge an die Applikation weitergegeben werden.

Public-Key Infrastruktur

System zur Verwaltung und Verteilung digitaler Zertifikate beziehungsweise öffentlicher Schlüssel, das durch *Certificate Authorities* und *Registration Authorities* verwaltet wird.

Public-Key Verfahren

Asymmetrische Verschlüsselungsverfahren

RADIUS

Remote Dial-In User Service, standardisiertes Protokoll zur zentralen Authentisierung von Benutzern.

RA

Registration Authority, Stelle, bei der für eine *CA* die Daten entgegengenommen und überprüft werden, sozusagen Registrierungsstelle für einen *Trust Center*.

RARP

Reverse Address Resolution Protocol, proprietäres Protokoll für die Herstellung einer Verbindung zwischen einer MAC- und IP-Adresse. Wird heutzutage durch BOOTP ersetzt.

Registration Authority

Registrierungsstelle öffentlicher Schlüssel, die auch Zertifikate ausgeben kann. Sie arbeitet mit *Certificate Authorities* zusammen.

Repeater

Signalverstärker im Netzwerk ohne Routing- oder Filterfunktionalität, das heißt, auf physikalischer Ebene.

Resolver

Clientprogramm, das *DNS*-Anfragen der lokalen Maschine an einen oder mehrere *Nameserver* weiterleitet und dem Benutzer die Möglichkeit gibt, mit Namen und nicht nur IP-Adressen zu arbeiten.

Ressource

Innerhalb von Next Generation bestehende Möglichkeit, für die Protokolle HTTP, FTP und SMTP auch in der Applikationsschicht Kontrollen beziehungsweise Modifikationen durchzuführen.

RDP

Reliable Datagram Protocol, 259/udp. Proprietäres Protokoll von Check Point zur Schlüsselverwaltung im Protokoll *FWZ* und zur Kontrolle der Verfügbarkeit von Gateways durch Clients – nicht zu verwechseln mit dem Protokoll gleichen Namens von Microsoft.

Referral

Antwort eines Nameservers, der wie beispielsweise ein Root-Nameserver nicht für einzelne Zonen zuständig ist, auf der ein anfragender Client nähere Informationen findet.

RFC

Request for Comments, Festlegung der Standards des Internet.

RIP

Routing Information Protocol, 520/udp, Protokoll für dynamisches Routing.

RIPE

Réseaux IP Européens, Verwaltung und Administration des Internet in Europa (beispielsweise Verwaltung von IP-Adressen).

Root-Domain

Im Nameservice die oberste Domain innerhalb der Baumstruktur, die mit einem ».« beschrieben wird.

Root-Server

Für die Toplevel-Domains zuständige *Nameserver*, die normalerweise nur *Referrals* an die anfragenden Nameserver zurücksenden, also keine eigenen Daten haben.

Routing

Verbindung verschiedener logischer Netzwerke, genau genommen die Weiterleitung von Paketen über Netzwerkgrenzen hinweg.

Router

Maschine mit mehreren Netzwerkinterfaces in verschiedenen Netzwerken, die für die Weiterleitung von Paketen zwischen diesen Netzwerken zuständig ist. Meist haben Router lediglich die unteren drei Schichten des ISO/OSI-Schichtenmodells implementiert, eine Untersuchung von Daten in der Applikationsebene ist nicht möglich.

ROBO

Kurzform von Check Point für Remote Office, Branch Office. Diese Lösungen runden das Spektrum von Next Generation nach unten ab.

RPC

Remote Procedure Call, zur Ausführung von Programmen auf einem Server.

RR

Resource Record, Datei mit den autoritativen Zonendaten eines *Nameservers*.

RST

Reset Flag, Flag im TCP-Header, dient dem »kalten Zurücksetzen« einer TCP-Verbindung.

RTO

Retransmission Timeout.

RTT

Round-Trip Time, Zeit, die ein Frage/Antwort-Paket benötigt, um wieder beim Absendersystem anzukommen.

SAM

Suspicious Activity Monitoring, direkte Sperrung bestehender, verdächtiger Verbindungen.

SCSI

Small Computer System Interface, auf Bus-Topologie beruhendes rechnerinternes Schnittstellensystem, das für hohe Übertragungsraten und Ausfallsicherheit bekannt ist.

SCV

Secure Configuration Verification, Konfiguration für den *SecureClient*, durch die neben dem Regelsatz auch Prozesse auf dem Client sowie die Version von Software und Virenmustern zu überwachen ist.

SDLC

Synchronous Data Link Control.

Second-Level Domain

Unterhalb einer Top-Level Domain registrierte Domain, beispielsweise »aerasec.de«.

Secondary Nameserver

Für eine oder mehrere *Domains* beziehungsweise *Zonen* zuständiger und als *Slave* arbeitender *Nameserver*, der seine Daten vom *Primary Nameserver* (*Master*) holt. Der Name bezieht sich streng genommen auf BIND 4.x, wird aber auch heute noch oft verwendet.

Secure Socket Layer

Von Netscape entwickeltes Verschlüsselungsprotokoll zur Enkapsulierung und resultierender Absicherung anderer Protokolle (beispielsweise IP), basierend auf dem Schlüsselaustauschverfahren von Diffie-Hellman. Weit verbreitet für sichere Transaktionen im WWW.

Secure Platform

Von Check Point herausgegebenen Linux Distribution, die auf Red Hat Linux basiert. Diese ist einerseits abgesichert, andererseits für den Einsatz von Next Generation optimiert.

SecureServer

Einsatz eines Inspektions-Moduls, das nur eine einzige Maschine schützt und nicht als Gateway arbeiten kann. Er setzt ein Management-Modul voraus, das in der Enterprise-Version arbeitet.

SecuRemote

Bei VPN-1eingesetzter Client zum Aufbau eines *VPN* vom Client-PC zur Firewall.

SecureClient

Bezüglich der VPN-Funktionalität wie *SecuRemote*, aber mit einer zusätzlichen Firewall auf dem Client, damit dieser nicht für Unbefugte als Gateway in das Unternehmensnetzwerk nutzbar ist.

Security Association

Kurz »SA«. Vollständige Beschreibung der verwendeten Verschlüsselungsparameter bei *IPsec* und *ISAKMP*. Diese enthält das Verschlüsselungsverfahren, den eingesetzten Schlüssel, das Hashverfahren und den Hashwert. Ein SPI zeigt jeweils auf eine SA.

Security Policy

Gesamtheit aller Regeln, die Sicherheitsanforderungen einer Institution beschreiben, nicht nur auf die technische Ebene beschränkt.

Security Server

Teil der Next Generation, wird eingesetzt oberhalb der Inspect-Engine im FireWall-1 Kernel-Modul zur Authentisierung und Inhaltskontrolle (als transparenter *Proxy* arbeitend).

Segment

Zusammenhängendes Kabelstück in einem Netzwerk.

Server

Maschine, die anderen Rechnern beziehungsweise *Clients* Dienste zur Verfügung stellt.

Session Authentication

Komfortable Methode zur Benutzerauthentisierung bei Next Generation, die für alle Dienste einsetzbar ist. Sie setzt voraus, daß ein *Session Authentication Agent* auf dem Client (beispielsweise Arbeitsplatz-PC unter Windows) installiert ist.

Session Authentication Agent

Client-Programm, das vom Security Server der FireWall-1 zur Authentisierung von Benutzern angesprochen wird. Dieser Agent läuft nur unter Microsoft Windows und bietet innerhalb der FireWall-1 eine sehr komfortable Methode, Benutzer für alle Dienste zu authentisieren.

SIC

Secure Internal Communication, zertifikatsbasierte Kommunikation der Komponenten von Next Generation über *SSL*. Die Gesamtheit der Kommunikation wird auch als *SVN* bezeichnet.

Single Gateway

Einsatz der Check Point FireWall-1/VPN-1 für eine begrenzte Anzahl interner IP-Adressen. Eine Trennung zwischen Management- und Inspektions-Modul ist bei dieser Lizenz nicht möglich.

SKIP

Simple Key Management for Internet Protocols, von Sun Microsystems entwickeltes Verschlüsselungsprotokoll, das mit einem Zeitstempel im Paket-Header arbeitet. Dieses Protokoll wird seit Next Generation Feature Pack 1 nicht mehr unterstützt.

Slave

Nameserver, der vom Master die aktuellen Zonendaten in regelmäßigen Abständen holt und über diese Zone autoritative Auskunft geben kann.

Früher: Ein als Forward-Only eingerichteter Nameserver, der selbst keine Anfragen in das Internet richten kann, weil er beispielsweise die Root-Server nicht erreicht. Die Anfragen laufen einzig über den bei diesem Nameserver eingetragenen Forwarder, der die gewünschten Daten aus dem Internet holt und dem Slave die zum angefragten Namen gehörende IP-Adresse liefert.

SMART

Seit Next Generation Feature Pack 3 ist “alles SMART”. Hierbei ist dieses eine Abkürzung für *S*ecurity *M*anagement *AR*chi*T*ecture, über die alle Programme von Check Point miteinander kommunizieren und zusammenarbeiten können.

SmartConsole

Mit NG AI neu eingeführter Begriff für den SmartDesktop. Insgesamt wird hierunter die Gesamtheit der GUI-Clients verstanden.

SmartMap

siehe *Visual Policy Editor*.

SMTP

Simple Mail Transfer Protocol, 25/tcp, von Mail Transport Agents (*MTA*) genutzt für die Auslieferung von *E-Mail* an den empfangenden Mailserver.

SNA

Systems Network Architecture, innerhalb der »Hostwelt« verwendetes Protokoll für das Ansprechen des Hosts über Terminals beziehungsweise Terminalemulationen. Das *Tunneln* dieses Protokolls über TCP/IP wird heute häufig vorgenommen.

Sniffing

Abhören von Datenpaketen innerhalb des gleichen Segments, obwohl sie nicht an die eigene Maschine gerichtet sind.

SNMP

Simple Network Management Protocol, für das Netzwerkmanagement eingesetztes Protokoll (161/udp) zum Abrufen von Daten einzelner Server durch das NMS. Für SNMP Traps wird 162/udp eingesetzt.

SOA

Start of Authority, Startzeile für die *RR* eines *Nameservers*, in der unter anderem die *Domain*, Kontakte und Timings für die *Slave Nameserver (Secondary Nameserver)* festgelegt wird.

SPI

Security Parameters Index: Eine 32-Bit-Zahl, die auf eine *Security Asscociation* (SA) zeigt. Anwendung des SPI bei der Verschlüsselung nach *IPsec*.

Spoofing

Vortäuschen falscher Tatsachen, die eine Fehlreaktion verursachen sollen. Beispiele: IP-Spoofing (Fälschen der IP-Absenderadresse), DNS Spoofing (Fälschungen im Nameservice), Web Spoofing (Nachbau von Web-Servern), E-Mail Spoofing (Fälschen von E-Mails).

SPX

Sequenced Packet Exchange, unter Novell verwendetes Protokoll in der Transportschicht, auf TCP/IP übertragen dem TCP beziehungsweise UDP entsprechend.

SSL

Secure Socket Layer, heute noch sehr weit verbreitete zur Übertragung verschlüsselter Daten von einem Web-Server zum Browser, eigentlich ein Satz von Bibliotheksfunktionen, die sowohl vom Server als auch vom Client eingesetzt werden.

SSAP

Source Service Access Point, im *SNAP* die Typenbezeichnung der Nutzdaten des verschickten *Frames* zum De-/Multiplexing im Schichtenmodell.

Stateful Inspection

Von Check Point entwickelte Firewall-Architektur, die unterhalb der Netzwerkschicht ansetzt. Sie arbeitet als Kernelprozeß direkt zwischen dem Netzwerk-Interface und der Netzwerkschicht. Dadurch kann beispielsweise eine hohe Performance erreicht werden. Zusätzlich erfolgt eine Kontrolle der States, das heißt, auch die Verbindungsparameter sind gespeichert. Die Bewertung der Pakete kann auch in den höheren Schichten erfolgen, wobei die volle Kontrolle aller Protokolle in Schicht 7 allerdings nicht möglich ist. Check Point spricht an dieser Stelle immer von einer »Application Level Awareness«. Die wörtliche Übersetzung hiervon sei dem Leser selbst überlassen.

STT

Secure Transaction Technology, von Visa und Microsoft entwickeltes und verwendetes Protokoll zur sicheren Übertragung von Kreditkartendaten über das Internet.

Subdomain

Teil einer Domain, der an eine andere, untergeordnete Instanz delegiert ist, Verwaltung meist durch eigene Nameserver innerhalb dieses Bereichs.

SVN

Secure Virtual Networking, im Rahmen der *SIC* die sichere Kommunikation der einzelnen Komponenten von Next Generation untereinander. Hierzu ist die SVN Foundation zuständig.

SYN

Synchronize Sequence Numbers, Flag im TCP-Header, das beim Aufbau einer Verbindung gesetzt ist.

SYN Defender

Applikation der FireWall-1/VPN-1 zum Schutz gegen *SYN-Flooding*.

SYN-Flooding

Überfluten einer Maschine mit Connect Requests, meist mit gefälschter IP-Absenderadresse. Diese Angriffsart ist ein Denial-of-Service Angriff, dessen Ursache auch mit einer FireWall-1 nicht ausräumbar ist – wohl aber die Auswirkung dieses Angriffs auf den geschützten Server.

T1

Trunk 1 mit 1,544 MBit/Sek., Anschlußbandbreite in den USA.

T3

Trunk 3 mit 43,74 MBit/Sek., Anschlußbandbreite in den USA.

TACACS

Von Cisco entwickeltes Protokoll zur zentralen Authentisierung von Benutzern.

TCP

Transmission Control Protocol, arbeitet in Schicht 4 des ISO/OSI-Schichtenmodells, die im TCP/IP auch Transportschicht genannt wird. Gegenüber dem UDP bietet TCP virtuelle Verbindungen sowie zuverlässige Zustellung von Paketen in richtiger Reihenfolge.

Telnet

Remote Terminal Protocol, 23/tcp. Telnet-Clients können meist auch durch die Übergabe einer Portnummer zum Aufbau einer TCP Verbindung zu einem beliebigen Port genutzt werden.

TFTP

Trivial File Transfer Protocol, 69/udp, Protokoll zur Datenübertragung mit UDP.

Thin Ethernet

RG-58 Dual-Shielded (Koaxialkabel), auch Cheapernet genannt, Ein auf der Bus-Topologie aufbauendes Netzwerkmedium.

Toplevel-Domain

kurz »TLD«, Zone, die direkt unter der Root im Namensraum des Internets angesiedelt ist. Neben den »klassischen« TLDs com, net, org, edu, mil und gov sind heute hauptsächlich auch TLDs auf Länderebene (beispielsweise »de«, »at«) in Betrieb. Auch neue TLDs wie info oder biz sind inzwischen verfügbar.

TOS

Type of Service, Feld im IP-Header zur Kennzeichnung der Dringlichkeit eines Pakets.

Transceiver

Transmitter/Receiver, Sender und Empfänger – hier bezogen auf Netzwerk-Interfaces.

Triple-DES, 3DES

Dreifache Verschlüsselung durch *DES* mit 2 beziehungsweise 3 verschiedenen Schlüsseln (Summe 112 beziehungsweise 168 Bit Schlüssellänge).

Trust Center

siehe *Certificate Authority*

TTL

Time to live, auch Feld im IP-Header. Die TTL wird hier meist in Hops, das heißt, der Anzahl von Gateways zwischen Absender und Empfänger angegeben. Jedes Passieren eines Hops verringert die TTL um Eins.

Im Nameservice ist dies die Zeitdauer, die eine nicht-autoritative Antwort im Cache gespeichert und ohne weitere Rückfrage bei autoritativen Servern an Clients weitergeleitet wird.

Tunneling, Tunneln

Versehen von Paketen mit neuen Headern, die alten Header werden im Datenteil transportiert.

TP

Twisted Pair, Kabeltyp zum physikalischen Aufbau von Netzwerken mit Sternverkabelung.

Twofish

Frei verfügbarer, symmetrischer Verschlüsselungsalgorithmus von Bruce Schneier mit einer variablen Schlüssellänge von bis zu 448 Bit.

UAS

UserAuthority Server, in Kombination mit dem WAM u.a. zuständig für die Authentisierung von Benutzern beim Abruf von Dokumenten von einem geschützten Web-Server.

UDP

User Datagram Protocol, in der Transportschicht arbeitendes Protokoll für den Versand einzelner Pakete über das Netzwerk.

UFP

URL Filtering Protocol, 18182/tcp, genutzt von FireWall-1/VPN-1 zur Verbindung mit Content Security Servern, die beispielsweise Inhalte des World Wide Web filtern.

UPS

Uninterruptable Power Supply, siehe *USV*.

URG

Urgent Pointer Flag, Flag im TCP-Header, welches das Ende wichtiger Nachrichten kennzeichnet.

URI

Uniform Resource Identifier, von Next Generation genutzt für die Beschreibung von *Ressourcen* für HTTP.

URL

Uniform Resource Locator, oft auch als Web-Adresse bezeichnet.

User Authentication

Von FireWall-1/VPN-1 genutzte Authentisierung für die Dienste FTP, TELNET, HTTP und RLOGIN.

USV

Unterbrechungsfreie Stromversorgung, *UPS*, für die Sicherstellung des Dauerbetriebs von Servern, auch bei Stromausfall.

UUCP

Unix-to-Unix Copy, inzwischen kaum noch verwendetes Protokoll zum Austausch von Daten zwischen einzelnen Maschinen unter Unix.

Visual Policy Editor

kurz VPE, seit Next Generation Feature Pack 3 *SmartMap*. Grafische Darstellung der Beziehungen von Netzwerkobjekten untereinander. Separat zu lizenzieren, Exportmöglichkeit zu Microsoft Visio.

VPE

Siehe *Visual Policy Editor*.

VPN

Virtual Private Network. Über ein sicheres VPN können vertrauliche Daten sicher über nicht vertrauenswürdige Netzwerke wie beispielsweise das Internet transportiert werden. Hierzu sind pro VPN zwei Endpunkte zu definieren, an denen jeweils die Ver- und Entschlüsselung stattfindet.

VRRP

Virtual Router Redundancy Protocol, im Rahmen der Check Point Appliance von Nokia eingesetztes Protokoll zur Sicherstellung der Ausfallsicherheit der beteiligten Router. VRRP in Verbindung mit der FireWall-1/VPN-1 bildet eine von mehreren Möglichkeiten, die Firewall ausfallsicher aufzubauen, allerdings ohne Load-Balancing.

WAM

WebAccess Modul, Software zur Übergabe von Dokumenten an die UserAuthority, sofern sich der Benutzer hier richtig authentisiert und demnach die entsprechenden Rechte erhalten hat.

WAN

Wide Area Network.

WINS

Windows Internet Nameservice, proprietärer Nameservice von Microsoft für Netzwerke mit Windows 9x oder NT, wird häufig in Kombination mit dem *DNS* eingesetzt.

WKS

Well Known Service, ein Dienst, der durch die RFCs festgelegt und beschrieben ist. Unter WKS erfolgt häufig auch lediglich die Angabe der Portnummer und des Protokolls zur Beschreibung, beispielsweise Telnet: 23/tcp.

WWW

World Wide Web, ausgehend vom 1992 am CERN (Genf) entwickelten HTTP-Protokoll, mit dem Text sowie Bilder strukturiert übertragen werden können, resultierende Familie von Servern, mit denen eine interne Verlinkung zu anderen Dokumenten möglich ist.

X.500

ISO- und Internet-Standard, in dem festgelegt ist, wie globale Verzeichnisse aufgebaut sein sollten. Liegt beispielsweise LDAP zu Grunde.

X.509

ISO-Standard zur Definition und Verwaltung von Zertifikaten.

Zertifikat

Sichere Zuordnung eines öffentlichen Schlüssels zu einer Person oder Einheit (beispielsweise Server), von der *CA* meist digital signiert.

Zone

Bereich im Namens- oder Adreßraum, für den ein *Nameserver autoritative* Antworten liefert.