

1 Administration

1.1 Benutzer-Oberfläche

- Bedienung über Web-Browser
- Zugriff mit HTTP und HTTPS
- Deutsch oder Englisch
- Online-Hilfe
- Zugriff für Benutzer mit entsprechender Berechtigung auf
 - Home-Menü
 - individuell freigegebene Menü-Punkte der 2. Menü-Ebene

1.2 System-Konsole

- Monitor / Tastatur
- serielle Verbindung
 - in Grundkonfiguration deaktiviert
 - Baud-Rate einstellbar (19200 voreingestellt)
- Secure-Shell
 - Protokoll-Version 2
- telnet
 - in Grundkonfiguration deaktiviert

1.3 Benutzer-Verwaltung

- Gruppenbasiert
- Vordefinierte System-Gruppen zur Rechtevergabe
 - Mail-Server (lokales Postfach)
 - Proxies
 - RAS-Einwahl
 - Administrations-Oberfläche
- Kennwörter
 - von berechtigten Benutzern über Administrations-Oberfläche änderbar
 - Nicht änderbares Kennwort je System-Gruppe separat einstellbar
- Benutzer- und Gruppen-Import aus Microsoft Active-Directory
 - Auswahl der zu importierenden Gruppen über Gruppemitgliedschaft im Active-Directory
 - Import aller zugeordneten Active-Directory Benutzer
 - Import von Passwörtern die nach Installation einer DLL gesetzt wurden

1.4 X.509 CA

- Selbstsigniertes root CA-Zertifikat
 - 10 Jahre gültig
 - Geschützt mit separatem Kennwort
 - Jederzeit neu erstellbar
 - Export und Import im PKCS#12-Format
 - Löschen des privaten Schlüssels möglich
 - Export des öffentlichen Schlüssels im PEM-Format
- Erstellen signierter Zertifikate
 - 1 Jahr gültig
 - Vorzeitig für ungültig erklären möglich
 - Export im PKCS#12-Format
 - Privater Schlüssel wird nach Generierung gelöscht
 - Öffentlicher Schlüssel jederzeit im PEM-Format verfügbar
 - Vordefinierter Eintrag zum Erstellen des Zertifikats für DEFENDO VPN-Server
- Zertifikats-Sperlliste
 - manuelle Erstellung
 - Export im PEM-Format

1.5 Backup

- Manuelles Backup

- Automatisches Backup
 - per E-Mail
 - über FTP
 - über Secure-Copy mit RSA-Authentifizierung
 - täglich, wöchentlich oder monatlich
 - Variablen im Dateinamen bei FTP und Secure-Copy
- User-Backup mit allen benutzerbezogenen Einstellungen
- System-Backup mit allen weiteren Einstellungen
- Mail-Backup mit lokalen Postfächern und Home-Verzeichnissen
- Backup-Dateien älterer DEFENDO-Versionen jederzeit installierbar

1.6 Log-Dateien

- Zugriff und Suchfunktionen über Web-Oberfläche
- automatisches Rotieren der Log-Dateien
 - wöchentlicher Zyklus
 - automatisches Löschen nach 12 Wochen
 - vorzeitiges manuelles Löschen aller alten Logs möglich
 - kürzere Zeitspannen bei unwichtigen Log-Dateien
- Externe Archivierung
 - per Mail
 - über FTP
 - über Secure-Copy mit RSA-Authentifizierung
 - syslog, messages, maillog, Web-Proxy und Web-Server Zugriffs-Logs

2 Netzwerk

2.1 LAN-Anschluss

- Ausstattung und Verfügbarkeit modellabhängig
- Ethernet 10/100 TP
- Ethernet 1000 TP auf Anfrage
- Tokenring auf Anfrage

2.2 ADSL

- Ausstattung und Verfügbarkeit modellabhängig
- Anschluss an ADSL-Modem über 10/100 MBit TP Ethernet
- Protokolle PPP-over-Ethernet (PPPoE) oder PPP-over-PPTP
- Authentifizierung bei Gegenstelle mit PAP oder CHAP
- Feste oder dynamische IP-Adressen
- Verbindungstrennung
 - nie - getrennte Verbindung sofort wieder aufbauen
 - zu bestimmter Uhrzeit (täglich)
 - bei Inaktivität
- Automatischer Fallback auf ISDN PPP-Verbindung bei Störung

2.3 ISDN

- Ausstattung und Verfügbarkeit modellabhängig
- Anschluss an ISDN Mehrgeräte-Anschluss, S0-Bus
- ISDN-Protokolle E-DSS1 (Euro-ISDN), 1TR6, NI1
- ISDN-Standleitungen
 - Typ 64S1 (64 kbit/s)
 - Typ 64S2 (128 kbit/s)
 - Über fest zugeordnete ISDN-Karte
- ISDN-Wählverbindungen
 - Ein- und ausgehende Verbindungen
 - Rufnummern-Identifizierung
 - D-Kanal Callback
 - Verbindungstrennung bei Inaktivität
 - Gebührenoptimierung durch Eingabe der Taktung
- HDLC RawIP Schnittstellen
 - unbegrenzte Anzahl
 - Kanalbündelung (128 kbit/s) möglich

- HDLC syncPPP Schnittstellen
 - max. 63 Stück
 - dynamische MPPP-Kanalbündelung (128 kbit/s) für 1 Schnittstelle
 - Authentifizierung bei Gegenstelle mit PAP oder CHAP
 - Authentifizierung der Gegenstelle mit PAP
 - Feste oder dynamische IP-Adressen
 - Proxyarp bei RAS-Einwahl
- Alle Schnittstellen teilen sich die verfügbaren B-Kanäle

2.4 Analog Modem

- Ausstattung und Verfügbarkeit modellabhängig
- Serielles Modem
- Nur RAS-Einwahl (eingehende Verbindungen)
- Authentifizierung der Gegenstelle mit PAP
- Proxyarp

3 IPsec VPN

3.1 IPsec VPN

- Automatisches Keying
- Authentifizierungs-Methoden
 - Preshared Key
 - RSA X.509-Zertifikat
- IKE Phase 1
 - Main-Mode
 - TripleDES (3DES)
 - MD5-96 oder SHA1-96
 - Oakley Gruppen MODP1024 oder MODP1536
 - Zeitintervall für Rekeying einstellbar
- IKE Phase 2
 - TripleDES (3DES)
 - AH oder ESP, MD5-96 oder SHA1-96
 - Optional Perfect-Forward-Secrecy wie in Phase 1
 - Zeitintervall für Rekeying einstellbar
- NAT-Traversal
 - draft-ietf-ipsec-nat-t-ike-01 bis -04
 - draft-ietf-ipsec-udp-encaps-01 bis -04
- Bis zu vier IPsec-Schnittstellen
 - Unbegrenzte Anzahl VPN-Verbindungen je Schnittstelle
 - Eigene Firewall-Konfiguration in der IPsec-Schnittstelle
 - Exklusive Zuordnung der IPsec-Schnittstelle zu Ethernet-, Tokenring- und ISDN-Schnittstelle
 - Dynamische Zuordnung einer IPsec-Schnittstelle zu aktueller Internet-Schnittstelle (auch ADSL)
 - MTU konfigurierbar
- Aufgrund Main-Mode ist die Authentifizierungsmethode für alle Gegenstellen mit dynamischer IP je IPsec-Schnittstelle einheitlich
- Aufgrund Main-Mode nur ein Preshared Key für alle Verbindungen
 - über dynamisch zugeordneter IPsec-Schnittstelle
 - je exklusiv zugeordneter IPsec-Schnittstelle zu Gegenstellen mit dynamischer IP
- Authentifizierung der Gegenstelle mit X.509 Zertifikat
 - über importierten öffentlichen Schlüssel der Gegenstelle
 - über festgelegte CA
 - CRL-Import im PEM-Format möglich

- X.509 Zertifikat des VPN-Servers
 - Erstellen über DEFENDO CA
 - Import eines beliebigen Zertifikats als PKCS#12-Datei möglich
 - Export öffentlicher Schlüssel im PEM-Format
 - Export als PKCS#12-Datei
- L2TP-over-IPsec VPN
 - Proxyarp für LAN
 - max. 255 gleichzeitige L2TP-Verbindungen
 - L2TP-Authentifizierung mit PAP
 - Eigene Firewall-Konfiguration in der L2TP-Schnittstelle
 - IPsec-Adresse des DEFENDO darf nicht über NAT laufen

4 Firewall

4.1 Standard-Firewall

- Basierend auf GNU/Linux iptables Firewall
- 16.000 gleichzeitige Verbindungen bei 256MB Hauptspeicher
- Integriertes Stateful-Inspection-Regelwerk
- Integrierte Plausibilitätsprüfungen (z.B. Adress-Spoofing)
- Integrierte Liste zur Sperre bekannter Ad-/Spyware-Adressen *)
- SNAT und DNAT
- Template basierte Konfiguration über 4 vordefinierte Vertrauensstufen
- Freie Zuweisung der Vertrauensstufen zu Schnittstellen
- Freigabe von Verbindungen innerhalb der Vertrauensstufen

4.2 Dynamische Firewall

- Sensoren für Denial-of-Service und Portscan
- Auswertung der Information aus Standard-Firewall und Sensoren
- Anbindung an DEFENDO Intrusion-Detection
- Assoziation von Vorfällen mit Quell-Adresse des Angriffs
- Automatische zeitlich begrenzte Sperre einzelner Quell-Adressen
- Erkennung von massiven Angriffen mit gefälschten Adressen
- Konfigurierbares Verhalten für verteilte Angriffe

4.3 Intrusion Detection und Prevention

- Integrierte Signatur-Datenbank
- Auswählbare erweiterte Signatur-Gruppen
- Signatur-Whitelist
- Aktivierbar je Schnittstelle
- Optionaler promiscuous mode
- Protokollierung
 - Datum / Uhrzeit
 - Regel-ID
 - Schnittstelle
 - IP-Signatur
 - Kurzbeschreibung
 - Klassifizierung
 - Links zu weiterführenden Informationen
- Anbindung an DEFENDO's dynamische Firewall

4.4 Bandbreiten-Management

- Für Internet-Schnittstelle
- Zur Verfügung stehende Bandbreite frei konfigurierbar
- Fünf Prioritäts-Klassen
 - leere TCP-Ack-Pakete
 - Voice-over-IP (SIP, H.323, RTP)
 - Benutzerdefiniert Hochprior und VPN (IKE, ESP, AH)
 - Standard
 - Benutzerdefiniert Niederprior

- Dynamische Verteilung ungenutzter Bandbreite auf niedrigere Klassen
- Mindestbandbreite 20% je Klasse

5 Proxies / Application-Gateways

5.1 Web-Proxy

- Protokolle http, https (mit connect), ftp (über http), gopher, wais
- Transparenter Proxy für http
- Einbindung in Proxy-Hierarchie möglich
- Virensan von Downloads basierend auf Content-Type (Virens Scanner nicht enthalten)
- Maskierung von HTML-Tags zur Ausblendung aktiver Inhalte wie ActiveX
- Zugriffskontrolle über Client-IP
- Benutzer-Authentifizierung mit Basic-Auth
 - Benutzerverwaltung intern, über Windows-PDC oder LDAP
 - Schutz vor Weitergabe der Zugangsdaten durch Erkennung von Mehrfachanmeldungen
- User-Agent-Filter gegen Ad-/Spyware, Instant Messengers und Peer-to-Peer *)
- Gruppenbezogener URL-Filter
 - uhrzeitabhängige Konfiguration
 - mit in Kategorien organisierter URL-Datenbank
 - selbst definierbare Positiv- und Negativ-Domainlisten
 - Sperrung des Zugriffs anhand Endung des Dateinamens
 - Sperrung von Adressen mit pornographischen Schlüsselwörtern
 - Standardverhalten je Gruppe einstellbar (Zugriff erlaubt oder verboten)
- Zeit- und Mengenkongente je Benutzer
- Integrierter ICAP-Client
- Begrenzung von Up- und Download-Größe
- Caching in Hauptspeicher und auf Festplatte
- Zugriffs-Statistik der letzten 12 Monate mit
 - Jahresübersicht (graphisch und numerisch)
 - Monatsübersicht (numerisch)
 - Tagesübersicht je Monat (graphisch und numerisch)
 - Stundenübersicht je Monat (graphisch)
 - Top-URLs je Monat (numerisch)
 - Top-Client-IPs je Monat (numerisch)
 - Top-Benutzer je Monat (numerisch)

5.2 FTP-Proxy

- Proxy-Typ "USER ohne Login" bzw. "USER user@host:port"
- Transparenter Proxy
- Virensan von Downloads (Virens Scanner nicht enthalten)
- Zugriffskontrolle basierend auf Konto und Adresse des Ziel-Servers

5.3 SOCKS-Proxy *)

- SOCKS Protokoll-Versionen 4 und 5
- Unterstützung von TCP- und UDP-Verbindungen
- Bind-Erweiterung
- Zugriffskontrolle über Client-IP
- Freigabe von Verbindungen anhand IP- und Port-Signatur
- Benutzerbezogene Verbindungen bei Authentifizierung

5.4 Reverse-Proxy

- Reverse-Proxy und Load-Balancer für http und https
- SSL-Offloader: Zugriff auf Backend nur mit http
- Optional Authentifizierung mit Basic-Auth
- Syntax-Prüfung von Anfragen zum Schutz vor Angriffen
- Größenbeschränkung für Uploads

- Reverse-Proxy Funktion mit
 - Zugriff auf DEFENDO Webmail oder Administration
 - Zugriff auf benutzerdefiniertes Backend
 - Prüfung des Host-Headers
- Load-Balancer Funktion mit
 - zufälliger Verteilung von Verbindungen
 - Gewichtung der Backends
 - Sitzungserkennung anhand Client-IP, Basic-Auth, URL-Parameter oder Cookie
 - Erkennung ausgefallener Server
- Zugriffs-Statistik der letzten 12 Monate mit
 - Jahresübersicht (graphisch und numerisch)
 - Monatsübersicht (numerisch)
 - Tagesübersicht je Monat (graphisch und numerisch)
 - Stundenübersicht je Monat (graphisch)
 - Top-URLs je Monat (numerisch)
 - Top-Client-IPs je Monat (numerisch)
 - Top-Benutzer je Monat (numerisch)
 - Top-Länder je Monat (graphisch und numerisch)

5.5 SIP-Proxy

- SIP Outbound-Proxy für ein- und ausgehende Verbindungen
- Integrierter RTP-Proxy
- Transparenter Proxy
- Nutzung als Registrar möglich
- Zugriffskontrolle über Client-IP
- Registrierung nur von Clients über LAN-Schnittstelle eth0

6 Mail-System

6.1 Mail-Server

- Protokolle SMTP und ESMTP
- Konfigurierbare TLS-Verschlüsselung
- Empfang eingehender E-Mails
 - Direkter Empfang per SMTP
 - E-Mail-Abwurf von POP- und ETRN-Servern via DEFENDO Mail-Client
- Zustellung eingehender E-Mails an interne Mail-Server
 - Konfigurierbar je Domain
- Zustellung eingehender E-Mails an lokale Postfächer
 - Konfigurierbar je Domain
 - Virtuelle Mail-Adressen und Domains
 - Verteilerfunktion je Benutzergruppe
 - Beliebig viele Alias-Adressen je Empfänger-Postfach
 - Mail-Weiterleitung an beliebige viele Adressen je Empfänger-Postfach
 - Individuelle Auto-Reply je Empfänger-Postfach
 - Zugriff via DEFENDO Webmail, POP3- oder IMAP4-Server
- Mail-Relay / SMTP-Proxy für ausgehende E-Mails
 - optional als transparenter Proxy
 - Zugriffskontrolle per Client-IP, optional mit SMTP Auth
 - SMTP Auth Methoden LOGIN, PLAIN, LOGIN+TLS, PLAIN+TLS
- Mail-Relay für externe Benutzer
 - Zugriffskontrolle mit SMTP Auth
 - SMTP Auth Methoden LOGIN, PLAIN, LOGIN+TLS, PLAIN+TLS
- Versand ausgehender E-Mails
 - Direkter Versand
 - Versand über Relay-Server
 - SMTP Auth Methoden LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5
 - Synchronisation mit Verbindungsaufbau von PPP Wählverbindungen

- E-Mail Virensan (Virens Scanner-Lizenz nicht enthalten)
 - Prüfung ein- und ausgehender E-Mails
 - Extra Dekodier- und Entpack-Stufe zusätzlich zum Virens Scanner
 - Rekursives Entpacken einer Vielzahl von Archivtypen
 - Schutz vor Denial-of-Service Angriffen
 - Optional E-Mail-Benachrichtigung des Administrators
 - Quarantäne Verzeichnis
- MIME-Dateianhangs-Filter
 - für eingehende und optional für ausgehende E-Mails
 - Entfernung von Dateianhängen basierend auf Dateinamens-Erweiterung
 - Ersetzt Dateianhänge durch Warnmeldung
 - Optional E-Mail-Benachrichtigung des Administrators
 - Quarantäne Verzeichnis
- HTML-Mail-Filter *)
 - Unschädlich machen von aktiven Inhalten, Formularen und Web-Bugs
 - Optionales Entfernen von HTML wenn Inhalt alternativ auch als Text vorliegt
- SPAM-Filter
 - Prüfung eingehender E-Mails
 - Globaler Filter oder Filter je Benutzer
 - Konfigurierbare Schwellwerte
 - Je Benutzer: Schwellwerte zum Markieren und Verwerfen
 - Global: Schwellwerte zum Markieren und Abweisen
 - Quarantäne-Empfänger im globalen SPAM-Filter
 - Nutzung mehrerer RBL-Server
 - Nutzung von URIBL-Servern
 - DCC-Client
 - Integrierte Signatur-Datenbank
 - Änderung der Signatur-Bewertung möglich
 - Benutzerdefinierte Regeln
 - Manuelle Black- und Whitelists
 - Extra-Bewertung von englischsprachigen E-Mails
 - Extra-Bewertung von E-Mails mit Fernost-Zeichensatz
- Graue Liste (Greylisting) *)
 - Konfigurierbares Zeitverhalten
 - Absender- und Empfänger-Whitelist
- Automatische E-Mail Archiv-Funktion
 - Zustellung einer E-Mail-Kopie an beliebige Adresse
 - Getrennt für ein- und ausgehende E-Mails konfigurierbar
- Automatisches Hinzufügen eines Textbausteins an ausgehende Mails
- Einstellmöglichkeiten für berechnete Benutzer über Administrations-Oberfläche:
 - Passwort
 - E-Mail Weiterleitung
 - Auto-Reply
 - SPAM-Filter Schwellwerte
 - SPAM-Bewertung englischsprachiger E-Mails
 - Benutzerdefinierte SPAM-Filter Regeln
 - SPAM-Filter Black- und Whitelist
 - Webmail-Parameter
- Zugriffs-Statistik der letzten 12 Monate mit *)
 - Jahresübersicht (graphisch und numerisch)
 - Monatsübersicht (numerisch)
 - Tagesübersicht je Monat (graphisch und numerisch)
 - Stundenübersicht je Monat (graphisch)
 - Top-SPAM-Merkmal-Kategorie je Monat (numerisch)
 - Top-Viren-Liste je Monat (numerisch)
 - Top-Empfänger-Domains je Monat (numerisch)
 - Top lokale Absender je Monat (numerisch)
 - Top lokale Empfänger je Monat (numerisch)

6.2 Mail-Client

- Protokolle POP3, APOP und ETRN
- Weitere Varianten auf Anfrage
- Optional TLS/SSL-Verschlüsselung
- Abruf von beliebig vielen Servern möglich
 - Zeitgesteuerte Abholung
 - Synchronisation mit Verbindungsaufbau von PPP Wählverbindungen
- Gespiegelte POP-Konten (single-drop)
- Verteilung von POP Sammel-Konten (multi-drop)
 - Konfigurierbares Domain-Matching
 - Konfigurierbare Header-Analyse

6.3 POP3- / IMAP4-Server

- Optional TLS/SSL-Verschlüsselung
- Benutzerdefinierte IMAP4 Unterordner
- UIDL Erweiterung

6.4 Webmail

- Zugriff mit HTTP und HTTPS
- Benutzerdefinierte Unterordner
- Suchfunktion
- E-Mail Filter
 - Individuell vom Benutzer einstellbar
 - Globaler Filter vom Administrator gepflegt
- Adressbuch-Funktion
 - Individuell vom Benutzer einstellbar
 - Globale Einträge vom Administrator gepflegt
 - Suchfunktion
 - Im- und Export
- Kalender-Funktion
 - Individuell vom Benutzer einstellbar
 - Globale Einträge vom Administrator gepflegt

7 Viren-Scanner

7.1 Virens Scanner

- Lizenzen nicht enthalten
- Scanner müssen separat erworben und installiert werden
- Speziell an DEFENDO angepasste Versionen
 - F-Secure Anti-Virus
 - Kaspersky Anti-Virus for Appliance Server
 - Unabhängig von Anzahl der Benutzer
 - Engine-Updates Bestandteil der regulären DEFENDO-Updates
- Ausserdem installierbar
 - McAfee Virus Scan for Linux v4.x
- Automatische Signatur-Updates
 - Zeitgesteuerte Aktualisierung
 - Kürzestes Intervall stündlich
 - Nur geänderte Signatur-Dateien werden heruntergeladen
 - Bereitstellung der Signaturen auf FTP-Server für lokale Clients
 - E-Mail Benachrichtigung im Fehlerfall
 - Optional E-Mail Benachrichtigung über jedes Update

8 Weitere Komponenten

8.1 DHCP

- Secondary DHCP Option
- Mehrere Adressbereiche definierbar
- Feste Adress-Zuordnung anhand MAC-Adresse

Leistungsbeschreibung DEFENDO V4.2-3-0

- Konfigurierbare Lease-Dauer
- Konfigurierbare Optionen
 - Domain-Name
 - Router
 - zwei DNS
 - zwei WINS
 - NetBIOS Knotentyp

8.2 DNS

- DNS-Forwarder / Proxy
 - Optional als transparenter Proxy
 - Zugriffskontrolle über Quell-IP
 - Client-Schutz durch Prüfung der Antwort-Pakete
 - Ad-/Spyware-Schutz mit DNS-Blackhole-Domains *)
 - Caching
 - Auflösung über feste Forwarder und/oder Root-Server
- Name-Server
 - Unbegrenzte Anzahl von Zonen
 - Primary (Master) oder Secondary (Slave) je Zone wählbar
 - Öffentlicher oder lokaler Zugriff je Zone wählbar
 - Zugriffskontrolle für Zonentransfer über Quell-IP

8.3 Client für dynamisches DNS

- Unterstützung verschiedener Anbieter
 - DynDNS
 - easyDNS
 - ZoneEdit
 - DyNS
 - ODS
 - HN
- Aktualisierung bei Verbindungsaufbau

8.4 FTP-Server

- Anonymous FTP-Server
 - Pflege über vordefinierten Benutzer
 - Zugriff nur für lokale Clients oder öffentlich
 - Deaktivierbar
 - Optionaler geschützter Upload-Bereich
 - Kein anonymer Download möglich
 - Begrenzte Verzeichnis-Tiefe
 - Feste Dateinamens-Konventionen
- Pflege der lokalen Web-Server Verzeichnisse
 - Vordefinierte Benutzer je Web-Server-Bereich
 - Zugriff nur für lokale Clients oder öffentlich
 - Deaktivierbar
- Administrator-Zugang
 - Zugriff nur für lokale Clients oder öffentlich
 - Deaktivierbar

8.5 HTTP-Server

- Intranet-Server
 - Zugriff nur für lokale Clients
 - Vordefinierter Benutzer zur Pflege der Inhalte
 - Pflege über FTP
 - Pflege über Windows-Freigabe im LAN
 - CGI-Verzeichnis
- Öffentlicher Web-Server
 - Vordefinierter Benutzer zur Pflege der Inhalte
 - Pflege über FTP
 - Pflege über Windows-Freigabe im LAN
 - CGI-Verzeichnis
 - Graphische Zugriffs-Statistik

8.6 Zeit-Server

- Synchronisation mit beliebig vielen Internet-Zeitservern
 - Protokolle NTP oder time (TCP)
 - täglich oder wöchentlich
- Zeit-Server für lokale Clients
 - Protokolle NTP, time, daytime oder über NetBIOS