DEFENDO INTERNET SECURITY GATEWAY

DEFENDO

DEFENDO vm

Leistungsbeschreibung

Stand: 2019-11-11, V7.1-1-2

LINOGATE INTERNET TECHNOLOGIES

1 Hardwarenahe Funktionen

1.1 Betriebssystem
- GNU/Linux 64-bit Kernel 4.4
- SELinux

1.2 SMART
- Überwachung der Festplatten mit SMART
- Benachrichtigung per E-Mail

2 Administration

2.1 Benutzer-Oberfläche
- Bedienung über Web-Browser
- Zugriff mit HTTP und HTTPS
- Bei Zugriff über Reverse-Proxy auch mit Client-Zertifikaten
- Optionale Zweifaktor-Authentifzierung
  - Zeitbasierte Einmalpasswörtern (TOTP)
  - Separat konfigurierbar für direkte Zugriffe und Zugriffe über Reverse-Proxy
  - Für alle Benutzer oder nur für Benutzer mit aktivierten Einmalpasswörtern
- Deutsch und Englisch
- Online-Hilfe
- Zugriff für Benutzer mit entsprechender Berechtigung auf
  - "Mein Konto"-Menü
  - individuell freigegebene Menü-Punkte der 2. Menü-Ebene (nur lesend oder auch schreibend)
- Protokollierung aller Änderungen
  - Mit IP und Benutzername für 7 Tage
  - Anonymisiert für 6 Monate
- Export-, Import-Funktion für viele Tabellen

2.2 System-Konsole
- Monitor / Tastatur
- in Grundkonfiguration deaktiviert:
  - serielle Verbindung
  - Secure-Shell
  - Telnet

2.3 Benutzer-Verwaltung
- Gruppenbasiert
- Vordefinierte System-Gruppen zur Rechtevergabe
  - Mail-Server (lokales Postfach)
  - Proxies
  - RAS-Zugang
  - Administrations-Oberfläche
- Kennwörter
  - von berechtigten Benutzern über Administrations-Oberfläche änderbar
  - Nicht änderbares Kennwort je System-Gruppe separat einstellbar
- Zeitbasierte Einmalpasswörter (TOTP)
  - für einzelne Dienste
  - 80, 120 oder 160 Bit Schlüssel
  - 6 Stellen, 30 Sekunden, SHA1
  - Bequeme Konfiguration über QR-Code
- Benutzer-/ Gruppen-Import aus Microsoft Active-Directory
  - Auswahl der zu importierenden Gruppen über Gruppenmitgliedschaft im Active-Directory
  - Import aller zugeordneten Active-Directory Benutzer
  - DLL zur Installation auf Active-Directory-Server im Lieferumfang, die den Import von nach Installation geänderten Passwörtern erlaubt

2.4 Zertifikatsverwaltung
- Schlüsselbund
  - Erstellen von CA-Anfragen an externe CAs
  - Automatisierter Zertifikatsabruf über ACMEv2 (Let's Encrypt)
  - Erstellen selbstsignierte Zertifikate
  - Export und Import im PKCS#12-Format
- DEFENDO-CA
  - Stammzertifizierungsstelle für interne Nutzung (z.B. VPN)
  - bei Auslieferung nicht vorinstalliert
  - kann jederzeit vom Administrator neu erstellt werden
  - max. RSA-4096 / SHA2-512
  - 20 Jahre gültig (max. bis 31.12.2037)
  - alternativ Import von extern erzeugtem Schlüssel
  - Geschützt mit separatem Kennwort
  - Export und Import im PKCS#12-Format
  - Löschen und Re-Import des privaten Schlüssels möglich
  - Export des öffentlichen Schlüssels im PEM-Format
- Erstellen von End-Zertifikaten
  - max. RSA-4096 / SHA2-512
  - 1 bis 6 Jahre gültig
  - optionale Erweiterungen:
    - Subject-Alternative-Names
    - Extended-Key-Usage serverAuth/clientAuth/ emailProtection
  - Export
    - im PKCS#12-Format
    - Installationspaket für Windows IPsec-L2TP VPN-Client
    - Installationspaket für Windows OpenVPN-Client
    - Installationspaket für iOS IPsec-Xauth VPN-Client
    - Installationspaket für iOS Zugriff auf Exchange mit Client-Zertifikat
    - Installationspaket für DEFENDO/Orbiter-Gegenstelle
  - Privater Schlüssel wird nach Generierung gelöscht
  - Öffentlicher Schlüssel jederzeit im PEM-Format verfügbar
  - Vordefinierter Eintrag zum Erstellen des Zertifikats für DEFENDO VPN-Server
- Zertifikats-Sperrliste
  - manuelle Erstellung
  - Export im PEM-Format

2.5 Backup
- Manuelles Backup
- Automatisches Backup
  - per E-Mail
  - über FTP
  - auf Windows-Freigabe
  - über Secure-Copy mit RSA-Authentifizierung
  - täglich, wöchentlich oder monatlich
  - Variablen im Dateinamen (nicht bei E-Mail)
  - Testfunktion
- User-Backup mit allen benutzerbezogenen Einstellungen
- System-Backup mit allen weiteren Einstellungen
- Mail-Backup mit lokalen Postfächern, Home-Verzeichnissen und Groupware-Daten
- Backup-Dateien älterer DEFENDO-Versionen jederzeit installierbar

2.6 Log-Dateien
- Zugriff und Suchfunktionen über Web-Oberfläche
  - Suchfunktion mit Vorfilterung und Histogramm
  - Live-Log mit Pause-Taste
  - Filterfunktionen (inkl./exkl., und/oder)
  - Farbliche Hervorhebung bestimmter Meldungen
  - Schaltfläche zum Speichern als Text-Datei
- automatisches Rotieren der Log-Dateien
  - täglicher Zyklus
  - automatisches Löschen nach 7 Tagen
  - vorzeitiges manuelles Löschen aller alten Logs möglich
  - kürzere Zeitspannen bei unwichtigen Log-Dateien
- Externe Archivierung
  - über FTP
  - auf Windows-Freigabe
  - über Secure-Copy mit RSA-Authentifizierung
  - per Mail

für Logdateien
- wichtige Meldungen (syslog)
- sonstige Meldungen (messages)
- Firewall
- IPsec
- Mail
- Web-Proxy Zugriffs-Log
- Web-Server Zugriffs-Log
- Reverse-Proxy
- Administrationsoberfläche

mit Testfunktion
- Protokollierung auf externe Syslog-Server für diverse Log-Dateien

2.7 SNMP
- SNMPv3 Server

3 Netzwerk

3.1 ADSL/VDSL/Mobilfunk
- Ausstattung und Verfügbarkeit modellabhängig
- Anschluss an ADSL-Modem über Ethernet
- PPPoE, PPPoE über VLAN (VDSL), PPTP zu PPTP-to-PPPoA-Relay
- Mobilfunk (LTE/UMTS/GPRS) über separat erhältlichen USB-Stick
- 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 bei Störung
  - auf Ethernet oder andere DSL- bzw. Mobilfunk-Verbindung
  - E-Mail Benachrichtigung

3.2 Ethernet
- Ausstattung und Verfügbarkeit modellabhängig
- Ethernet 10/100/1000 TP
- Bündelung von Netzwerkkarten (aktiv/passiv, IEEE 802.3ad/802.1AX, nach MAC oder pro Paket)
- Bridging mit Ethernet-, WLAN- und VLAN-Schnittstellen (transparente Firewall)
- Senden von Wake-on-LAN-Paketen über Oberfläche

3.3 VLAN
- Tagged-VLAN nach IEEE 802.1q
- Tag von 1 bis 4094 frei wählbar
- Bis zu 4094 VLAN-Schnittstellen (eine je Tag)
- Bindung auf frei wählbare Netzwerkkarte
- Eigene Firewall-Konfiguration je Schnittstelle
- Bridging mit Ethernet-, WLAN- und VLAN-Schnittstellen (transparente Firewall)

3.4 WLAN
- Nur in bestimmten Hardware-Modellen verfügbar
- 802.11a/g/n
- WPA2-EAP/CCMP an externem Radius-Server, WPA2-PSK/CCMP oder offenes WLAN
- optionale Client-Isolierung
- optionaler MAC-Filter
- als Bridge mit Ethernet- und VLAN-Schnittstellen (transparente Firewall) oder geroutet
- bis zu 8 SSIDs auf einer Frequenz unabhängig konfigurierbar

3.5 IPv6
- Host- oder Router-Modus
- IPv6-NAT
- IPv6 Schnittstellenkonfiguration
  - Aktivierbar in DSL-, Ethernet-, VLAN- und WLAN-Schnittstellen
  - Statisch oder dynamisch (SLAAC oder stateful/DHCPv6)
  - Dual-Stack oder DS-Lite
  - In WLAN-Schnittstellen nur statisch
- Präfix-Delegation
  - je Schnittstelle aktivierbar bei dynamischer IPv6-Konfiguration
  - delegierter Präfix in Administrations-Oberfläche als IP-Objekt verfügbar
  - spezielle IP-Objekte mit allen delegierten Präfixen und mit Präfix der primären Internet-Anbindung
  - spezielle IP-Objekte zur Aufteilung des Präfix in Teilpräfixe und Einzeladressen
- Router-Advertisement
  - je Ethernet-, VLAN- und WLAN-Schnittstelle aktivierbar bei statischer IPv6-Konfiguration
  - Multicast oder Unicast an konfigurierte Link-Local-Adressen
  - beliebig viele Präfixe für SLAAC
  - optionale Parameter
    - Other-Flag bzw. Other- und Managed-Flag
    - RDNSS mit max. zwei DNS
    - DNSSL
    - Veröffentlichung von Routen
- DHCPv6-Server
  - je Ethernet-, VLAN- und WLAN-Schnittstelle separat konfigurierbar
  - Ein Adressbereich für dynamische Adressvergabe
  - Konfigurierbare Lease-Dauer
  - Feste Adress-Zuordnung anhand MAC-Adresse
    - IPv6-Adresse
    - optional Delegation eines IPv6-Präfixes

3.6 Routing
- Erweitertes Routing in DSL-, Ethernet- und VLAN-Schnittstellen
- nach Protokoll-/Port-Signatur
- nach Quell-Adresse
- nach Ziel-Adresse

3.7 Failover-Cluster
- Active-/Passive-Cluster
- VRRP-Protokoll
- Individueller oder gemeinsamer Internetzugang für beide Knoten
- Manuelle oder automatische Replikation der Einstellungen
- Replikation des Stateful-Inspection-Status der Firewall
- Replikation der Benutzer-Postfächer
- Überwachung des Linkstatus der Netzwerkkarten hardwareabhängig
- optional Failover bei Ausfall wichtiger Dienste

4 VPN

4.1 IPsec VPN
- Automatisches Keying mit IKEv1/IKEv2
- Authentifizierungs-Methoden
  - Preshared-Key
  - RSA X.509-Zertifikat
- IKE Phase 1
  - Main-Mode
  - TripleDES (3DES), AES-128/256
  - MD5, SHA1, SHA2-256/512
  - Oakley Gruppen 2, 5, 14-18 (MODP-1024/1536/2048/3072/4096/6144/8192)
  - Zeitintervall für Rekeying einstellbar
- IKE Phase 2
  - TripleDES (3DES), AES-128/256
  - MD5, SHA1, SHA2-256/384/512
  - Optional
    - Perfect-Forward-Secrecy
    - Dead-Peer-Detection
    - IPComp
  - Zeitintervall für Rekeying einstellbar
- IKE-Fragmentation
- NAT-Traversal

- Bis zu vier IPsec-Schnittstellen
  - Unbegrenzte Anzahl VPN-Verbindungen je Schnittstelle
  - Eigene Firewall-Konfiguration in der IPsec-Schnittstelle
  - Dynamische Zuordnung einer IPsec-Schnittstelle zu aktueller Internet-Schnittstelle
  - Exklusive Zuordnung von IPsec-Schnittstelle zu DSL-, Ethernet-, VLAN- und WLAN-Schnittstellen mit fester IP
  - MTU konfigurierbar
- Authentifizierung der Gegenstelle mit Preshared-Key
  - konfigurierbare ID der Gegenstelle (IP, FQDN oder USER-FQDN)
  - konfigurierbare lokale ID bei Server-Verbindungen (IP, FQDN oder USER-FQDN)
  - aufgrund Main-Mode je IPsec-Schnittstelle nur ein gemeinsamer PSK für Gegenstellen mit dynamischer IP
- Authentifizierung der Gegenstelle mit X.509 Zertifikat
  - über festgelegte CA mit Angabe des Zertifikat DNs oder
  - über importierten öffentlichen Schlüssel der Gegenstelle
  - CRL-Import im PEM-Format möglich
- L2TP-over-IPsec VPN
  - Proxyarp für LAN
  - Zugewiesener DNS konfigurierbar
  - max. 245 gleichzeitige L2TP-Verbindungen
  - L2TP-Authentifizierung mit PAP
  - Feste IP je Benutzer möglich
  - Eigene Firewall-Konfiguration in der L2TP-Schnittstelle
  - Rekeying durch Client
- XAuth/Modecfg-Server
  - Proxyarp für LAN
  - Zugewiesener DNS konfigurierbar
  - Feste IP je Benutzer möglich
  - Rekeying durch Client
- Start, Stop, Neustart je konfigurierter Verbindung

4.2 OpenVPN

- OpenVPN 2.3 Server und Client
- UDP oder TCP mit frei wählbarem Port
- Authentifizierung mit RSA X.509-Zertifikaten
- Verschlüsselungsverfahren AES-128/256-CBC, Blowfish-128/256-CBC
- Hashverfahren MD5, SHA1, SHA2-224/256/384/512
- Server-Schnittstellen
  - Unbegrenzte Anzahl Schnittstellen
  - Unbegrenzte Anzahl Verbindungen je Schnittstelle
  - gemeinsames X.509-Zertifikat mit IPsec
  - Eigene Firewall-Konfiguration je OpenVPN-Server-Schnittstelle
  - Oakley Gruppen 2, 5, 14-18 (MODP-1024/1536/2048/3072/4096/6144/8192)
  - Zugewiesener DNS konfigurierbar
  - Feste IP je Client möglich
  - Konfiguration der Remote-Netze je Client
- Client-Schnittstellen
  - Unbegrenzte Anzahl Schnittstellen
  - individuelles X.509-Zertifikat möglich
  - Eigene Firewall-Konfiguration je OpenVPN-Client-Schnittstelle
  - Optionale Prüfung von nsCertType, keyUsage/ extendedKeyUsage oder CommonName/DN des Server-Zertifikats
  - Beziehen der Konfiguration vom Server (pull)

4.3 SSH TCP-Weiterleitung

- Authentifizierung mit SSH RSA-Schlüsseln
- Konfiguration je Benutzer
- Für beliebige TCP-Ports und Ziel-IPs

4.4 Webclient

- Zugriff auf RDP-, VNC- und SSH-Server mit HTML5-fähigem Web-Browser
- Konfiguration je Benutzer
- Lizenzierung nach Anzahl gleichzeitiger Verbindungen
- RDP
  - Zwischenablage zur Übertragung von Text
  - Optional emulierter Drucker (öffnet lokal ein PDF-Dokument)
  - Optional emulierte Dateiübertragung (Up-/Download im Browser, Netzwerkfreigabe im RDP-Server)
- VNC
  - Passiver Modus konfigurierbar
- Auf Docker basierter Software-Container
- Abgesicherte Laufzeitumgebung
- Zugriff über Reverse-Proxy
- HTTP, HTTPS oder HTTPS mit Client-Zertifikaten
- Optionale Zweifaktor-Authentifzierung mit zeitbasierten Einmalpasswörtern (TOTP)

5 Firewall

5.1 Standard-Firewall

- Basierend auf GNU/Linux iptables Firewall
- Anzahl gleichzeitiger Verbindungen abh. vom Hauptspeicher
  - 65.536 bis 4 GB
  - 262.144 über 4 GB
  - kann auf Anfrage erhöht werden
- Integriertes Stateful-Inspection-Regelwerk
- Integrierte Plausibilitätsprüfungen (z.B. Adress-Spoofing)
- SNAT und DNAT
- Zonenbasierte Konfiguration
  - vier vordefinierte Vertrauensstufen
  - freie Zuweisung der Vertrauensstufen an Schnittstellen
- Aufbau der Firewall-Regeln
  - optionales Logging je Regel
  - Regeltypen allow, drop, reject (nicht bei DNAT)
  - einzeln deaktivierbar bzw. mit Gültigkeitsende (Datum und Uhrzeit)
  - optional mit Gültigkeit nach Wochentag und Uhrzeit
  - Protokoll-/Port-Signaturen objektbasiert
  - Quelle/Ziel optional objektbasiert (u.a. Gruppen, DNS, Geolokation auf Länderebene)
  - MAC-Adresse als Quelle (objektbasiert)
  - Bereiche (von-bis) für Quelle/Ziel möglich
- Statistik der letzten 12 Monate mit
  - Jahresübersicht (graphisch und numerisch)
  - Monatsübersichten gesamt und je Schnittstelle (numerisch)
  - Tagesübersicht (graphisch und numerisch)
  - Stundenübersicht (graphisch)
  - Top Schnittstellen eingehend, ausgehend, weitergeleitet je Monat (numerisch)
  - Top Dienste abgewiesen, verworfen je Monat (numerisch)
  - Top Quell- und Zieladressen je Monat (numerisch)
  - IP-Adressen anonymisiert

5.2 Dynamische Firewall

- Sensoren für Denial-of-Service, Portscan, Portsweep
- reputationsbasierter Algorithmus basierend auf Information aus Standard-Firewall und Sensoren
- je Schnittstelle zeitlich begrenzte Sperre auffälliger Quell-Adressen aktivierbar
- konfigurierbare IP-Whitelist
- Anzeige des Status aller aktuell bekannten IPs mit Löschmöglichkeit

5.3 Intrusion-Detection und -Prevention

- Integrierte Signatur-Datenbank
- Aktualisierung mehrmals pro Woche *)
- Signatur-Whitelist
- Protokollierung
  - Datum / Uhrzeit
  - Regel-ID
  - Kurzbeschreibung
  - Klassifizierung
  - IP-Signatur
  - Paket-Dump über Logdatei-Ansicht der Administrationsoberfläche

Einzelne Leistungsmerkmale sind nicht in allen angebotenen Modellen enthalten.
**) innerhalb der Versionsreihe 7.1 nur auf Geräten mit Software-Pflegevertrag verfügbar.*

- Intrusion Prevention in allen Schnittstellen mit Default-Route
  - Auswählbare erweiterte Signatur-Gruppen
  - Blockade verdächtiger Verbindungen
- Intrusion Detection über Netzwerkkarte an Monitor-Port eines Switches
  - Auswählbare erweiterte Signatur-Gruppen
  - Protokollierung verdächtiger Pakete
- Zugriffs-Statistik der letzten 12 Monate mit
  - Jahresübersicht (graphisch und numerisch)
  - Monatsübersicht (numerisch)
  - Tagesübersicht je Monat (graphisch und numerisch)
  - Stundenübersicht je Monat (graphisch)
  - Top Ereignisse nach Priorität je Monat (numerisch)
  - Top Quell-Adressen je Monat (numerisch)
  - Top Dienste je Monat (numerisch)
  - IP-Adressen anonymisiert

5.4 Bandbreiten-Management / QoS

- Je DSL-, Ethernet- und VLAN-Schnittstelle separat konfigurierbar
  - Ausgehende Bandbreite
  - Eingehende Bandbreite (bei Aktivierung verringert sich die nutzbare Bandbreite um 20%)
  - Priorisierung nach Port und IP-Adressen
  - Anzahl Gespräche und Codec für VoIP
- Priorisierung und VoIP in IPSec-Verbindungen
- Klassifizierung über Diffserv-Paketmarkierung (DSCP)
- Quality-of-Service-Modul für Voice-over-IP
  - Optimierung der Latenzzeit
  - Erkennung der Datenpakete über Diffserv-Markierung DSCP EF
- Vier weitere Prioritäts-Klassen
  - Mindestbandbreite anteilig auf Gesamtbandbreite abzgl. VoIP
  - leere TCP-Ack-Pakete (10%)
  - Benutzerdefiniert Hochprior (50%)
  - Standard (20%)
  - Benutzerdefinert Niederprior (20%)
- Dynamische Verteilung ungenutzter Bandbreite auf niedrigere Klassen

6 Proxies / Application-Gateways

6.1 Web-Proxy

- Protokolle HTTP, HTTPS (mit CONNECT), FTP (über HTTP)
- Transparenter Proxy für HTTP zu Port 80 und HTTPS zu Port 443
- Browserkonfiguration über Web-Proxy Auto-Discovery (WPAD) via DNS und DHCP
- Vorgefertigte, konfigurierbare Proxy-Autoconf-Datei
- Einbindung in Proxy-Hierarchie möglich
- Virenscan von Downloads (Virenscanner-Lizenz nicht enthalten)
  - Maximale Dateigröße einstellbar (bis 2 GB)
  - Ablehnen oder Pass-Through für größere Dateien
  - Quarantäne-Bereich für Problemfälle
- Maskierung von HTML-Tags zur Ausblendung aktiver Inhalte wie ActiveX
  - für object, embed, applet und Script-Sprachen
  - Whitelist für Class-ID, Content-Typ und Java-Klasse
- Beschränkungen für CONNECT-Methode
  - nur zu definierten Ports oder Server/Port
  - CONNECT zu IP-Adressen kann gesperrt werden
  - Prüfung der SSL-Version
  - Optionales Aufbrechen der Verschlüsselung für Filterung in HTTPS-Verbindungen
- Prüfung oder Blockade von Content-Typen
- Content-Typ-Filter
  - Abgleich des Content-Typs mit Daten
  - Blockade unerwünschter Content-Typen
- Server Whitelist für Virenscan, Tag-Maskierung, Content-Typ- und SSL-Filter
- Zugriffskontrolle über Client-IP
- Benutzer-Authentifizierung
  - Basic-Auth: Benutzerverwaltung intern oder über LDAP
  - Digest-Auth: Benutzerverwaltung intern
  - NTLM-Auth: Single Sign-on über ActiveDirectory
  - Schutz vor Weitergabe der Zugangsdaten durch Erkennung von Mehrfachanmeldungen
  - Deaktivierbar für einzelne Client-IPs und Ziel-Adressen
- URL-Filter
  - Konfiguration nach Benutzer-Gruppe oder Client-IP/-Netzwerk
  - Benutzergruppen intern oder über ActiveDirectory
  - Uhrzeitabhängige Konfiguration
  - In Kategorien organisierter URL-Datenbank
  - Benutzerdefinierte Domainlisten
  - Zugriffskontrolle anhand Endung des Dateinamens
  - Zugriffskontrolle für Adressen mit pornographischen Schlüsselwörtern
  - optionale Protokollierung geblockter Zugriffe
- 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-Domains je Monat (numerisch)

6.2 FTP-Proxy

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

6.3 Reverse-Proxy

- Reverse-Proxy und Load-Balancer für HTTP und HTTPS
- Optionales SSL-Offloading
- HTTPS-Server Zertifikat je Port
- Konfigurierbare Strict-Transport-Security bei HTTPS
- Optional Authentifizierung mit Basic-Auth oder Client-Zertifikat
- Unterstützung für Web-Socket-Protokoll
- Syntax-Prüfung von Anfragen zum Schutz vor Angriffen
- Größenbeschränkung für Uploads
- Reverse-Proxy Funktion mit
  - Zugriff auf DEFENDO-Dienste
    - Administrationsoberfläche
    - Freigabelinks für E-Mail Quarantäne
    - Groupware-App
    - Web-Client-App
  - Zugriff auf Exchange-Dienste mit separater Freigabe für
    - Outlook-Web-App (OWA)
    - Exchange-Admin-Center / -Control-Panel (EAC/ECP)
    - Active-Sync
    - RPC/Outlook-Anywhere
    - MAPI-über-HTTP
    - Exchange Web-Services (EWS)
    - Autodiscover
  - Zugriff auf Remotedesktop-Gateway und RD-Web-Access
  - Zugriff auf benutzerdefinierte Backends
  - konfigurierbarer Redirect für Startseite
  - Virtuelle Hosts

- 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-Länder je Monat (graphisch und numerisch)

6.4 POP3/SMTP-Proxy

- Transparenter Proxy für POP3 und SMTP
- interne Kommunikation unverschlüsselt
- externe Kommunikation wenn möglich verschlüsselt mit optionaler Zertifikatsprüfung
- E-Mail Virenscan (Virenscanner-Lizenz nicht enthalten)
  - Prüfung ein- und ausgehender E-Mails
  - Optional E-Mail-Benachrichtigung des Administrators
- Optional SPAM-Filterung bei POP3
  - Konfigurierbarer Schwellwert zum Markieren
  - Verwendet globale SPAM-Filter-Konfiguration aus Mail-Server

6.5 SIP-Proxy

- SIP Outbound-Proxy für ein- und ausgehende IPv4-Verbindungen
- Integrierter RTP-Proxy
- Transparenter Proxy
- Nutzung als Registrar möglich
- Zugriffskontrolle über Client-IP
- Registrierung nur von Clients über LAN-Schnittstelle eth0
- Entfernen konfigurierbarer Header in ausgehenden Paketen

6.6 SOCKS-Proxy

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

7 Mail-System

7.1 Mail-Server

- Protokolle SMTP und ESMTP
- Konfigurierbare TLS-Verschlüsselung mit optionaler Verifikation von Server-Zertifikaten
- Empfang eingehender E-Mails
  - Direkter Empfang per SMTP
  - Abholung mit DEFENDO POP/IMAP-Client
- Zustellung eingehender E-Mails an interne Mail-Server
  - Weiterleitung ganzer Domains oder einzelner Adressen
  - Vor Annahme der Mail auf DEFENDO optionale Prüfung von Absender- und Empfänger am internen Mail-Server per SMTP oder LDAP
- 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 beliebig viele Adressen je Empfänger-Postfach
  - Zeitlich begrenzbare Abwesenheits-Schaltung mit Auto-Reply und/oder Weiterleitung
  - Optional eigener Ordner für als SPAM markierte E-Mails
  - Täglicher E-Mail-Report über neue Mails im SPAM-Ordner
  - Automatische Löschung von Mails aus SPAM-Ordner nach konfigurierbarer Anzahl von Tagen
  - Zugriff via DEFENDO Groupware-, POP3- oder IMAP4-Server
- Mail-Relay für ausgehende E-Mails
  - 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
  - unterschiedliche Relay-Server je Absender-Domain möglich
  - SMTP-Auth Methoden LOGIN, PLAIN, CRAM-MD5, DIGEST-MD5
  - Synchronisation mit Verbindungsaufbau von PPP Wählverbindungen
- Konfigurierbare Obergrenzen
  - Anzahl gleichzeitiger Verbindungen
  - Anzahl gleichzeitiger Verbindungen je externer IP
  - Anzahl Verbindungen je externer IP und Minute
  - Anzahl Empfänger je Mail
  - E-Mail Größe
- PGP- / S/MIME-Filter
  - verbietet unverschlüsselten Versand zu konfigurierbaren Ziel-Adressen
- Optionales Unterdrücken von Lesebestätigungen (MDN)
- E-Mail Archiv-Funktion
  - Zustellung einer E-Mail-Kopie an beliebige Adresse
  - Getrennt für ein- und ausgehende E-Mails konfigurierbar
- Hinzufügen eines Textbausteins an ausgehende Mails
- Milter-Client zur Anbindung von Miltern über TCP/IP
- Einstellmöglichkeiten für berechtigte Benutzer über Administrations-Oberfläche:
  - Passwort
  - E-Mail Weiterleitung
  - Abwesenheits-Schaltung
  - 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-Merkmals-Kategorie je Monat (numerisch)
  - Top-Viren-Liste je Monat (numerisch)
  - Top-Empfänger-Domains je Monat (numerisch)

7.2 S/MIME-Gateway

- Basierend auf S/MIME
- Unterstützung des Domain-Zertifikat-Konzepts
- Als Domain-Zertifikat genutzte S/MIME-Schlüssel kostenfrei
- Individuelle S/MIME-Schlüssel gegen Aufpreis
- Entschlüsseln eingehender Mails
  - vor sicherheitsrelevanten Funktionen wie Virenscan oder Dateianhangsfilterung
  - Markierung im Betreff, optional über Sensitivity-Header
- Verifikation der Signaturen eingehender Mails
  - Markierung im Betreff
  - Optionale CRL-Prüfung
  - Benutzerdefinierte CAs je Absender-Adresse oder -Domain
  - Optionales Entfernen korrekter Signaturen
  - Konvertierung opaquer Signaturen zu Signatur als Anhang
  - Automatischer Import oder Import nach Freigabe von Zertifikaten für Verschlüsselung ausgehender Mails

- Signieren ausgehender Mails
  - Zuordnung der Schlüssel über Authentifzierung
  - Zuordnung der Schlüssel über Absender-Adresse für konfigurierbare IPs
  - Nutzung eines Domain-Zertifikats bei Versand an konfigurierbare Empfänger-Adressen oder -Domains
- Verschlüsseln ausgehender Mails
  - Kann über Schlüsselwort im Betreff oder Sensitivity-Header erzwungen werden
  - Manueller Import der Empfängerzertifikate
  - Automatischer Import beim Empfang signierter Mails
  - Manuelle Konfiguration von Domain-Zertifikaten

7.3 Anti-SPAM/Virus/Malware

- Schutzfunktion gegen SMTP-Slamming
- Prüfung des HELO/EHLO Namens
- Prüfung des Reverse-DNS Eintrags in zwei Stufen
- Prüfung der Absender-Domain in zwei Stufen
- Schutz vor CEO-Fraud durch Abweisen oder Markieren eingehender Mails mit lokalem Absender
- SPF-Filter mit IP-Whitelist
- Graue Liste (Greylisting)
  - Konfigurierbares Zeitverhalten
  - Absender- und Empfänger-Whitelist
  - Schwächster Modus: nur nach RBL-Prüfung
  - Optional freischalten von aktiv genutzen Adressen oder Antwort-Mails
- E-Mail Virenscan (Virenscanner-Lizenz nicht enthalten)
  - Prüfung ein- und ausgehender E-Mails
  - Extra Dekodier- und Entpack-Stufe zusätzlich zum Virenscanner
  - Rekursives Entpacken einer Vielzahl von Archivtypen
  - Schutz vor Denial-of-Service Angriffen
  - Optional E-Mail-Benachrichtigung des Administrators
  - Quarantäne Verzeichnis
- MIME-Dateianhangs-Filter
  - Erkennung von Office-Makros und Autostart Office-Makros
  - Sperrung von Dateianhängen basierend auf Dateinamens-Erweiterung
  - Modi für eingehende Mails: Annahme verweigern, Quarantäne des Anhangs, Quarantäne der Mail
  - Modus für ausgehende E-Mails: Annahme verweigern
  - Virenprüfung des Quarantäne-Verzeichnises nach jedem Signatur-Update der Scanner
  - Optionaler Benutzerzugriff auf Quarantäne (sofort, nach Signatur-Update oder zeitverzögert)
  - Absender-Whitelist
  - Liste kritischer Dateiarten und Makros (ohne Benutzerzugriff und Absender-Whitelist)
  - Black- oder Whitelisting weiterer Dateiarten und Makros (mit Benutzerzugriff und Absender-Whitelist)
  - Automatisches Löschen der Quarantäne nach konfigurierbarer Zeitdauer
  - Optional E-Mail-Benachrichtigung des Administrators
- 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
  - Optionale Inhaltsvorschau bei markierten Mails
  - Quarantäne-Empfänger für markierte Mails im globalen SPAM-Filter
  - Selbstlernender Bayes-Filter
  - Manuelles Lernen von SPAM/HAM über Webmail und IMAP-Ordner
  - Nutzung mehrerer RBL-Server
  - Nutzung von URIBL-Servern
  - Razor2-Client
  - Texterkennung (OCR) gegen Bilder-SPAM
  - Integrierte Signatur-Datenbank
  - Änderung der Signatur-Bewertung möglich
  - Benutzerdefinierte Regeln
  - Manuelle Black- und Whitelists
  - Extra-Bewertung von englischsprachigen E-Mails
  - Extra-Bewertung bei kyrillischem oder Fernost-Zeichensatz

7.4 POP/IMAP-Client

- Protokolle POP3, IMAP4, APOP und ETRN
- Weitere Varianten auf Anfrage
- TLS/SSL-Verschlüsselung mit optionaler Zertifikatsprüfung
- Abruf von beliebig vielen Server 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

7.5 POP3/IMAP-Server

- TLS-Verschlüsselung
- Benutzerdefinierte IMAP4 Unterordner
- UIDL Erweiterung

7.6 Groupware

- Zugriff via Webbrowser
- Zugriff mit ActiveSync, CalDAV, CardDAV gegen Aufpreis
- Die über ActiveSync verfügbare Funktionalität unterscheidet sich je nach Client
- E-Mail
  - Zugriff auf Postfach via IMAP
  - Suchfunktion
  - Markierung von Mails
  - IMAP-Label
  - Mail-Filter auf Sieve-Basis
  - Delegation mit "Senden als"
  - Weiterleitungsfunktion
  - Abwesenheitsnachricht konfigurierbar
- Adressbuch
  - Beliebig viele Adressbücher je Benutzer
  - Freigabe für andere Benutzer mit individuellen Berechtigungen je Adressbuch
  - Je ein gemeinsam gepflegtes und vom Administrator gepflegtes Adressbuch bereits angelegt
  - Globales Adressbuch mit lokalen Benutzern je Domain
  - Suchfunktion
  - Import im vCard- oder LDIF-Format
  - Export im LDIF-Format

- Kalender-Funktion
  - Beliebig viele Kalender je Benutzer
  - Verwaltung von Terminen und Aufgaben
  - Einstufung als öffentlich, vertraulich und privat
  - Freigabe für andere Benutzer mit individuellen Berechtigungen je Kalender und Einstufung
  - Je ein gemeinsam gepflegter und vom Administrator gepflegter Kalender bereits angelegt
  - Verschiedene Ansichten (u.a. Liste mit Filter, Tag, Woche, Monat)
  - Individuell einstellbare Farbe je Kalender
  - Ein- und Ausblenden je Kalender
  - Anzeige und Abfrage der Verfügbarkeit (Free/Busy-Information)
  - Versand und Bestätigungen von Einladungen per Mail
  - Optionale E-Mail-Benachrichtigungen
  - Kategorien mit farbiger Markierung
  - Suchfunktion
  - Import und Export im ICS-Format
- Auf Docker basierter Software-Container
- Abgesicherte Laufzeitumgebung
- Zugriff über Reverse-Proxy
- HTTP, HTTPS oder HTTPS mit Client-Zertifikaten

8 Viren-Scanner

8.1 Virenscanner

- Lizenzen nicht enthalten
- Scanner müssen separat erworben und installiert werden
- Parallele Installation mehrerer Scanner möglich
- Speziell an DEFENDO angepasste Versionen
  - Avira Anti-Virus
  - F-Secure Anti-Virus
  - Kaspersky Anti-Virus for Appliance Server
- Avira und Kaspersky: Optionale Cloud-Unterstützung (Abfrage von Hash-Werten)
- Automatische Signatur-Updates
  - Zeitgesteuerte Aktualisierung
  - Kürzestes Intervall stündlich
  - Nur geänderte Signatur-Dateien werden heruntergeladen
  - E-Mail Benachrichtigung im Fehlerfall
  - Optional E-Mail Benachrichtigung über jedes Update
- Engine-Updates Bestandteil der regulären DEFENDO-Updates

9 Weitere Komponenten

9.1 DHCPv4

- je Ethernet-, VLAN- und WLAN-Schnittstelle separat konfigurierbar
- DHCPv4-Server oder DHCPv4-Relay
- Secondary DHCPv4-Option
- Mehrere DHCPv4-Adressbereiche für dynamische Adressvergabe
- Konfigurierbare Lease-Dauer
- Feste Adress-Zuordnung anhand MAC-Adresse
- Konfigurierbare DHCP-Optionen
  - Domain-Name
  - Router
  - zwei DNS
  - zwei WINS
  - NetBIOS Knotentyp
  - WPAD-URL
  - Bootp
  - Benutzerdefinierte Optionen

9.2 DNS

- DNS-Forwarder
  - Zugriffskontrolle über Quell-IP
  - Client-Schutz durch Prüfung der Antwort-Pakete
  - optionaler Schutz vor Rebind-Attacken
  - optional DNSSEC-Validierung
  - Caching
  - Konfiguration von Forward-Zonen
  - Auflösung über feste Forwarder und/oder Root-Server
  - Automatisches Beziehen der Forwarder bei PPP- oder DHCP-basierter Internet-Verbindung
  - Response-Policy-Zone zum Überschreiben von DNS-Informationen
- 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

9.3 Client für dynamisches DNS

- Konfigurierbar je Schnittstelle mit dyn. IP
- Unterstützung verschiedener Anbieter/Protokolle
  - DynDNS
  - easyDNS
  - ZoneEdit
  - Hammernode
  - FreeDNS
  - No-IP
  - benutzerdefinierte URL
- Aktualisierung bei Bezug einer neuen IP

9.4 FTP-Server

- Anonymous FTP-Server
  - Pflege über vordefinierten Benutzer
  - Deaktivierbar
  - Optionaler Upload-Bereich
- 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

9.5 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

9.6 NTP Zeit-Server

- Synchronisation mit beliebig vielen Internet-Zeitservern
  - laufend, täglich oder wöchentlich

Einzelne Leistungsmerkmale sind nicht in allen angebotenen Modellen enthalten.
**) innerhalb der Versionsreihe 7.1 nur auf Geräten mit Software-Pflegevertrag verfügbar.*