

Secure Email Gateways – Vergleichsübersicht

- Email Appliance 4.0 (SEA)
- UTM 9.4 (UTM)
- XG Firewall / SF-OS v15 (SF-OS)
- Email on Sophos Central 1.0 (Central)
- (PureMessage for Unix (PMX) für nächste Revision geplant)

Lizenzmodell

		UTM	SF-OS	SEA	Central
Hardware Appliance	Lizensierungsgrundlage	Hardware	Hardware	Anzahl Benutzer	-
	Lizenzkosten	Preis der Hardware + E-Mail Subscription + Premium Support (optional)	Preis der Hardware + E-Mail Subscription + Enhanced Plus Support (optional)	Hardware + Sophos E-Mail Protection Subscription (# users) + Enhanced Plus Support (optional)	-
Virtuelle Appliance	Lizensierungsgrundlage	Pro virtuelle Appliance lizenziert nach # Benutzer (IP Adressen)	Pro virtuelle Appliance lizenziert nach vCPU/RAM	Bis 10 virtuelle Appliances beinhaltet, Anzahl Benutzer	-
	Lizenzkosten	Preis für Anzahl IP-Adressen oder Mailboxen (was höher ist) + E-Mail Subscription + Premium Support (optional)	Software Basis Lizenz + E-Mail Subscription + Enhanced Plus Support (optional)	Sophos E-Mail Protection subscription (Anzahl Benutzer) + Enhanced Plus Support (optional)	-
SaaS		bring your own license			Anzahl Benutzer

Technischer Vergleich

		UTM	SF-OS	SEA	Central
Protokolle	SMTP/S	x	x	x	x
	POP3	x	x		x
	IMAP		x		
Threat Protection	Malware Scanning (Anzahl AV)	2	2	1	1
	Unscannable Attachment Handling	x		x	
	Encrypted Attachment handling	x	x	x	
	Attachments Stripping (True File Type)	x	x	x	
	DKIM	x		x	
	SPF	x		x	x
	Sandstorm	x		x	
	Time of click protection			x	
Anti-SPAM	Snowshoe spam protection (Delay Queue)			x	
	Sender Genotype Reputation	x		x	
	Live Anti-Spam (SXL)	x	x	x	
	IP Reputation Filter	x	x	x	x
	Greylisting	x			
	Block / Allowlist	x	x	x	x
	RDNS	x		x	x
	BATV	x		x	
	Recipient validation	x		x	x
	Reject-before-Accept SMTP	x			x
	Quarantine/Report	x	x	x	x
	Quarantine/Portal	x	x	x	x
	Add Header	x		x	
	Add Subject	x	x	x	
	Harvesting Protection	x	x	x	x
Inhaltsfilter	Sophos Content Control Lists CCL	x	x	x	
	Text Filter/Regex	x		x	
	Offensive Language Filter			x	
	Bulk Mail Filter			x	
	Header Check	x	x	x	x
	Source IP Check	x	x	x	
	Aktive Inhalte	x	x	x	x
	E-Mail Größe gesamt	x	x	x	
	Anhang Größe			x	
	Country/GeoIP	x			
	pro Gruppe		x	x	
	pro Domäne	x	x	x	

Technischer Vergleich

		UTM	SF-OS	SEA	Central
Policy Aktionen	Outbound Scanning	x	x	x	
	Add Footer	x		x	
	Weiter zur nächsten Regel			x	
	Löschen nach dieser Regel			x	
	Verwerfen		x	x	x
	In die Quarantäne schieben	x	x	x	x
	Kopie in Quarantine und Zustellen			x	
	Re-Route zu anderem Server			x	
	Re-Route zu weiterem Empfänger			x	
	Kopie zu anderem Server			x	
Tag in Betreff und Zustellen	x	only Spam	x		
Integrationen	HA	x	x	x	x
	Active Directory	x	x	x	x
	Lotus Domino			x	
	Lotus Domino (Groups by OU)			x	
	Novell eDirectory	x	x	x	
	OpenLDAP	x	x	x	
	Sun JSMS			x	
	SNMP	x	x	x	
	Syslog	x	x	x	
	Sophos Managed Appliance			x	
	Hardware Monitoring			x	
Quarantine-Backup			x		
Sonstiges	TLS	x	x	x	x
	SPX	x	x	x	
	S/MIME Encyption	x			
	PGP Encryption	x			
	Smarthost Routing	x		x	x
	Domain based routing	x		x	x
	Adress based routing	x			x
	End to End Message forensics			x	
	Reporting	x	x	x	
	Header Filtering			x	
	Adresse umschreiben		x	x	
Domäne umschreiben			x		

Fallbeispiele

Beispiel 1:

Unternehmen mit 100 MA, ein Standort. Eine ältere UTM eines anderen Herstellers ist im Einsatz, die nicht mit E-Mail Security belastet werden soll. Außerdem soll ein besserer Schutz vor aktuellen Krypto-Trojanern bereitgestellt werden.

Empfehlung: ES100 mit Mail Protection Advanced für 100 User und Sandstorm.

Beispiel 2:

Unternehmen mit 400 Mitarbeitern, drei Standorte mit lokalen Breakouts. Sophos UTM ist bereits vorhanden. Derzeit wird nur Websecurity genutzt. E-Mail Security und besserer Schutz vor aktuellen Krypto-Trojanern soll bereitgestellt werden.

Empfehlung: SG 330 Email Subscription für 400 User plus Sandstorm, je eine SG230 Appliance an jedem Standort mit max. 100 User. Upsell Möglichkeit auf FullGuard.

Case 3:

Unternehmen mit 4000 Mitarbeitern, 3 Standorte mit GigaBit MPLS/Standleitungen zwischen den Standorten, ein zentraler Breakout. Kunde setzt momentan Cisco IronPort ein und möchte besseren Schutz vor aktuellen Bedrohungen haben.

Empfehlung: 2 x ES5000 and Mail Protection Advanced für 4000 User im Hauptstandort und Sandstorm.

Case 4:

Unternehmen mit Microsoft Exchange Online, Office 365, Google Apps for Work oder gehosted Email Dienste im Einsatz und Bedarf für erweiterten Schutz und Ausfallsicherheit.

Empfehlung: Email auf Sophos Central

General recommendations

		UTM	SF-OS	SEA	Central
	UTM eines anderen Hersteller im Einsatz	SG Hardware	XG Hardware		
	Dedicated Firewall / Email / Web Gateways in place			Hardware or virtual E-mail Appliance(s)	
	Multiple locations with local Firewalls/Breakouts				
	Protection against current threats with Sandstorm	Hardware or virtual UTM			
	Exchange-Online / Office 365 customer				x

Sophos GmbH
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Deutschland

Amtsgericht Wiesbaden HRB 25915,
Ust.-ID Nr. DE189 689 369

Tel.: +49 (0)611 5858-0
Fax: +49 (0)611 5858-1042
E-Mail: info@sophos.de