SOPHOS
Security made simple.

Sophos Secure Web Gateways - Vergleichsübersicht

- Web Appliance 4.3.1 (SWA)
- UTM 9.4 (UTM)
- XG Firewall / SF-OS v16.05 (SF-OS)
- Web in Sophos Central (Stand 02/2017)

Lizenzmodell

		UTM	SF-OS	SWA	Central Web
Hardware-Appliance	Lizensierungs-grundlage	Hardware-Modell	Hardware-Modell	Anzahl User	Anzahl User
	Kosten	Preis der Hardware + Web Subscription + Premium Support (optional)	Preis der Hardware + Web Subscription + Enhanced Plus Support (optional)	Preis der Hardware + Sophos Web Protection Subscription (für Anzahl User)	-
Virtuelle Appliance	Lizensierungsgrundlage	Pro virtuelle Appliance lizensiert nach Usern (IP-Adressen)	Pro virtuelle Appliance lizensiert nach CPU-Cores/RAM	Bis zu 10 Appliances beinhaltet, lizensiert nach Anzahl User	Pro User
	Kosten	Preis der Lizenz für X IP-Adressen + Web Subscription + Premium Support (optional)	Software Base License + Web Subscription + Enhanced Plus Support (optional)	Sophos Web Protection Subscription (für Anzahl User) + Enhanced Plus Support (optional)	Subscription per User Lizenz Web-Gateway in Central

Technischer Vergleich

		UTM	SF-OS	SWA	Central Web
Funktionen	HTTP Scanning	x	x	x	
	HTTPS Scanning	x	x	x	
	FTP over HTTP Scanning	x	x	x	
	Native FTP Scanning	x	x		
	Bandbreitenmanagement	x (eingeschränkt)	x		
	Caching Proxy	x	x	x	
AV	Anti-Viren Scanner (# Engines)	2	2	1	
	Sandstorm	x		x	
	Sandstorm selective			x	
	Sandstorm Datacenter			x	
Synchronized Security	Security Heartbeat mit Cloud Endpoints		x		
	Netzwerk-NAC (VPN, WLAN) mit SMC	x			
	Konfig-Verteilung (VPN, WLAN) mit SMC	x			
	Kann Policy für SEC Endpoints bereitstellen	x		X	
Redundanz / Deployment	Active-Standby (HA)	x	x	x (per Sophos Mgmt Appliance oder Load Balancer)	
	Active-Active	x	x (2 XGs)	x (per Sophos Mgmt Appliance oder Load Balancer)	
	Expliziter Proxy	x	x	x	
	Transparent L2	x	x	x (B-Modell, 2 IF)	
	Transparent L3	x	x		
	Transparent mit WCCP			x	
	Als Router mit mehreren Interfaces	x	x		
	Parent Proxy pro	FQDN		FQDN/Domain	
	PAC File Hosting	x			
Management / Logging / Reporting	Zentrales Management	x (eingeschränkt)	x	x	
	Reporting on Box	x	x	x	
	Reporting per iView2	x	x		
	Externes Logging (Syslog)	x	x	x	

	Rollenbasierte Administration	x (eingeschränkt)	x	x	
	Log-Anonymisierung	x	x	x (Ausblenden)	
	Sophos Managed Appliance			x	

		UTM	SF-OS	SWA	Central Web
Filterung	URL Filter	x	x	x	
	Applikationskontrolle	> 1.400 Applikationen/ Funktionen	> 2500 Applikationen/ Funktionen	Wenige Social Apps, aber feinkörnig einstellbar	
	Blacklist/Whitelist per Domain/URL	x	x	x	
	Blacklist/Whitelist per Regex/Wildcard	x	x		
	MIME Dateityp	x	x	x	
	Dateierweiterung	x	x		
	Country/GeoIP	x	x		
	Aktive Inhalte	x	x	x	
	Dateigröße	x	x		
	Surfing Quota	x	x	x	
	"Block Override"	x	geplant		
	Feedback zur Rekate-gorisierung/Freischal tung			x	
	SafeSearch	x	x	x	
	Youtube für Schulen	x	x	x	
Authentisierung	Lokale User-DB	x	x		
	RADIUS	x	x		
	TACACS+	x	x		
	Active Directory	x	x	x	
	Novell eDir	x	x	x	
	Apple OpenDir	x	x		
	OpenLDAP/Generic LDAP	x	x		
	Browser/User agent		x	x	
	Windows Agent	x	x		
	SSO NTLM/NTLMv2	x	x	x	
	SSO Kerberos	x		X	
	SSO using RADIUS		x		
	SSO in bridged/ transparent Mode	x	x	x	
	SSO mit AD Controller Integration (STAS)	x	x		
	SSO mit Terminal Server Integration (STAC)		x		

	IP-Addresse	x	x	x	
	Captive Portal		x	x	

Fallbeispiele

Fallbeispiel 1:
Unternehmen mit 100 MA, ein Standort. Eine ältere UTM eines anderen Herstellers ist im Einsatz, am Endpoint ein Wettbewerber. Es soll Webfilterung inkl. Applikationskontrolle genutzt werden und besserer Schutz vor aktuellen Krypto-Trojanern bereitgestellt werden.

Empfehlung: SG Hardware mit Web und Netzwerksubscription zzgl. Sandstorm.
Cross-Sell Opportunity: FullGuard, WLAN-APs, SEC Endpoint

Fallbeispiel 2:
Unternehmen mit 400 MA, drei Standorte mit lokalen Breakouts. Firewall eines Mitberwerbers vorhanden.
Webfilterung soll genutzt werden und besserer Schutz vor aktuellen Krypto-Trojanern bereitgestellt werden.

Empfehlung: SWA für 400 User plus Sandstorm, je eine virtuelle Appliance an jedem Standort
Cross-Sell-Opportunity: SEC Endpoint

Fallbeispiel 3:
Unternehmen mit 4000 Mitarbeitern, 3 Standorte mit GigaBit MPLS/Standleitungen zwischen den Standorten, ein zentraler Breakout. Kunde hat SEC Endpoint im Einsatz. Kunde setzt momentan BlueCoat/IronPort ein und möchte besseren Schutz vor aktuellen Bedrohungen.

Empfehlung: 2 große Hardware-Web-Appliances (WS5000) am zentralen Standort plus Sandstorm

Fallbeispiel 4:
Unternehmen mit 1000 MA, ein Hauptstandort, 10 kleine Außenstellen, Kunde schaut sich gerade Sophos Cloud Endpoint an, ist überzeugt von Synchronized Security Ansatz

Empfehlung: Größere XG am zentralen Standort, XG85 in den Außenstellen, Cloud Endpoint Advanced/Cloud EndUser Protection
Cross-Sell-Opportunity: Cloud Endpoint/Mobile, FullGuard, WLAN-APs

Generelle Empfehlungen

	UTM	SF-OS	SWA
UTM eines anderen Herstellers im Einsatz	Hardware-UTM	Hardware-XG	
Dedizierte Firewall / Email / Web Gateways im Einsatz			Hardware oder virtuelle SWA(s)
Mehrere Standorte mit lokalen Firewalls/Internet-Breakouts.			Hardware oder virtuelle SWA(s)
Schutz vor aktuelle Bedrohungen per Sandstorm	Hardware oder virtuelle UTM		Hardware oder virtuelle SWA(s)
SEC-Endpoints im Einsatz	Hardware oder virtuelle UTM		Hardware oder virtuelle SWA(s)
Partner möchte als MSP auftreten und Sophos Central zur Verwaltung nutzen		Hardware- oder virtuelle XG	
Cloud Endpoints/Server im Einsatz		Hardware- oder virtuelle XG	

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

SOPHOS