

GYM Bilgi ve İletişim Hizmetleri

Bilgi Güvenliđi Ürünleri Katalođu



Giriş

GYM Teknoloji'nin Security, yani Bilgi Güvenliği ürünleri üç sınıfa ayrılmaktadır;

1. Bilgi Sızdırmayı Engelleme Sistemi :

DLP (Data Loss Prevention) diye adlandırılan bu sistemle, gizli ve önemli bilgilerin şirket dışına çıkarılması engellenir. Yazacağınız kurallarla, istediğiniz her türlü engellemeyi yapabilirsiniz. Örneğin belli dosyaların taşınabilir belleklere kopyalanmasını kısıtlayabilir, hatta sadece istediğiniz özellikteki veya markadaki belleklere kopyalanabilmesini saptayabilirsiniz. Değerli verilerin, çeşitli uygulamalarla (e-mail, P2P, ftp) veya LAN bağlantılarıyla transfer edilmesini de sınırlandırabilirsiniz. Aynı şekilde print almayı, CD'ye yazdırmayı, kopyala-yapıştır yapmayı, vb. birçok işlemi engelleyebilirsiniz. Finans, tıp, sigortacılık gibi birçok sektörde ihtiyaç duyulan bu işlev sayesinde, artık şirket kaynakları / değerleri (örneğin müşteri veritabanı) şirket içinde kalacak, çalınamayacak.

DLP ile koruma altına aldığınız kaynaklar üzerinde yapılan tüm işlemler monitor edilebilir.

Basel II gibi oluşumların da ön şart olarak istediği bir sistemdir.

2. Logların Güvenli Saklanması :

5651 sayılı kanun ve TK yönetmeliği gereği sistem loglarının elektronik zaman damgasıyla imzalanarak saklanması zorunludur. Üstelik bu loglar edit edilemez ortamlarda tutulmalıdır. Sistem loglarından kasıt, sistemde yapılan tüm aktivitelerdir (Gönderilen e-mailler, veritabanına yapılan erişimler,vb.). Bunlar ileride delil olarak başvurulmak üzere, en az bir yıl, değiştirilemez şekilde muhafaza edilmelidir.

3. İç ve Dış Tehlikelerden Korunma (UTM = Unified Threat Management)

UTM, security pazarındaki firewall uygulamalarında yükselen bir trenddir. Geleneksel firewall 'un, sadece saldırılara (intrusion) karşı koruma sağlamakla kalmayan, bunun yanında içerik ve spam filtreleme yapan (content / spam filtering) ve de antivirüs işlevi gören bir sisteme dönüşümüdür.

Önceleri IT birimleri, mevcut firewall'larına ilaveten antivirüs gatewayleri satın alırlardı. Bunun üzerine bir de içerik filtreleme ve spam engelleme sistemleri aldılar. Sonunda sistem odalarında bir yığın cihaz karmaşası oluştu. Günümüzde, tüm bu işlevleri ve daha fazlasını UTM denen tek bir platformla yapabilmekteyiz.

1. DLP – Data Loss Prevention

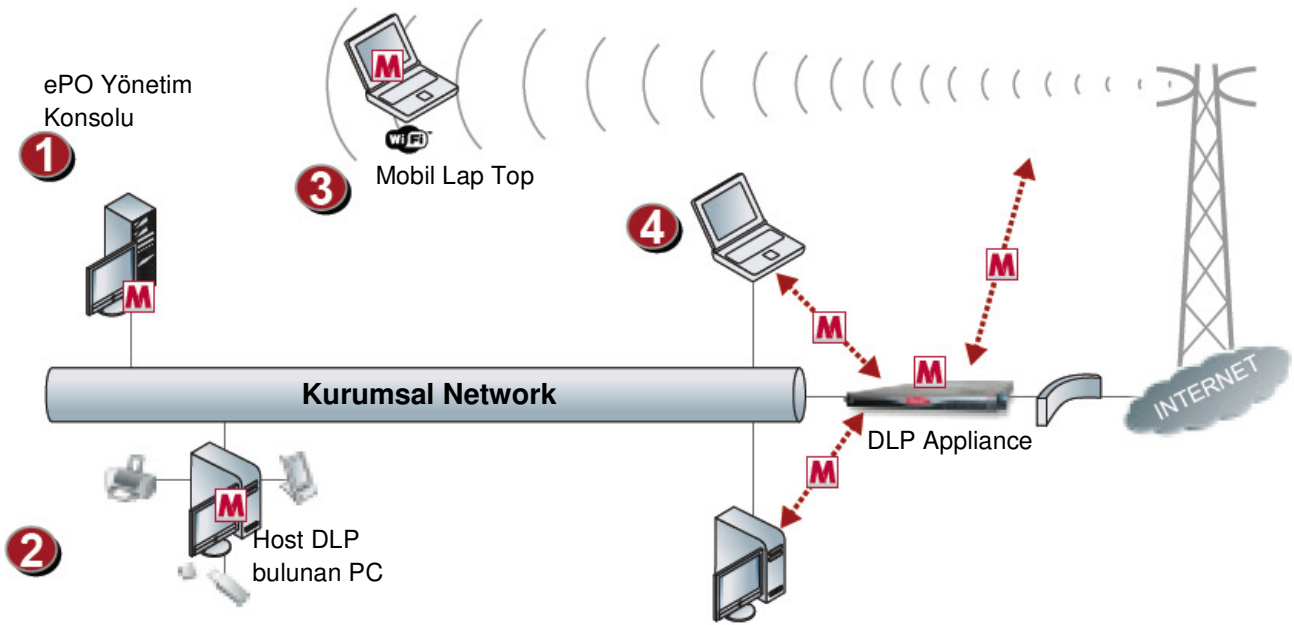
Kurumlar her tarafta dolaşan verilerini koruma çareleri aramaktadırlar. Bu veriler harici hırsızlardan çok bizzat kendi çalışanları tarafından, bilerek ya da bilmeyerek, dışarıya çıkarılır. Bu da maddi kayıplar yanında reputasyon ve iş kaybına sebep olmaktadır.

McAfee®

DLP işleyiş prensibi:

- Şirketin sahip olduğu veriler sınıflandırılır, muhtemel sızma yolları ve sızmayı engellemek için policy'ler belirlenir. Örneğin belli dosyalar bir yönetici onayı olmadan e-mail olarak yollanamaz.
- Belirlenen tedbirler kural olarak yazılır.
- Bu kurallar dahilindeki tüm aktiviteler monitor edilir.

1.1 DLP Mimarisi



1 ePO Yönetim Sunucusu
Merkezi olarak policy yönetimi, izlenmesi, raporlanması.

2 Host DLP ve Şifreleme: Risk oluşturabilecek kullanıcı davranışlarını engeller. Çalınlmalara karşı diski, tüm dosya ve klasörlerle birlikte şifreler.

3 Mobil kullanıcılar için Şifreleme: Hassas verileri tutmak için şifrelenmiş korumalı alan oluşturur. Verilerin bütünlüğünü ve gizliliğini korur.

4 DLP Appliance
Çıkan SNMP, HTTP gibi trafikler kontrol edilir. Harici medyalarla etkileşim kontrol edilir.

1.2 Teknik Özellikleri



Network DLP Appliance 1650



Network DLP Appliance 3650

Veri Depolama Kapasitesi	500GB	6TB
Drive Bay Sayısı	4	16
Disk Kapasitesi	500GB	500GB
Disk Teknolojisi	SATA 2	SATA 2
RAID	RAID-1	RAID-1 ve RAID-5
Sistem Hafızası	16Gb	16GB
Network interface	10/100/1000T 2 Adet	10/100/1000T 2 Adet

2.1 Log Saklama Sistemi - loglogic



loglogic™

- **Veri Toplama**

Log tutabilen her cihazdan sürekli olarak logları alır

- **Analiz**

Gerçek zamanlı ya da eski, bilinen ya da bilinmeyen tüm logları indexler ve analiz eder

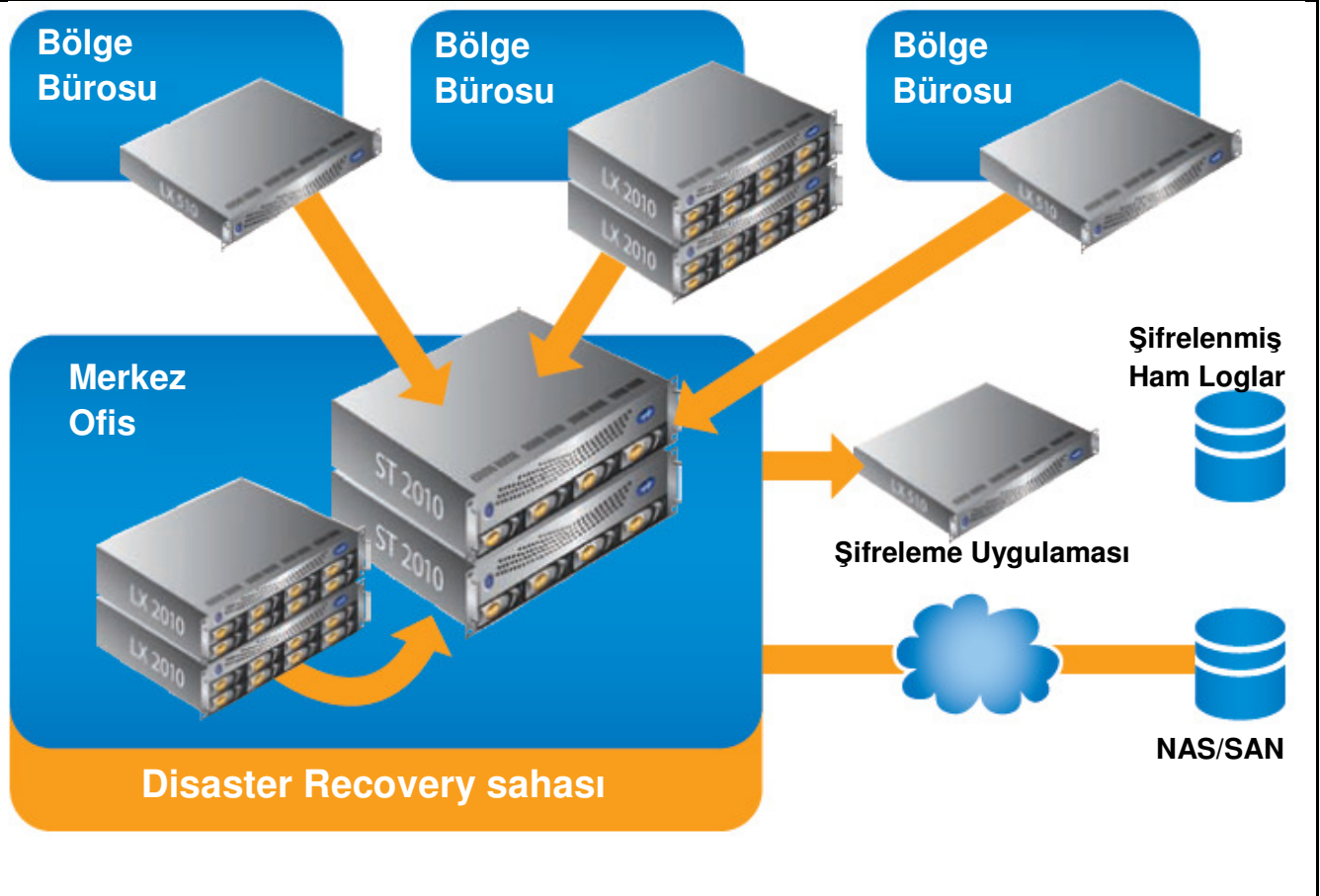
- **Kullanım Kolaylığı**

Web tabanlı olarak uzaktan yönetilebilir.

- **Saklama**

Ham ve işlenmiş tüm log dataları edit edilemeyecek bir şekilde depolar. Bu veriler kanuni açıdan delil kabul edilir.

2.1.1 Loglogic Mimarisi



2.1.2 Teknik Özellikleri

	LX510	LX1010	LX2010	ST2010	ST3010
Mesaj Saklama Hızı (Sn)	500	1500	4000	75000	75000
Sıkıştırma Oranı	12:1	12:1	12:1	12:1	12:1
Ham Depolama Kapasitesi	250GB	250GB	2TB (RAID 10)	500GB (RAID 1)	4TB (RAID 5)
Ham Depolama Ömrü	90 gün (Metalog)	90 gün (Metalog)	90 gün (Metalog)	Sonsuz (SAN/NAS Desteği)	Sonsuz (SAN/NAS Desteği)
CPU	Tek işlemci	Tek işlemci	Çift işlemci	Çift işlemci	Çift işlemci
Maksimum Güç Tük.	200W	200W	500W	500W	500W
Ethernet	1x10/100 1x10/100/1000	1x10/100 1x10/100/1000	1x10/100 2x10/100/1000	1x10/100 4x10/100/1000	1x10/100 4x10/100/1000

2.2 Log Saklama Sistemi – JUNIPER STRM



Özellik	Fayda
Merkezi komut ve kontrol sistemi	Log yönetimi, güvenlik bilgi ve olay yönetimi (SIEM), ve ağ davranışı anajiz sistemi tek bir konsoldan yönetilebilir. Bu sayede güvenlik yönetimi maliyeleri düşer ve IT verimliliği artar.
Ağ, güvenlik, uygulama, ve kimlik gibi unsurları takip etme.	Ağ ve güvenlik olaylarının, uygulamaların işlediği dataların ve tüm kimlik bilgilerinin merkezi olarak yönetimi sayesinde IT güvenlik vizyonunu yakalama yeteneğini artırır.
Gelişmiş tehlike ve güvenlik açığı tespiti.	STRM Serisinin eşsiz "offense management" özelliği sayesinde, diğer güvenlik unsurlarının kaçırdığı tehlikeler tespit edilir.
Yasalara uygun raporlama özelliği	5651 sayılı kanun ve TK yönetmeliği gereklerine uygun raporlama yapar.
Ölçeklenebilir log toplama ve arşivleme	STRM Serisi mimarisi, tüm enterprise networklerde logları ve olayları ölçeklendirir. Çok büyük ve dağıntık ağlarda bile çalıştırılabilir.

2.2.1 JUNIPER STRM – Teknik Özellikleri



STRM500

Hard Drives: 2 x 500 GB RAID 1
Memory: 8 GB
Maximum Events per Second: 500
Maximum Flows per Minute: 15, 000



STRM2500

Hard Drives: 6 x 250 GB RAID 5
Memory: 8 GB
Maximum Events per Second: 2500
Maximum Flows per Minute: 100, 000



STRM5000

Hard Drives: 6 x 500 GB RAID 10
Memory: 8 GB
Maximum Events per Second: 10,000
Maximum Flows per Minute: 400, 000

3. UTM – Unified Threat Management



UTM konusunda, McAfee'nin satın aldığı Secure Computing, Netasq ve Juniper Networks ürünleri ile güvenlik pazarındayız.



3.1 Secure Computing - Ürünlerimiz



Sidewinder UTM

Tek bir platformda tüm security fonksiyonları

- Firewall
- Intrusion Prevention (IPS)
- Anti-virus ve anti-spyware
- Anti-spam ve anti-fraud
- URL filtreleme
- SSL Decryption

Sidewinder UTM ailesinin modelleri : 210, 410, 510, 1100, 2100, 2150, 4150 dir

Daha çok küçük işletmelerin ağlarını ve dışarıdaki kullanıcılarını koruma amaçlı, kompakt ve zengin özellikli bir uygulamadır.



SnapGear SG300

LAN tarafında 4 port 10/100 ethernet switch, WAN tarafında ise 1 eth ve genişband olarak ADSL,SHDSL yanında darband ISDN mevcuttur. ISDN, genişband hattı yedekleme amaçlı kullanılabilir.



SnapGear SG560

Daha yüksek performansa ihtiyaç duyan daha büyük ofislerde kullanılır. Daha yüksek VPN performansı için hardware encryption acceleration yapar.



SnapGear SG565

Diğer özelliklere ilave olarak 802.11b/g Wireless LAN desteği vardır ve iki adet USB portu sayesinde depolama cihazları ve printer lar bağlanabilir.



SnapGear SG580

Beş farklı security zone destekler. Link failover ve internet load balancing yapabilir. Dahili olarak web proxy cache içerir.



SnapGear SG640

Desktoplar ve kritik server lar için bir PCI kartı içine yerleştirilmiş olan firewall/ VPN/IDS/IPS çözüm paketidir.

Üzerinde bir RISC işlemcisi ve iki ethernet arayüzü bulunmaktadır.



SnapGear SG720




Çok geniş işletmeler için düşünülmüş, multi-megabit throughput, enterprise sınıfı bir firewall çözümdür.




3.2 NETASQ – Ürünlerimiz

NETASQ, uygulamalarında UTM konseptinden esinlenerek, tüm security fonksiyonlarını, her ölçekteki müşterilerinin ihtiyaçları doğrultusunda bir araya getirerek entegre ürünler çıkarmıştır.

- Real-time intrusion prevention
- Network and application firewall
- SSL VPN
- IPSEC VPN
- Advanced content filtering
- PKI
- SSO (Single sign-on) Authentication
- Bandwidth management
- Integrated anti-virus
- Anti-spam
- Anti-spyware
- URL filtering

3.2.1 NETASQ – U Serisi

 NETASQ U30 Çok Fonksiyonlu Firewall . IPS . UTM	Performance <ul style="list-style-type: none">. Firewall throughput+IPS (Mbps): 200. IPsec VPN throughput (AES): 80. 10/100/1000 interfaces: -. 10/100 interfaces: 2. Simultaneous connections: 50,000. New sessions/second: 4,000	Network - Specification <ul style="list-style-type: none">. 802.1Q VLANs: 32. IPsec VPN tunnels: 50. SSL VPN tunnels: -. Max. no. of filter rules: 1,000. Simultaneous PPTP clients: 48. Redundant WAN link: 4. Policy-Based Routing: Yes	Firewall - Intrusion prevention <ul style="list-style-type: none">. ASQ intrusion prevention engine: Yes. Protocol detection and analysis: Yes. Protection contextual signatures: Yes. VoIP protection: Yes. Risk
 NETASQ U70 Çok Fonksiyonlu Firewall . IPS . UTM	Performance <ul style="list-style-type: none">. Firewall throughput+IPS (Mbps): 600. IPsec VPN throughput (AES): 120. 10/100/1000 interfaces: 6. 10/100 interfaces: -. Simultaneous connections: 100,000. New sessions/second: 6,000	Network - Specification <ul style="list-style-type: none">. 802.1Q VLANs: 32. IPsec VPN tunnels: 100. SSL VPN tunnels: 50. Max. no. of filter rules: 2,000. Simultaneous PPTP clients: 48. Redundant WAN link: 4. Policy-Based Routing: Yes	Firewall - Intrusion prevention <ul style="list-style-type: none">. ASQ intrusion prevention engine: Yes. Protocol detection and analysis: Yes. Protection contextual signatures: Yes. VoIP protection: Yes. Risk management - SEISMO: Optional
 NETASQ U120 Çok Fonksiyonlu Firewall . IPS . UTM	Performance <ul style="list-style-type: none">. Firewall throughput+IPS (Mbps): 700. IPsec VPN throughput (AES): 160. 10/100/1000 interfaces: 6. 10/100 interfaces: -. Simultaneous connections: 200,000. New sessions/second: 6,500	Network - Specification <ul style="list-style-type: none">. 802.1Q VLANs: 128. IPsec VPN tunnels: 500. SSL VPN tunnels: 256. Max. no. of filter rules: 8,000. Simultaneous PPTP clients: 96. Redundant WAN link: 8. Policy-Based Routing: Yes	Firewall - Intrusion prevention <ul style="list-style-type: none">. ASQ intrusion prevention engine: Yes. Protocol detection and analysis: Yes. Protection contextual signatures: Yes. VoIP protection: Yes. Risk management - SEISMO: Optional
 NETASQ U250 Çok Fonksiyonlu Firewall . IPS . UTM	Performance <ul style="list-style-type: none">. Firewall throughput+IPS (Mbps): 850. IPsec VPN throughput (AES): 190. 10/100/1000 interfaces: 6. 10/100 interfaces: -. Simultaneous connections: 400,000. New sessions/second: 8,500	Network - Specification <ul style="list-style-type: none">. 802.1Q VLANs: 128. IPsec VPN tunnels: 1,000. SSL VPN tunnels: 512. Max. no. of filter rules: 8,000. Simultaneous PPTP clients: 96. Redundant WAN link: 8. Policy-Based Routing: Yes	Firewall - Intrusion prevention <ul style="list-style-type: none">. ASQ intrusion prevention engine: Yes. Protocol detection and analysis: Yes. Protection contextual signatures: Yes. VoIP protection: Yes. Risk management - SEISMO: Optional
 NETASQ U450 Çok Fonksiyonlu Firewall . IPS . UTM	Performance <ul style="list-style-type: none">. Firewall throughput+IPS (Mbps): 1,000. IPsec VPN throughput (AES): 225. 10/100/1000 interfaces: 15. 10/100 interfaces: -. Simultaneous connections: 600,000. New sessions/second: 10,500	Network - Specification <ul style="list-style-type: none">. 802.1Q VLANs: 128. IPsec VPN tunnels: 1,000. SSL VPN tunnels: 512. Max. no. of filter rules: 8,000. Simultaneous PPTP clients: 96. Redundant WAN link: 8. Policy-Based Routing: Yes	Firewall - Intrusion prevention <ul style="list-style-type: none">. ASQ intrusion prevention engine: Yes. Protocol detection and analysis: Yes. Protection contextual signatures: Yes. VoIP protection: Yes. Risk management - SEISMO: Optional

 <p>NETASQ U1100 Çok Fonksiyonlu Firewall . IPS . UTM</p>	<p>Performance</p> <ul style="list-style-type: none"> . Firewall throughput+IPS (Mbps): 2,800 . IPSec VPN throughput (AES): 450 . 10/100/1000 interfaces: 8 . 10/100 interfaces: - . Simultaneous connections: 800,000 . New sessions/second: 20,000 	<p>Network - Specification</p> <ul style="list-style-type: none"> . 802.1Q VLANs: 256 . IPSec VPN tunnels: 4,000 . SSL VPN tunnels: 1,024 . Max. no. of filter rules: 16,000 . Simultaneous PPTP clients: 192 . Redundant WAN link: 12 . Policy-Based Routing: Yes 	<p>Firewall - Intrusion prevention</p> <ul style="list-style-type: none"> . ASQ intrusion prevention engine: Yes . Protocol detection and analysis: Yes . Protection contextual signatures: Yes . VoIP protection: Yes . Risk management - SEISMO: Optional
 <p>NETASQ U1500 Çok Fonksiyonlu Firewall . IPS . UTM</p>	<p>Performance</p> <ul style="list-style-type: none"> . Firewall throughput+IPS (Mbps): 3,800 . IPSec VPN throughput (AES): 600 . 10/100/1000 interfaces: 10 . 10/100 interfaces: - . Simultaneous connections: 1,200,000 . New sessions/second: 25,000 	<p>Network - Specification</p> <ul style="list-style-type: none"> . 802.1Q VLANs: 256 . IPSec VPN tunnels: 6,000 . SSL VPN tunnels: 1,024 . Max. no. of filter rules: 16,000 . Simultaneous PPTP clients: 192 . Redundant WAN link: 12 . Policy-Based Routing: Yes 	<p>Firewall - Intrusion prevention</p> <ul style="list-style-type: none"> . ASQ intrusion prevention engine: Yes . Protocol detection and analysis: Yes . Protection contextual signatures: Yes . VoIP protection: Yes . Risk management - SEISMO: Optional
 <p>NETASQ U6000 Çok Fonksiyonlu Firewall . IPS . UTM</p>	<p>Performance</p> <ul style="list-style-type: none"> . Firewall throughput+IPS (Mbps): 5,000 . IPSec VPN throughput (AES): 800 . 10/100/1000 interfaces: 6-24 . 10/100 interfaces: - . Simultaneous connections: 2,500,000 . New sessions/second: 40,000 	<p>Network - Specification</p> <ul style="list-style-type: none"> . 802.1Q VLANs: 512 . IPSec VPN tunnels: 10,000 . SSL VPN tunnels: 2,048 . Max. no. of filter rules: 32,000 . Simultaneous PPTP clients: 192 . Redundant WAN link: 12 . Policy-Based Routing: Yes 	<p>Firewall - Intrusion prevention</p> <ul style="list-style-type: none"> . ASQ intrusion prevention engine: Yes . Protocol detection and analysis: Yes . Protection contextual signatures: Yes . VoIP protection: Yes . Risk management - SEISMO: Optional

3.2.2 NETASQ – F Serisi



SİSTEM PERFORMANSI

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
IPS-Firewall performansı	65 Mbps	100 Mbps	115 Mbps	200 Mbps	450 Mbps	810 Mbps	1,6 Gbps	2 Gbps	3 Gbps
VPN AES Performansı	14 Mbps	16 Mbps	16 Mbps	33 Mbps	150 Mbits/s	180 Mbps	210 Mbps	263 Mbps	332 Mbps
Max. bağlantı sayısı	5 000	15 000	15 000	65 000	200 000	400 000	600 000	800 000	1 500 000
Max. VPN IPSEC tünel sayısı	50	100	100	1 000	1 000	3 750	3 750	3 750	15 000
Max. VPN SSL client sayısı	×	×	5	256	256	512	512	512	1 024
Max. filtre kuralı sayısı	512	512	512	4 096	4 096	16 384	16 384	16 384	16 384

DONANIM SPEKTLERİ

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
Route edilebilen interface max. sayısı	2	3	4	4	6	8	10	24	24
Gigabit interfacerlerin max. sayısı	×	×	×	×	2	8	10	24	24
Depolama Kapasitesi	-	-	-	40 Go HDD	70 Go HDD	70 Go HDD	74 Go SATA	73 Go RAID	140 Go RAID
Hot-swap RAID desteği	×	×	×	×	×	×	×	✓	✓
Yedek Güç Kaynağı	×	×	×	×	×	×	×	✓	✓
SSL Hızlandırma kartı desteği	×	×	×	×	×	×	×	✓	✓

VPN

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
IPSec VPN gateway-gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPSec VPN client-gateway	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPSec VPN NAT-Traversal	✓	✓	✓	✓	✓	✓	✓	✓	✓

IPSEC VPN Keep-alive	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPSec VPN Dead Peer Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓
IPSec VPN Hub & Spoke	✓	✓	✓	✓	✓	✓	✓	✓	✓
AES, 3DES, DES, Blowfish ve CAST 128	✓	✓	✓	✓	✓	✓	✓	✓	✓
SSL VPN	✗	✗	✗	✓	✓	✓	✓	✓	✓
Desteklenen PPTP client sayısı	16	16	16	32	32	64	64	64	64

AUTHENTICATION

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
Embedded CA & CRL PKI	✗	✗	✗	✓	✓	✓	✓	✓	✓
Dahili ya da harici authentication	✓	✓	✓	✓	✓	✓	✓	✓	✓
Single-sign-On desteği	✓	✓	✓	✓	✓	✓	✓	✓	✓
Harici PKI desteği	✓	✓	✓	✓	✓	✓	✓	✓	✓

ANTI-VIRUS

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
Embedded Anti-virus	✓	✓	✓	✓	✓	✓	✓	✓	✓
Antivirus Kaspersky	Option	Option	Option	Option	Option	Option	Option	Option	Option
HTTP, SMTP, POP3 support	✓	✓	✓	✓	✓	✓	✓	✓	✓
Otomatik signature güncelleme	✓	✓	✓	✓	✓	✓	✓	✓	✓

İÇERİK FİLTRELEME

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
Statik native ya da gelişmiş URL filtreleme	✓	✓	✓	✓	✓	✓	✓	✓	✓
Otomatik URL updateeleri	✓	✓	✓	✓	✓	✓	✓	✓	✓
ICAP uygunluğu (HTTP - Respmode & reqmode)	✓	✓	✓	✓	✓	✓	✓	✓	✓
HTTP, SMTP, POP3 Proxyleri	✓	✓	✓	✓	✓	✓	✓	✓	✓
İçerik imzası (P2P, IM, multimedia trafik...)	✓	✓	✓	✓	✓	✓	✓	✓	✓

ANTI-SPAM

	F25	F50	F60	F200	F500	F800	F1200	F2500	F5500
Otomatik updatelerle DNS (RBL)leri kara listeleme	✓	✓	✓	✓	✓	✓	✓	✓	✓

Sorularınız ve talepleriniz için sait.yildiz@gym-tech.net