KÖK SEBEP ANALİZİ DETAY FORMU

Proje Adı:	GlassHouse Public Cloud
Tarih:	28.06.2026 14:31 - 14:52
İlgili İş Birimi:	Network & Security Team
İlgili Veri Merkezi	İstanbul 1 Veri Merkezi

Kök Sebebi Araştırılan Olay Özeti

28.06.2026 tarihinde saat 14:31 itibarıyla İstanbul 1 Veri Merkezi'nde bulunan güvenlik duvarı cihazında yüksek CPU kullanımı kaynaklı performans problemi yaşanmış ve buna bağlı olarak erişim sorunları gözlemlenmiştir. Monitoring tarafına yansıyan alarmlar üzerine saat 14:40'ta Network & Security ekibine bilgi verilmiş ve ilk müdahale başlatılmıştır. Yapılan kontrollerde, cihaz üzerinde yüksek CPU tüketimine bağlı hata loglarının oluştuğu tespit edilmiştir.

Servis sürekliliğinin sağlanması amacıyla saat 14:50'de birincil güvenlik duvarı cihazı yeniden başlatılmış, trafik yüksek erişilebilirlik mimarisi kapsamında yedek güvenlik duvarı cihazı üzerinden karşılanmıştır. Bu aksiyon sonrasında erişim sorunu giderilmiş ve tüm sistemlerin saat 14:52 itibarıyla aktif duruma geldiği doğrulanmıştır.

Yeniden başlatılan birincil cihaz, saat 14:58'de sorunsuz şekilde devreye alınmış ve trafiği yeniden karşılamaya başlamıştır. Bu geçiş sırasında ek bir kesinti yaşanmamıştır.

Hata loglarının detaylı analizi ve üreticiden alınan bilgi doğrultusunda, güvenlik duvarı cihazında acil yazılım güncellemesi yapılmasına karar verilmiştir. Bu kapsamda, 17:00 - 19:00 saatleri arasında uygulanmak üzere acil müdahale değişiklik planı oluşturulmuş ve çalışma takvimlendirilmiştir. (CH-7067)

Saat 17:09'da cihaz yazılım versiyonu yükseltilmiştir. Güncelleme sırasında oluşan 4-5 paketlik ping kaybı dışında ağ genelinde kesinti meydana gelmemiştir. Yapılan son kontrollerde hata loglarının durduğu ve problemin giderildiği tespit edilmiştir.

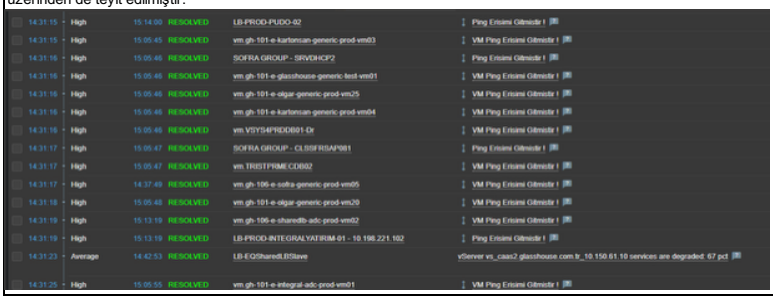
Güvenlik Cihazı Konsol Hata Logu:
np7_fos_vxlan_tunnel_vs_set 317.
np7_fos_vxlan_tunnel_vs_set 317.
np7_fos_vxlan_tunnel_vs_set 317.
np7_fos_vxlan_tunnel_vs_set 317.
np7_fos_vxlan_tunnel_vs_set 317.

191	2026-06-28 14:52:36	notice	876	Virtual cluster's member state moved
192	2026-06-28 14:51:17	critical	868	Heartbeat packet lost
193	2026-06-28 14:51:15	critical	868	Heartbeat packet lost
194	2026-06-28 14:51:15	critical	868	Heartbeat packet lost
195	2026-06-28 14:51:13	critical	868	Heartbeat packet lost
196	2026-06-28 14:51:13	critical	868	Heartbeat packet lost
197	2026-06-28 14:51:11	critical	868	Heartbeat packet lost
198	2026-06-28 14:51:11	critical	868	Heartbeat packet lost
199	2026-06-28 14:51:08	critical	868	Heartbeat packet lost
200	2026-06-28 14:51:08	critical	868	Heartbeat packet lost
201	2026-06-28 14:51:07	critical	868	Heartbeat packet lost

Kök Sebebi Araştırılan Olay Akışı ve Geçici Çözüm Uygulanması

Saat 14:31 itibarıyla ağ genelinde erişim sorunları gözlemlenmiş ve yapılan ilk kontrollerde birincil güvenlik duvarı cihazının CPU kullanımının kritik seviyelere ulaştığı tespit edilmiştir. Yaşanan performans kaybının servis etkisini azaltmak amacıyla trafik, yüksek erişilebilirlik mimarisi kapsamında yedek güvenlik duvarı cihazı üzerinden karşılanacak şekilde yönlendirilmiştir.

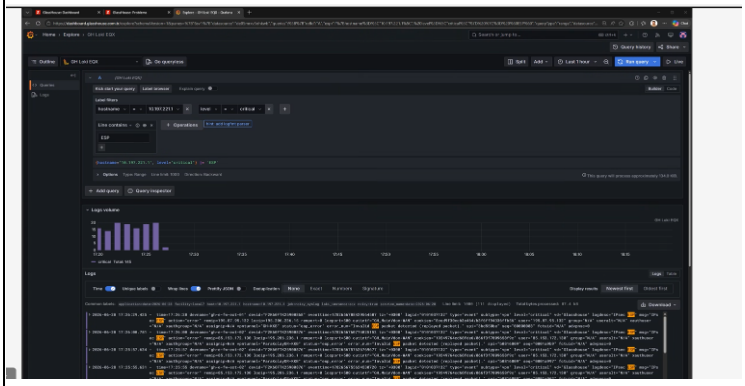
Geçici çözüm kapsamında birincil cihaz yeniden başlatılmış, erişimlerin normale döndüğü saat 14:52 itibarıyla doğrulanmıştır. Sistemlerin kararlı çalıştığı saat 15:05 itibarıyla izleme platformu üzerinden de teyit edilmiştir.



Kök Sebebe Yönelik Geçici Çözümler

Geçici çözüm adımları kapsamında, yüksek CPU kullanımı gözlemlenen birincil güvenlik duvarı cihazı yeniden başlatılmıştır. Bu işlem sırasında trafik, yüksek erişilebilirlik mimarisi uyarınca yedek güvenlik duvarı cihazı üzerinden karşılanmış ve erişimlerin saat 14:52 itibarıyla normale döndüğü gözlemlenmiştir.

Ağ altyapısı ve servislerin kararlılığından emin olmak amacıyla sistemler, acil yazılım güncellemesi öncesine kadar operasyon ekipleri tarafından yakından takip edilmiş ve ek bir olumsuzluk tespit edilmemiştir.

Kök Sebebe Yönelik Kalıcı Çözümler
İstanbul 1 Veri Merkezi'nde bulunan güvenlik duvarı cihazı üzerinde yapılan incelemelerde, IPsec tüneli içerisinden taşınan VXLAN arayüzüne ait yanıt paketlerinde (reply-packet) kararsızlık yaşandığı tespit edilmiştir. Üretici tarafında yapılan değerlendirmelerde bu durumun yazılım kaynaklı bir hata ile ilişkili olduğu doğrulanmıştır. Hata Tanımı: VLAN-over-VXLAN trafiğinin donanımsal ağ hızlandırıcısı katmanına aktarılamaması nedeniyle ilgili trafik ana işlemci (CPU) üzerinde işlenmiş; bu durum CPU kullanımının kritik seviyelere çıkmasına ve performans sorunlarına neden olmuştur. Üreticiden alınan teknik bilgiye göre, söz konusu yazılım hatasının önerilen güncel sürümlerde giderildiği belirtilmiştir. Bu kapsamda acil yazılım güncellemesi planlanmış ve başarıyla uygulanmıştır. Yazılım yükseltme işlemi sonrasında sistemin kararlı çalıştığı, ilgili hata loglarının tekrar oluşmadığı ve problemin giderildiği gözlemlenmiştir. 

Kök Sebebe Yönelik Alınacak Aksiyonlar							
Aksiyon 1:	Güvenlik duvarı yazılım güncellemesinin uygulanması	**Sorumlu:**	Network & Security Team	**Hedef Tarih:**	28.06.2026	**Durum:**	Tamamlandı
Aksiyon 2:	Güncelleme sonrası servis ve log kontrollerinin yapılması	**Sorumlu:**	Network & Security Team	**Hedef Tarih:**	28.06.2026	**Durum:**	Tamamlandı
Aksiyon 3:	CPU kullanımı ve hata loglarının düzenli izlenmesi	**Sorumlu:**	Monitoring Team	**Hedef Tarih:**	28.06.2026	**Durum:**	Tamamlandı
Aksiyon 4:		**Sorumlu:**		**Hedef Tarih:**		**Durum:**	

Aksiyon Sonuç Değerlendirmesi
Planlanan aksiyonlar başarıyla tamamlanmıştır. Güncelleme sonrasında sistem normal çalışma durumuna dönmüş olup, yapılan kontrollerde herhangi bir olumsuzluk tespit edilmemiştir.