E-POSTA GÜVENLİK CİHAZI KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: ESA C690, C690X

Genel bakış:

Her ölçekten müşteri aynı yıldırıcı zorlukla karşı karşıya: e-posta aynı zamanda en önemli ticari iletişim aracı ve güvenlik ihlalleri için önde gelen saldırı vektörüdür. Cisco® Email Security, kullanıcıların güvenli bir şekilde iletişim kurmasını sağlar ve kuruluşların iş e-posta uyuşmazlığı (BEC), fidye yazılımı, gelişmiş kötü amaçlı yazılım, kimlik avı, spam ve veri kaybı ile mücadeleye çok katmanlı bir yaklaşımla savaşmasına yardımcı olur.

Cisco E-posta Güvenlik Farkı

Cisco Email Security, tehditleri daha hızlı tespit etmek, engellemek ve düzeltmek için gelişmiş tehdit koruma yetenekleri içerir; veri kaybını önlemek ve uçtan uca şifreleme ile taşınırken önemli bilgilerin güvenliğini sağlamak.

Cisco Email Security müşterileri ile şunları yapabilirsiniz:

- Tehdit araştırma ekibimiz Talos ™ 'dan üstün tehdit istihbaratı ile daha fazla tehdit tespit edin ve engelleyin.
- Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) ve Cisco Threat Grid ile ilk algılamadan kaçınan eklerde gizlenmiş fidye yazılımıyla mücadele edin.
- Riskli bağlantılara sahip e-postaları otomatik olarak bırakın veya kimlik avına ve BEC'ye karşı korumak için gerçek zamanlı URL analiziyle yeni virüs bulaşan sitelere erişimi engelleyin.
- Giden e-postalardaki hassas içeriği veri kaybı önleme (DLP) ve kullanımı kolay e-posta şifrelemesi ile tek bir çözümde koruyun.
- Bulut, sanal, şirket içi veya karma dağıtım ile maksimum dağıtım esnekliği elde edin veya aşamalar halinde buluta geçiş yapın.

Özellikler ve faydalar:

Günümüzün e-posta güvenliği tehditleri, fidye yazılımı, gelişmiş kötü amaçlı yazılım, ticari e-posta uyuşmazlığı (BEC), kimlik avı ve spam'den oluşmaktadır. Cisco Email Security teknolojisi, tehditleri engeller, böylece şirketler yalnızca meşru mesajlar alır. Cisco, savunmanızı güçlendirmek için önleyici ve reaktif önlemler içeren en kapsamlı e-posta güvenliğini sağlamak için birden fazla katman kullanır. Tablo 1, e-posta güvenliği çözümlerimizin temel yeteneklerini özetlemektedir.

Tablo 1. Ana Yetenekler

Kabiliyet	Açıklama
Küresel tehdit istihbarat	Dünyanın en büyük tehdit algılama ağlarından biri olan Talos tarafından desteklenen hızlı ve kapsamlı e-posta koruması edinin. Talos, aşağıdakiler dâhil geniş bir görünürlük ve geniş bir kullanım alanı sağlar: • Günde 600 milyar e-posta • Günde 16 milyar web talebi • 1.5 milyon kötü amaçlı yazılım örneği Talos, küresel trafik etkinliğine 24 saat boyunca bakış sağlar. Anomalileri analiz eder, yeni tehditleri açığa çıkarır ve trafik eğilimlerini izler. Talos, sürekli olarak müşterilerin e-posta güvenliği çözümlerine güncellemeleri besleyen kurallar oluşturarak sıfır saatlik saldırıların önlenmesine yardımcı olur. Bu güncellemeler her üç ila beş dakikada bir meydana gelir ve sektör lideri tehdit savunması sağlar.

İtibar filtreleme	Talos'un tehdit istihbaratına dayanan itibar filtrelemeyle istenmeyen e-postaları engelleyin. Her gömülü köprü için, kaynağın bütünlüğünü doğrulamak için bir itibar kontrolü yapılır. Bilinen kötü itibarlı web siteleri otomatik olarak engellenir. İtibar filtreleme, istenmeyen e-postaların yüzde 90'ını ağınıza girmeden önce durdurarak çözümün daha küçük bir yükü analiz ederek ölçeklenmesini sağlar.
Spam koruması	Spam, karmaşık bir çözüm gerektiren karmaşık bir sorundur. Cisco kolaylaştırır. Cisco Email Security, milyonda bir değerinden daha düşük bir yanlış pozitif orana sahip, yüzde 99'dan daha yüksek en yüksek spam yakalama oranını sağlayan çok katmanlı bir tarama mimarisi kullanarak istenmeyen e-postaları engeller. Cisco Email Security'deki antispam işlevi, Cisco Context Adaptive Scanning Engine (CASE) kullanıyor. Bu motor, mesajın hangi içeriği içerdiğini, mesajın nasıl oluşturulduğunu, mesajı kimin gönderdiğini ve mesajın harekete geçirme ifadesinin sizi nereye götürdüğünü de içeren bir mesajın tüm içeriğini inceler. Cisco Email Security, bu unsurları birleştirerek, sektör lideri hassasiyetle en geniş tehdit yelpazesini durdurur.
Sahte e-posta algılama	Sahte E-posta Tespiti, yüksek değerli hedefler olarak kabul edilen yöneticilere odaklanan iş e-postası ihlal saldırılarına karşı korur. Sahte e-posta algılama, bu özelleştirilmiş saldırıları engellemenize yardımcı olur ve yapılan tüm girişimler ve eylemlerle ilgili ayrıntılı günlükler sağlar.
Virüs savunma	Cisco Email Security, ağ geçidine entegre edilmiş yüksek performanslı bir virüs tarama çözümü sunarak, virüs filtrelemede çok katmanlı, çok üreticili bir yaklaşım sunar.
Graymail tespiti ve güvenli abonelik iptali	Graymail, pazarlama, sosyal ağ ve toplu mesajlardan oluşur. Graymail algılama özelliği, bir kuruluşa giren graymail'i tam olarak sınıflandırır ve izler. Bir yönetici daha sonra her kategoride uygun işlemi yapabilir. Genellikle graymail, son kullanıcıların gönderene bu tür e-postaları almaktan vazgeçmek istediklerini gösterebilecekleri bir abonelik iptali bağlantısına sahiptir. Abonelikten çıkma mekanizmasını taklit etmek popüler bir kimlik avı tekniği olduğundan, kullanıcılar bu abonelikten çıkma bağlantılarını tıklatma konusunda dikkatli olmalıdırlar. Güvenli abonelik iptali çözümü şunları sağlar: • Abonelikten çıkma bağlantıları olarak gizleyen kötü amaçlı tehditlere karşı koruma • Tüm abonelikleri yönetmek için tek tip bir arayüz • E-posta yöneticileri ve son kullanıcılar için bu e-postaları daha iyi görebilme

Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması ve Cisco Threat Grid	Cisco Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) ve Cisco Threat Grid, tehditlerin sürekli analizi için dosya itibarı puanlama ve engelleme, dosya koruma ve dosya retrospeksiyonu sağlar. Kullanıcılar daha fazla saldırıyı engelleyebilir, şüpheli dosyaları izleyebilir, bir salgının kapsamını azaltabilir ve hızlı bir şekilde düzeltebilir. Office 365 müşterileri için Posta Kutusu Otomatik Düzeltme, ihlallerin daha hızlı ve daha az çabayla düzeltilmesine yardımcı olur. Müşteriler, virüs bulaşmış e-postalar üzerinde otomatik işlem yapacak şekilde e-posta güvenlik çözümlerini ayarladılar. Müşteriler ayrıca AMP sistemlerini tamamen AMP özel bulutuyla tesislerinde kurmak için ek bir lisans satın alabilir. Bu, Tehdit Izgarası ile birlikte tüm AMP teklifini tamamen kurum içinde getiriyor.
Salgın Filtreleri	Salgın Filtreleri ortaya çıkan tehditlere ve karma saldırılara karşı savunur. Bir mesajdaki dosya türü, dosya adı, dosya boyutu ve URL'ler dâhil altı parametrenin herhangi bir kombinasyonu hakkında kurallar yayınlayabilirler. Talos bir salgın hakkında daha fazla şey öğrendiğinde, kuralları değiştirebilir ve mesajları karantinadan buna göre serbest bırakabilir. Salgın filtreleri, şüpheli mesajlara bağlı URL'leri de yeniden yazabilir. Tıklandığında, yeni URL'ler alıcıyı Cisco Web Security proxy üzerinden yönlendirir. Web sitesi içeriği daha sonra etkin bir şekilde taranır ve site kötü amaçlı yazılım içeriyorsa, salgın filtreleri kullanıcıya blok ekran görüntüler.
Web etkileşimi takibi	Web etkileşimi izleme, BT yöneticilerinin Cisco Email Security tarafından yeniden yazılmış URL'lere tıklayan son kullanıcıları izlemelerine olanak sağlayan tamamen entegre bir çözümdür. Raporlar göster: • Kötü amaçlı URL'leri tıklayan en iyi kullanıcılar • Son kullanıcılar tarafından tıklanan en iyi kötü amaçlı URL'ler • Tarih ve saat, yeniden yazma nedeni ve URL'lerde yapılanlar
Giden e-postalardaki hassas içerik için veri güvenliği	Cisco Email Security etkili veri kaybını önleme (DPL) ve e-posta şifrelemesi sunar. Merkezi yönetim ve raporlama veri korumasını kolaylaştırır. **Veri kaybı önleme** Cisco Email Security Veri Kaybını Önleme (DLP) ile giden mesajları koruyun. Dünya çapındaki endüstri ve hükümet düzenlemelerine uyun ve gizli verilerin ağınızdan çıkmasını önleyin. Devlet, özel sektör ve şirkete özel düzenlemeleri kapsayan 100'den fazla uzman politikası içeren kapsamlı bir politika kütüphanesinden seçim yapın. Önceden tanımlanmış DLP politikaları Cisco Email Security ile birlikte gelir ve içeriğe duyarlı giden e-posta politikasının uygulanmasını kolaylaştırır. Düzeltme seçenekleri arasında şifreleme, altbilgi ve feragatname ekleme, kör karbon kopyaları (BCC'ler) ekleme, bildirme ve karantinaya alma bulunur. Karmaşık bir özel politikaya ihtiyaç duyan şirketler için, önceden tanımlanmış politikaların yapı taşları süreci hızlı ve kolay hale getirmek için hazır durumdadır.

	Şifreleme Mesajlar gönderildikten sonra bile, gönderenlere içeriklerinin kontrolünü verin. E-posta şifrelemesinde, gönderenler yanlış yazılmış alıcı adreslerinden, içerikteki hatalardan veya zamana duyarlı e-postalardan korkmaz, çünkü her zaman bir mesajı kilitleyebilirler. Şifreli bir mesajın göndereni, bir alıcı bir mesaj açtığında bir okundu bilgisi alır ve uçtan uca mahremiyet ve kontrolü korumak için çok güvenli yanıtlar ve iletiler otomatik olarak şifrelenir. Dağıtmak için ek bir altyapı yok. Gelişmiş güvenlik için, mesaj içeriği doğrudan ağ geçidinizden alıcıya gider ve bulutta yalnızca şifreleme anahtarı depolanır. Ödeme Kartı Endüstri Veri Güvenliği Standardı (PCI DSS), Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası (HIPAA), Gramm-Leach-Bliley Yasası (GLBA) veya Sarbanes-Oxley Yasası (SOX) gibi düzenlemeler için şifreleme gereksinimlerini karşılayın Göndericilere, alıcılara veya e-posta yöneticilerine yük vermeden, devlet gizliliği düzenlemeleri ve Avrupa direktifleri gibi. Şifrelemeyi bir zorunlu olarak değil, kullanımı kolay ve gönderene tam kontrol sağlayan bir hizmet olarak sunun. Cisco Kayıtlı Zarf Hizmetine ek olarak, Cisco Teknolojisine sahip ZixGateway ile şirket içi şifreleme sunmak için ZixCorp ile ortaklık kurduk. En hassas e-posta içeriğinizin korunmasını otomatikleştirmek için Cisco Email Security ile sorunsuz bir şekilde bütünleşir.
İdare edilebilirlik	**Evrensel cihaz desteği** Akıllı telefonlarda, tabletlerde, dizüstü bilgisayarlarda veya masaüstü bilgisayarlarda bulunup bulunmadıklarına bakmadan, tüm kullanıcıların gerektiğinde mesajlara erişebildiğinden emin olun. Evrensel cihaz desteği, mesajı açmak için hangi cihazın kullanıldığı fark etmeksizin, herhangi bir alıcı tarafından yüksek güvenlikli mesajların okunabilmesini sağlamak için tasarlanmıştır. Özel eklenti uygulamaları, Microsoft Outlook ve Apple iOS ve Google Android akıllı telefonlar ve tabletlerde gelişmiş bir kullanıcı deneyimi sunar. **Sisteme genel bakış kontrol paneli** Merkezi, özel bir sistem genel bakış kontrol panelinden giden mesajları izleyin ve raporlayın. Birleştirilmiş iş raporlaması, kuruluşunuzdaki kapsamlı bilgiler için tek bir görünüm sunar. Gelişmiş görünürlük için herhangi bir raporun ayrıntılarını alın. **Detaylı mesaj takibi** Bir mesajı zarf alıcısı, zarf göndereni, konu, ekler ve DLP politikası veya kimlikleri dâhil olmak üzere mesaj olayları ile izleyin. Cisco Email Security'ye bir mesaj gönderdiğinizde, mesaj izleme veritabanı bir veya iki dakika içinde doldurulur ve işlemin her aşamasında sistemi geçen mesajlara ne olduğunu görebilirsiniz.

Özellikler:

Cisco E-posta Güvenliği Özellikleri

Tablo 3, Cisco Email Security için performans özelliklerini gösterirken, Tablo 4, donanım özelliklerini ve Tablo 5, sanal bir dağıtım için özellikleri göstermektedir. Tablo 6, Güvenli Yönetim Cihazı M-Serisi Platformu için spesifikasyonları sunmaktadır.

Tablo 3. Cisco Email Security Performans Özellikleri

Yayılma	Model	Disk alanı	RAID Yansıtma	Bellek	CPU'lar
Büyük işletme	ESA C690	2,4 TB (600 x 4)	Evet (RAID 10)	32 GB DDR4	2 x 2,4 GHz, 6 çekirdekli
Büyük işletme	ESA C690X	4,8 TB (600 x 8)	Evet (RAID 10)	32 GB DDR4	2 x 2,4 GHz, 6 çekirdekli

Not: Doğru boyutlandırma için, Cisco içerik güvenliği uzmanıyla en yüksek posta akış hızını ve ortalama mesaj boyutunu kontrol ederek seçiminizi doğrulayın.

Tablo 4. Cisco Email Security Donanım Özellikleri

Model	ESA C690	ESA C690X
Raf üniteleri (RU)	2RU	2RU
Boyutlar (Y x G x D)	3.4 inç x 19 inç x 29 inç (8,6 x 48,3 x 73,7 cm)	3.4 inç x 19 inç x 29 inç (8,6 x 48,3 x 73,7 cm)
DC güç seçeneği	Evet (930W)	Evet (930W)
Uzaktan güç bisiklet	Evet	Evet
Yedekli güç kaynağı	Evet	Evet
Çalışırken değiştirilebilir sabit disk	Evet	Evet
Güç tüketimi	2216.5 BTU / saat	2216.5 BTU / saat
Güç kaynağı	650W	650W
Ethernet arayüzleri	6 bağlantı noktalı 1GBASE-T bakır ağ arabirimi (NIC), RJ-45	6 bağlantı noktalı 1GBASE-T bakır ağ arabirimi (NIC), RJ-45
Hız (Mbps)	10/100/1000, özdevinir	10/100/1000, özdevinir

Fiber seçeneği	Evet, ayrı SKU'lar 2 bağlantı noktalı 1GBASE-SX Fiber: ESA-C690-1G 2 bağlantı noktalı 10GBASESR Fiber: ESAC690-10G	Evet, ayrı SKU'lar 2 bağlantı noktalı 1GBASESX Fiber: ESAC690-1G 2 bağlantı noktalı 10GBASE - SR Fiber: ESAC690-10G
Hd boyutu	Dört adet 600 GB sabit disk sürücüsü (2,5 inç 10K SAS 4Kn), SAS sürücüler için çalışırken değiştirilebilir erişim sağlayan ön panel sürücü bölmelerine takıldı	Sekiz 600 GB sabit disk sürücüsü (2,5 inç 10K SAS 4Kn), SAS sürücüler için çalışırken değiştirilebilir erişim sağlayan ön panel sürücü bölmelerine yerleştirilmiştir
İşlemci	İki E5–2620 v3 işlemci	İki E5–2620 v3 işlemci
Veri deposu	Dört adet 8GB DDR4-2133 DIMM1	Dört adet 8GB DDR4-2133 DIMM1

Tablo 5. Cisco Email Security Sanal Özellikleri

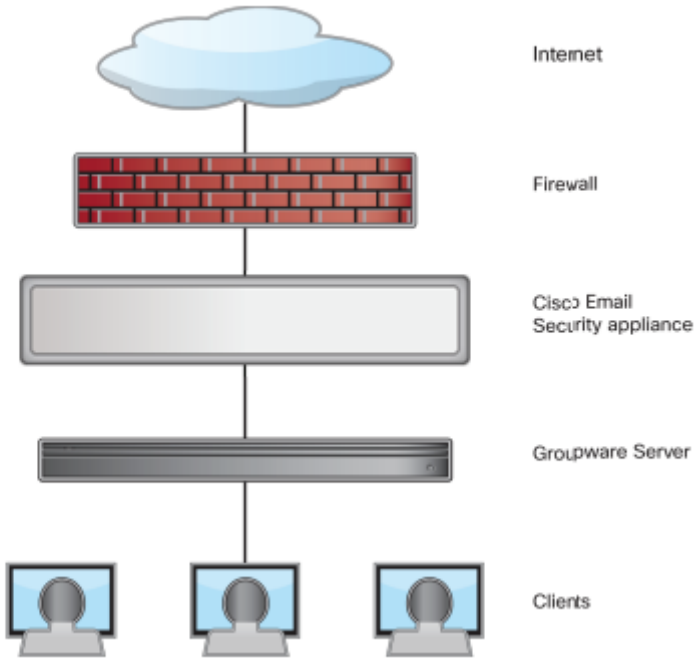
Email kullanıcıları				
	Model	**Disk**	**Bellek**	**Çekirdekler**
Küçük işletme (1000 çalışana kadar)	ESAV C100v	200 GB (10K RPM SAS)	6 GB	2 (2,7 GHz)
Orta ölçekli işletme (en fazla 5000 çalışan)	ESAV C300v	500 GB (10K RPM SAS)	8 GB	4 (2,7 GHz)
Büyük işletme veya servis sağlayıcı	ESAV C600v	500 GB (10K RPM SAS)	8 GB	8 (2,7 GHz)
Sunucular				
Cisco UCS	VMware ESXi 5,0, 5.1 ve 5.5 Hiper Yönetici			

KURULUM

Kurulumu Planlayın

E-posta sisteminizi spam, virüs, phishing ve diğer tehditlere karşı korumak için Cisco C690 cihazı ağınızın çevresine kurulmalıdır. İnternete erişebilen bir IP adresine sahip ilk cihaz olması gerekir.

Ağ yapılandırmanızın şöyle görünmesini sağlayın:



Cihazı Rafa Kurma

Verilen slayt raylarını kullanarak Cisco C690 Email Security Appliance'ı kurun.

Cihazı rafa takma hakkında bilgi için Cisco 90 Serisi İçerik Güvenliği Aletleri Kurulum ve Bakım Kılavuzu'na bakın.

Bir Rafa Cihazın Yerleştirilmesi

• Ortam Sıcaklığı - Cihazın aşırı ısınmasını önlemek için, ortam sıcaklığının 104 ° F (40 ° C) üzerindeki bir alanda çalıştırmayın.

• Hava Akışı — Cihazın çevresinde yeterli hava akışı olduğundan emin olun.

• Mekanik Yükleme - Tehlikeli durumlardan kaçınmak için cihazın düz ve sabit olduğundan emin olun.

Cihazı Takın

Her bir düz güç kablosunun dişi ucunu, cihazın arka panelindeki yedek güç kaynaklarına takın.

Erkek uçları bir elektrik prizine takın.

Uzaktan Erişim için IP Adresinizi Geçici Olarak Değiştirin

Ağ bağlantısını kullanarak Cisco C690'ı uzaktan yapılandırmak için, bilgisayarınızın IP adresini geçici olarak değiştirmeniz gerekir. Alternatif olarak, IP adresini değiştirmeden Cisco C690'ı yapılandırmak için seri konsolu kullanabilirsiniz.

Seri konsolu kullanıyorsanız, aşağıdaki bölüm 8'e ilerleyin.

Not Geçerli IP yapılandırma ayarlarınızı not edin çünkü konfigürasyonu tamamladıktan sonra bu ayarlara geri dönmeniz gerekecektir.

Pencereler için

Tam adımlar işletim sisteminizin sürümüne bağlıdır.

Adım 1 başlat menüsüne gidin ve Denetim Masası'nı seçin.

Adım 2 Ağ ve İnternet'i, ardından Ağ ve Paylaşım Merkezi'ni tıklayın.

Adım 3 Adaptör ayarlarını değiştir bağlantısını tıklayın.

Adım 4 Yerel Ağ Bağlantısı'na sağ tıklayın ve Özellikler'i seçin.

Adım 5 İnternet Protokolü Versiyon 4'ü tıkladıktan sonra Özellikler'i seçin.

Adım 6 Mevcut ayarlarınızı not edin.

Adım 7 Aşağıdaki IP Adresini Kullan'ı seçin.

Adım 8 Aşağıdaki değişiklikleri girin:

- IP Adresi: 192.168.42.43

- Alt Ağ Maskesi: 255.255.255.0

- Varsayılan Ağ Geçidi: 192.168.42.1

Adım 9 İletişim kutusundan çıkmak için Tamam ve Kapat'ı tıklayın.

Mac için

Tam adımlar işletim sisteminizin sürümüne bağlıdır.

Adım 1 Apple menüsünü başlatın ve Sistem Tercihleri'ni seçin.

Adım 2 Ağ'a tıklayın.

Adım 3 Değişikliklere izin vermek için kilit simgesini tıklayın.

Adım 4 Yeşil simgeli Ethernet ağ yapılandırmasını seçin. Bu senin aktif bağlantın. Ardından Gelişmiş'i tıklayın.

Adım 5 TCP / IP sekmesine tıklayın ve Ethernet ayarlarından açılır listeden El İle'yi seçin.

Adım 6 Aşağıdaki değişiklikleri girin:

- IP Adresi: 192.168.42.43

- Alt Ağ Maskesi: 255.255.255.0

- Yönlendirici: 192.168.42.1

Adım 7 Tamam'a tıklayın.

Cihaza Bağlan

Cisco C690 cihazları, aşağıdaki sayfada gösterildiği gibi beş gigabit ağ bağlantı noktasına ve bir Yönetim bağlantı noktasına sahiptir. E-posta göndermek ve almak için en az bir statik IP adresi gerekir.

Ağ topolojiniz bunu gerektiriyorsa, tek bir bağlantıdan her iki ağ bağlantı noktasına da e-posta alabilir ve gönderebilirsiniz. Bir ağ arayüzünde iki IP adresi yapılandırılabilir.

Veya Data 1 ağ bağlantı noktasını genel ağınıza bağlayabilir ve Data 2 ağ bağlantı noktasını özel ağınıza bağlayabilirsiniz.

Cihaza Ethernet ile erişmek ve yönetmek için, Yönetim şebekesini kullanın.

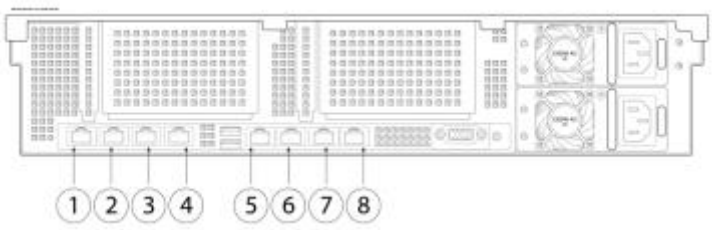
Liman. Fabrika tarafından Yönetim limanına atanan IPv4 adresi 192.168.42.42'dir.

Cihazın konsol portuna seri erişim için, bilgisayarı cihazdaki konsol portuna bağlamak için aksesuar setinde verilen RJ-45 - DB-9 Rollover kablosunu kullanın.

Aşağıdaki şekilde, Ethernet bağlantı noktalarına sahip bir model gösterilmektedir. Fiber Optik bağlantı noktaları, Cisco Web Security Appliance ürününün aşağıdaki modellerinde bulunur:

C690-1G ve C690-10G. Bu modellerin her birinde iki Fiber Optik bağlantı noktası vardır.

Bu portlar, aşağıdaki şekilde gösterilen Ethernet portlarının üstünde bulunur. Fiber Optik modellerde, Ethernet bağlantı noktaları mevcut değildir. Ayrıntılar için Cisco x90 Serisi İçerik Güvenliği Araçları Kurulum ve Bakım Kılavuzu'na bakın.



Madde	Port	Açıklama
1	Veri 1	Bir Gigabit Ethernet müşteri veri arayüzü
2	Veri 2	Bir Gigabit Ethernet müşteri veri arayüzü
3	Veri 3	Bir Gigabit Ethernet müşteri veri arayüzü.
4	Veri 4	Bir Gigabit Ethernet müşteri veri arayüzü.
5	Uzaktan güç döngüsü	Uzaktan Güç Döngüsü (RPC) için kullanılan port.
6	Konsol	Bir bilgisayarı doğrudan cihaza bağlayan konsol bağlantı noktası.
7	Veri 5	Bir Gigabit Ethernet müşteri veri arayüzü.
8	Yönetim arayüzü	Yalnızca yönetim kullanımıyla sınırlı bir Gigabit Ethernet arayüzü.

Cihazı Güçlendirin

Cisco C690'ın ön panelindeki Açma / Kapama düğmesine basarak cihazı açın. Sistemin her açılışında sistemin başlaması için 10 dakika beklemelisiniz. Makine açıldıktan sonra, cihazın önündeki sabit yeşil ışıklar cihazın çalıştığını gösterir. Ağ etkinlik ışığı yeşil olacaktır, ancak sabit olmayabilir. .

Not Cihaza güç verildikten sonra hızlı bir şekilde açılırsa, cihaz açılır, fanlar döner ve LED'ler yanar. 30-60 saniye içinde fanlar durur ve tüm LED'ler söner. Cihaz 31 saniye sonra açılır. Bu davranış, sistem üretici yazılımının ve denetleyicisinin senkronize edilmesine izin vermek için tasarım gereğidir.

Sistemin güç dizisini tamamlaması ve LED'lerin yeşile dönmesi için en az 10 dakika bekleyin. Başlatma işlemi tamamlanmadan önce gücü kapatırsanız, cihaz çalışma durumuna ulaşmaz ve Cisco'ya iade edilmelidir.

Cihazda Giriş Yap

İki arabirimden birini kullanarak Cisco C690 cihazına giriş yapabilirsiniz: web tabanlı arayüz veya komut satırı arayüzü.

Web Tabanlı Arayüz

Adım 1 Ethernet portu üzerinden web tarayıcısına erişmek için (sayfa 7'deki “Cihaza Bağlan” bölümüne bakın), bir web tarayıcısına aşağıdaki URL'yi girerek cihazın yönetim arayüzüne gidin:

http://192.168.42.42

Adım 2 Aşağıdaki kimlik bilgileriyle giriş yapın:

• Kullanıcı Adı: admin

• Şifre: ironport

Komut satırı arayüzü

Adım 1 Yerel veya uzaktan komut satırı arayüzüne erişin:

• CLI'ye yerel olarak erişmek için, 9600 bit, 8 bit, parite yok, 1 durdurma biti (9600, 8, N, 1) ve donanım ayarına göre akış kontrolü kullanarak seri porta bağlanacak bir terminal kurun. Terminali fiziksel olarak bağlamak için, sayfa 7'deki “Cihaza Bağlan” bölümüne bakın).

• CLI'ya uzaktan erişmek için IP adresine bir SSH oturumu başlatın.

192.168.42.42.

Adım 2 Şifre girişi ile yönetici olarak giriş yapın.

Adım 3 Komut isteminde, systemsetup komutunu çalıştırın.

Sistem Kurulum Sihirbazı'nı çalıştırın

Cihaza web tabanlı arayüz üzerinden eriştiğinizde (veya komut satırı arayüzünden systemsetup komutunu çalıştırdığınızda) Sistem Kurulum Sihirbazı otomatik olarak başlar.)

Adım 1 Sistem Kurulum Sihirbazı'nı başlatın.

Adım 2 Son kullanıcı lisans sözleşmesini kabul edin.

Adım 3 Sayfa 3'teki “Doküman Ağı Ayarları” bölümündeki bilgileri girin.

Adım 4 İstenmeyen posta önleme ve virüsten koruma güvenlik ayarlarını ayarlayın.

Adım 5 Yapılandırma özeti sayfasını inceleyin.

Adım 6 Bu Yapılandırmayı Kur'a tıklayın.

Cihaz konfigürasyonunuzu kabul etmiş gibi görünmüyor veya kurulumu gerçekleştiriyor olabilir. Bunun nedeni IP adresini değiştirmiş olmanızdır, ancak kurulum devam etmektedir.

Adım 7 Bilgisayarınızın IP adresini geçici olarak, 6. sayfadaki “Uzaktan Erişim için IP Adresinizi Geçici Olarak Değiştirin” bölümünde açıklandığı şekilde değiştirdiyseniz, IP adresi ayarlarını orijinal değerlerine geri getirin.

Adım 8 Dizüstü bilgisayarınızın ve cihazın ağa bağlı olduğundan emin olun.

Adım 9 Kullanıcı adı yöneticisi ve Sistem Kurulum Sihirbazı'nda ayarladığınız yeni parola ile cihaza tekrar giriş yapın.

Cisco C690 Email Security Appliance, web tarayıcınızdan bir uyarı tetikleyebilecek kendinden imzalı bir sertifika kullanır. Sadece sertifikayı kabul edebilir ve bu uyarıyı yok sayabilirsiniz.

Adım 10 Yeni yönetici şifrenizi yazın ve güvenli bir yerde saklayın.

Active Directory Sihirbazı'nı çalıştırın (isteğe bağlı)

Web arayüzünde Sistem Kurulum Sihirbazı'nı çalıştırdıktan sonra, Active Directory Sihirbazı belirir. Ağınızda bir Active Directory sunucusu kullanıyorsanız, Active Directory sunucusu için bir LDAP sunucusu profili yapılandırmak için Active Directory Sihirbazı'nı kullanın.

Active Directory kullanmıyorsanız veya daha sonra yapılandırmak istiyorsanız, Bu Adımı Atla öğesini tıklayın. Active Directory Sihirbazı'nı daha sonra Sistem Yönetimi> LDAP'ye giderek çalıştırabilirsiniz. “Active Directory Sihirbazı'nı kullanma” onay kutusunu seçin ve ardından LDAP Sunucu Profili Ekle'yi tıklayın.

Not Active Directory Sihirbazı'nı çalıştırmak için Active Directory hesabınızın ana bilgisayar adına ve giriş bilgilerine ihtiyacınız olacaktır.

Not GUI'de yaptığınız tüm değişiklikleri, Değişiklikleri Kabul Et'e tıklayarak tamamlayın. Bu düğme, kaydedilmesi gereken kaydedilmemiş değişiklikleriniz varsa görünür.

Mevcut Yükseltmeleri Kontrol Et

Cihaza giriş yaptıktan sonra, yükseltme bildirimi için (veya komut satırı arayüzündeki bir bildirim için) web tarayıcısı penceresinin üst kısmına bakın.) Bir yükseltme varsa, yüklemeniz gerekip gerekmediğini değerlendirin.

Her sürümle ilgili detaylar, Async OS versiyonunun sürüm notlarında mevcuttur.

Ağ Ayarlarını Yapılandırma

Ağ yapılandırmanıza bağlı olarak, güvenlik duvarınızın aşağıdaki bağlantı noktalarını kullanarak erişime izin verecek şekilde yapılandırılması gerekebilir. SMTP ve DNS servisleri İnternete erişebilmelidir.

• DNS: 53 numaralı bağlantı noktası

• SMTP: 25 numaralı bağlantı noktası

Diğer sistem işlevleri için, aşağıdaki hizmetler gerekli olabilir:

• FTP: port 21, veri portu TCP 1024 ve üstü

• HTTP: 80 numaralı bağlantı noktası

• HTTPS: 443 numaralı bağlantı noktası

• LDAP: 389 veya 3268 numaralı bağlantı noktası

• SSL üzerinden LDAP: 636 numaralı bağlantı noktası

• Genel katalog sorguları için SSL ile LDAP: port 3269

• NTP: 123 numaralı bağlantı noktası

• SSH: 22 numaralı bağlantı noktası

• Telnet: 23 numaralı bağlantı noktası

Not 80 ve 443 numaralı bağlantı noktalarını açmazsanız, özellik tuşlarını indiremezsiniz.

Daha fazla bilgi için, Cisco Email Security Appliance için AsyncOS sürümünüzün kullanım kılavuzundaki güvenlik duvarı bilgilerine bakın.

Yapılandırma Özeti

Madde	Açıklama
Yönetim	E-posta güvenlik cihazınızı yönetim portundan http://192.168.42.42 girerek veya sistem kurulumu sırasında cihazınıza atanmış olan ana bilgisayar adını kullanarak yönetebilirsiniz. Ayrıca, yönetim arabiriminizde güvenlik duvarı bağlantı noktalarını 80 ve 443'ü açtığınızı doğrulayın.
Gelen e-posta	Sistem Kurulum Sihirbazı'nı çalıştırdıktan sonra, Veri Bağlantı Noktası 2 bağlantı noktanız gelen e-postayı kabul edecek şekilde yapılandırılır
Giden E-posta	Aygıtı, Sistem Kurulum Sihirbazı'nda yapmadıysanız, giden e-postaları iletecek şekilde yapılandırmak için, Cisco E-posta Güvenliği için AsyncOS sürümünüzün kullanım kılavuzuna bakın.

Ek Yapılandırmalar

Tebrikler! Kurulumu ve temel konfigürasyonu tamamladınız. Artık cihazınızın ek özelliklerini yapılandırabilirsiniz. Tüm ayrıntılar için AsyncOS sürümünüzün çevrimiçi yardımına veya kullanım kılavuzuna bakın.

BAKIM, ONARIM VE KULLANIMDA UYULMASI GEREKEN KURALLAR:

Ürünün kullanıcı tarafından yapılabilecek her hangi bir bakım ya da onarım işlemi bulunmamaktadır. Potansiyel zararlardan korunmak için cihazı, sıcaktan, sıvı temasından, nemden ve tozdan koruyunuz. Cihaz ısı kaynağından en az 30 cm uzak olmalıdır.

KULLANIM SIRASINDA İNSAN VEYA ÇEVRE SAĞLIĞINA TEHLİKELİ VEYA ZARARLI OLABİLECEK DURUMLARA İLİŞKİN UYARILAR:

Lütfen kullanım ömrü tamamlandığında elektronik çöp dönüşümü yapabilen yerlere ürünü teslim ediniz.

KULLANIM HATALARINA İLİŞKİN BİLGİLER:

Burada belirtilenler ile sınırlı olmamak kaydı ile bu bölümde bazı kullanıcı hatalarına ilişkin örnekler sunulmuştur. Bu ve benzeri konulara özen göstermeniz yeterlidir.
Örnekler:
Aleti çalışır durumda taşımak, temizlemek vb. eylemler Alet üzerine katı ya da sıvı gıda maddesi dökülmesi Aletin taşıma sırasında korunmaması ve darbe alması

TÜKETİCİNİN KENDİ YAPABİLECEĞİ BAKIM, ONARIM VEYA ÜRÜNÜN TEMİZLİĞİNE İLİŞKİN BİLGİLER:

Ürünün tüketici tarafından yapılabilecek bir bakım prosedürü bulunmamaktadır. Cihaz çalışır durum da iken temizlik yapmayınız. Islak bezle, köpürtülmüş deterjanlarla, sulu süngerlerle temizlik yapmayınız.

ÜRÜN HERHANGİ BİR PERİYODİK BAKIM ONARIM GEREKTİRMEMEKTEDİR.

MALIN ENERJİ TÜKETİMİ AÇISINDAN VERİMLİ KULLANIMINA İLİŞKİN BİLGİLER

Satın almış olduğunuz ürünün ömrü boyunca enerji tüketimi açısından verimli kullanımı için bakım hizmetlerinin yetkilendirilmiş sertifikalı elemanlarca yapılması gerekmektedir.

TAŞINMA ve NAKLİYE SIRASINDA DİKKAT EDİLECEK HUSUSLAR

- Paketlerken, orijinal kutusunu ve paketleme malzemelerini kullanın.
- Cihazı kullanırken ve daha sonra bir yer değişikliği esnasında sarsmamaya, darbe, ısı, rutubet ve tozdan zarar görmemesine özen gösteriniz.

TÜKETİCİNİN SEÇİMLİLİK HAKLARI

Malın ayıplı olduğunun anlaşılması durumunda tüketici, 6502 sayılı Tüketicinin Korunması Hakkında Kanunun 11 inci maddesinde yer alan;

a- Sözleşmeden dönme,

b- Satış bedelinden indirim isteme,

c- Ücretsiz onarılmasını isteme,

ç- Satılanın ayıpsız bir misli ile değiştirilmesini isteme, haklarından birini kullanabilir.

Tüketicinin bu haklardan ücretsiz onarım hakkını seçmesi durumunda satıcı; işçilik masrafı, değiştirilen parça bedeli ya da başka herhangi bir ad altında hiçbir ücret talep etmeksizin malın onarımını yapmak veya yaptırmakla yükümlüdür. Tüketici ücretsiz onarım hakkını üretici veya ithalatçıya karşı da kullanabilir. Satıcı, üretici ve ithalatçı tüketicinin bu hakkını kullanmasından müteselsilen sorumludur.

Tüketicinin, ücretsiz onarım hakkını kullanması halinde malın;

- Garanti süresi içinde tekrar arızalanması,

- Tamiri için gereken azami sürenin aşılması,

- Tamirinin mümkün olmadığının, yetkili servis istasyonu, satıcı, üretici veya ithalatçı tarafından bir raporla belirlenmesi durumlarında; tüketici malın bedel iadesini, ayıp oranında bedel indirimini veya imkân varsa malın ayıpsız misli ile değiştirilmesini satıcıdan talep edebilir. Satıcı, tüketicinin talebini reddedemez. Bu talebin yerine getirilmemesi durumunda satıcı, üretici ve ithalatçı müteselsilen sorumludur.

Tüketici, garantiden doğan haklarının kullanılması ile ilgili olarak çıkabilecek uyuşmazlıklarda yerleşim yerinin bulunduğu veya tüketici işleminin yapıldığı yerdeki Tüketici Hakem Heyetine veya Tüketici Mahkemesine başvurabilir.

AEEE YÖNETMELİĞİNE UYGUNDUR. 

İthalatçı Firma

TECH DATA BİLGİSAYAR SİSTEMLERİ A.Ş.

Saray Mahallesi, Site Yolu Sokak

Anel İş Merkezi No:5 Kat:8

Ümraniye, İstanbul,34768

Tel : +90 216 999 53 50

Üretici Firma

Cisco Systems, Inc.

170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com

Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883