AĞ GÜVENLİK CİHAZI (FİREWALL)
KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: SMA M170

Cisco Content Security Management Appliance (SMA) ile birden fazla Cisco ® Email Security Appliance (ESA) ve Cisco Web Security Appliance (WSA)genelinde yönetim ve raporlama işlevlerini merkezileştirin. Cisco SMA'nın Cisco ESA'lar ve WSA'larla entegrasyonu, e-posta ve web güvenliğinin planlanmasını ve yönetimini basitleştirir, uyumluluk izlemesini geliştirir, kabul edilebilir kullanım politikalarının tutarlı bir şekilde uygulanmasını mümkün kılar ve tehdit korumasını geliştirir. Kurumlar, coğrafi dağınık ekipler arasında birden fazla cihazın yönetimini ve yönetimini sınırlı bir kadro ve bütçeyle koordine etmelidir. Raporlama ve izleme için optimize edilmiş sağlam bir platform üzerine inşa edilen Cisco SMA, yüksek performans ve ölçeklenebilirliğin yanı sıra uzun vadeli yatırım değeri için endüstri lideri koruma ve kontrol sunar.

Özellikler ve faydalar

Cisco SMA'nın özellikleri ve faydaları aşağıdaki bölümlerde tartışılmış ve Tablo 1'de daha ayrıntılı olarak açıklanmıştır.

Basitleştirilmiş Yönetim ve Planlama

Cisco SMA'nın kullanımı kolay sezgisel arayüzünü kullanan ağ yöneticileri, politika ayarlarını ve yapılandırma değişikliklerini tek bir konsoldan birden fazla Cisco ESA ve WSA'ya yayınlayabilir. Alternatif olarak, kuruluşlar belirli hacimli uygulamaları yüksek hacimli dağıtımlar için bireysel uygulamalara ayırabilir.

Ayrıca, güvenlik cihazları önerilen kapasiteyi aştığında ağ yöneticilerine bilgi verilebilir. Cisco SMA, saniye başına işlem sayısını ve sistemin gecikme, yanıt süresi ve proxy arabellek raporunu bildirir. Bu bilgi, ağ yöneticilerinin sistemi ne zaman yeniden yapılandırmaları gerektiğini veya ek aygıtları ne zaman kurmaları gerektiğini belirlemelerini sağlar.

Geliştirilmiş Uyum İzleme ve Uygulama

Merkezileştirilmiş raporlama ve izleme, hangi kullanıcıların kabul edilebilir kullanım politikalarını ihlal ettiğini belirlemeye yardımcı olur, herhangi bir departman veya sitedeki politika ihlallerini tespit eder ve Facebook ve YouTube gibi Web 2.0 uygulamalarının kullanımını izler ve ayrıca " kumar ya da "spor"

Yöneticiler, birden fazla cihazın yönetimini merkezileştirerek, kurum genelinde tutarlı ve kabul edilebilir kullanım politikaları uygulayabilirler.

Gelişmiş Tehdit Koruması

Cisco SMA, daha iyi tehdit istihbarat, savunma ve iyileştirme sağlayan bir kuruluşun güvenlik operasyonlarının kapsamlı bir görünümünü sunar. Önemli özellikler arasında e-posta spam karantinasının merkezi yönetimi, birden fazla web güvenliği ağ geçidi boyunca kapsamlı tehdit izlemesi, web itibarı puanlaması ve botnet tespiti bulunur. Cisco SMA'nın raporlama yetenekleri, yöneticilerin veri kaybını önleme (DLP) içeren faaliyetleri tanımlamasına ve ele almasına yardımcı olmak için de kullanılabilir.

Yüksek Performans ve Ölçeklenebilirlik

Cisco SMA, raporlama ve izleme için optimize edilmiş tek bir genel veritabanı yerine iki özel veritabanına sahiptir. Gerçek zamanlı raporların hızlı oluşturulması için her sorguya uygun hesaplamalar uygulanır.

Yüksek performanslı Cisco AsyncOS ® işletim sistemi üzerine kurulu Cisco SMA, küçük, orta ve büyük ölçekli işletmelerin ve ayrıca servis sağlayıcıların taleplerini karşılamak için endüstri lideri ölçeklenebilirlik sağlar.

Cisco Content Security Management Sanal Aracı ile Esnek Dağıtım

Cisco İçerik Güvenliği Yönetimi Sanal Uygulaması (SMAV), özellikle yüksek oranda dağıtılmış ağlarda, e-posta ve web güvenliğini yönetme maliyetini önemli ölçüde azaltır. Ağ yöneticiniz, mevcut ağ

altyapınızı kullanarak, nerede ve ne zaman gerektiğine dair örnekler oluşturabilir. Cisco SMAV, Cisco SMA'nın bir yazılım sürümüdür ve bir VMware ESXi hipervizörü ve Cisco Unified Computing System ™ (Cisco UCS ®) sunucularının üzerinde çalışır. Herhangi bir Cisco Email veya Web Security yazılım paketi için bir SMA yazılımı lisansı satın alarak sınırsız sayıda Cisco SMAV örneği alacaksınız. Cisco SMAV ile basitleştirilmiş kapasite planlaması ile artan trafik büyümesine anında cevap verebilirsiniz. Cihaz satın almanız ve göndermeniz gerekmez, böylece bir veri merkezine karmaşıklık eklemeden veya ek personel kiralamak zorunda kalmadan yeni iş fırsatlarını destekleyebilirsiniz.

Tablo 1. Cisco SMA ve SMAV'ın Özellikleri ve Avantajları

Özellik	**Yararları**
Merkezi yönetim ve raporlama	Cisco SMA, yapılandırmaları tek bir yönetim konsolundan birden fazla Cisco WSA'ya yayınlayarak yönetimi basitleştirir. Güncellemeler ve ayarlar, bağımsız cihazlardan ziyade o konsolda merkezi olarak yönetilir. Kuruluşlar, belirli aygıtları, yüksek hacimli dağıtımlar için bireysel uygulamalara ayırabilir. Tamamen entegre raporlama, birden fazla Cisco ESA ve WSA'dan gelen trafik verilerinin konsolide edilmesini sağlar.
Mesaj takibi	Veriler, gönderen, alıcı, mesaj konusu ve diğer parametrelere göre kategorilere ayrılan veriler dâhil olmak üzere birden fazla Cisco ESA'dan toplanır. Spam ve virüs kararları gibi tarama sonuçları da politika ihlalleri gibi görüntülenir.
Web takibi	IP adresi, kullanıcı adı, etki alanı adı, erişim süresi ve diğer ayrıntılar gibi bilgilerle bireysel web işlemlerinin kaydı tutulur. Facebook, YouTube ve anlık mesajlaşma gibi Web 2,0 uygulamalarının çalışanlara kullanımıyla ilgili görünürlük sağlanır.
Web raporlama	Web izleme bilgileri gerçek zamanlı olarak toplanır ve üst düzey, kullanımı kolay bir grafik biçiminde görüntülenir. Raporlama özellikleri, yöneticilerin web sitelerini, URL kategorilerini ve çalışanların şirket cihazlarında erişebilecekleri uygulamaları belirlemesine yardımcı olur.
Spam karantinaya alma	İstenmeyen posta ve pazarlama mesajları, kullanımı kolay self servis Cisco Spam Karantina çözümü ile merkezi olarak depolanır. Birden fazla Cisco ESA'ya sahip büyük işletmeler, kolay takip için spam trafiğini bir konuma boşaltabilir ve çalışanların erişimi için tek bir nokta sağlayabilir.
Tehdit izleme	Web tabanlı tehditlere ilişkin veriler, örneğin, hangi kullanıcıların en fazla engelle veya uyarıyla karşılaştıkları ve hangi web sitelerinin ve URL kategorilerinin en büyük riskleri taşıdığı dâhil olmak üzere gerçek zamanlı olarak sağlanır. Cisco WSA'ların tespit ettiği ve engellediği kötü amaçlı yazılımlar ve diğer tehditler de bildirilmektedir.
İtibar puanlaması	Bu özellik, kullanıcıların eriştiği web sitelerinin itibar puanları hakkında ayrıntılı bilgi sağlar. Bu puanlar, web sunucusu davranışını analiz eden ve kötü amaçlı yazılım içerme olasılığını yansıtan her URL'ye bir puan veren Cisco WSA'lar tarafından sağlanan verilere dayanmaktadır.
Botnet algılama	Kötü amaçlı yazılım bağlantısı olan bağlantı noktaları ve sistemler görüntülenir. Cisco WSA'lardaki Katman 4 trafik izleme özelliğinden elde edilen

Özellik	Yararları
	veriler, kuruluşların botnet bulaşmış ana bilgisayarları algılayıp düzeltmelerine yardımcı olabilir.

Ürün Özellikleri

Cisco SMA'lar, farklı boyutlardaki kuruluşların gereksinimlerini karşılamak ve tüm Cisco ESA'ları ve Cisco WSA'larını tamamlamak için üretilmiştir. Tablo 2 performans özelliklerini, Tablo 3 donanım özelliklerini ve Tablo 4 Cisco SMA için sipariş bilgilerini sunmaktadır.

Tablo 2. Cisco SMA Performans Özellikleri

	Kullanıcı Sayısı *	Model	Disk alanı	RAID Yansıtma	Bellek	CPU'lar
Büyük işletme	10.000 ya da daha fazla	Cisco SMA M690	6.0 TB (10 x 600 GB SAS)	Evet (RAID 10)	32 GB DDR4	2 x 2,4 GHz, 6C
Büyük işletme	10.000 ya da daha fazla	Cisco SMA M690X	9,6 TB (16 x 600 GB SAS)	Evet (RAID 10)	32 GB DDR4	2 x 2,4 GHz, 6C
Büyük işletme	10.000 ya da daha fazla	Cisco SMA M680	4.8 TB (8 x 600 GB SAS)	Evet (RAID 10)	32 GB, DDR3	2 x 2,0 GHz, 6C
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M390	3,6 TB (6 x 600 GB SAS)	Evet (RAID 10)	16 GB DDR4	2 x 2,4 GHz, 6C
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M390X	4.8 TB (8 x 600 GB SAS)	Evet (RAID 10)	16 GB DDR4	2 x 2,4 GHz, 6C
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M380	2,4 TB (4 x 600 GB SAS)	Evet (RAID 10)	32 GB, DDR3	2 x 2,0 GHz, 6C
Küçük işletme veya şube	2000 yılına kadar	Cisco SMA M190	1,2 TB (2 x 600 GB SAS)	Evet (RAID 1)	8 GB, DDR4	1 x 1,9 GHz, 6C
Küçük işletme veya şube	2000 yılına kadar	Cisco SMA M170	500 GB (2 x 250 GB SATA)	Evet (RAID 1)	4 GB, DDR3	1 x 2,8 GHz, 2C

* Çözümünüzün mevcut ve öngörülen gereksinimlerinizi karşılamasını sağlamak için boyutlandırma rehberliğini Cisco içerik güvenliği uzmanıyla teyit edin.

Tablo 3. Cisco SMA Donanım Özellikleri

	Cisco SMA M170
Donanım platformu	
Form faktörü	1 raf ünitesi (1RU)
Boyutlar (Y x G x D)	1.64 inç x 15.25 inç x 19 inç. (4.2 cm. X 38,7 cm. X 48,3 cm)
Yedekli güç kaynağı	Yok hayır
Uzaktan güç döngüsü	Yok hayır
DC güç seçeneği	Yok hayır
Çalışırken değiştirilebilir sabit sürücü	Evet
Güç tüketimi	1364 BTU / saat
Güç kaynağı	400W
Fiber seçeneği	Yok hayır
Ethernet arayüzleri	2 bağlantı noktası 1G Base-T bakır ağ arabirimi (NIC), RJ - 45
Hd boyutu	500 GB (2 x 250 GB SATA)
İşlemci	1 x 2.8 GHz, 2C
Veri deposu	4 GB, DDR3
Hız (Mbps)	10/100/1000, özdevinir

Tablo 4. Cisco SMAV

SMA Kullanıcıları				
SMA Kullanıcıları	Model	Disk	Bellek	Çekirdekler
Sadece değerlendirmeler	Cisco SMAV M000v	250 GB (10K RPM SAS)	4 CİGABAYT	1 (2,7 GHz)
Küçük İşletme (1K'ya kadar)	Cisco SMAV M100v	250 GB (10K RPM SAS)	6 GB	2 (2,7 GHz)
Orta Ölçekli İşletme (5K'a kadar)	Cisco SMAV M300v	1024 GB (10K RPM SAS)	8 GB	4 (2,7 GHz)
Büyük işletme veya servis sağlayıcı	Cisco SMAV M600v	2032 GB (10K RPM SAS)	8 GB	8 (2,7 GHz)
Sunucular				
Cisco UCS		VMware ESXi 5,0, 5,1 ve 5,5 Hiper Yönetici	vmware	

Tablo 5. Cisco SMA için Sipariş Bilgileri

Parça numarası	**Açıklama**
SMA-M690 / 690X / 680-K9	Cisco M690 / 690X / 680 (10.000'den fazla kullanıcılı kuruluşlar için)
SMA-M390 / 390X / 380-K9	Cisco M390 / 390X / 380 (10.000 kullanıcıya kadar olan organizasyonlar için)
SMA-M190 / 170-K9	Cisco M190 / 170 (1000 kullanıcıya kadar olan organizasyonlar için)

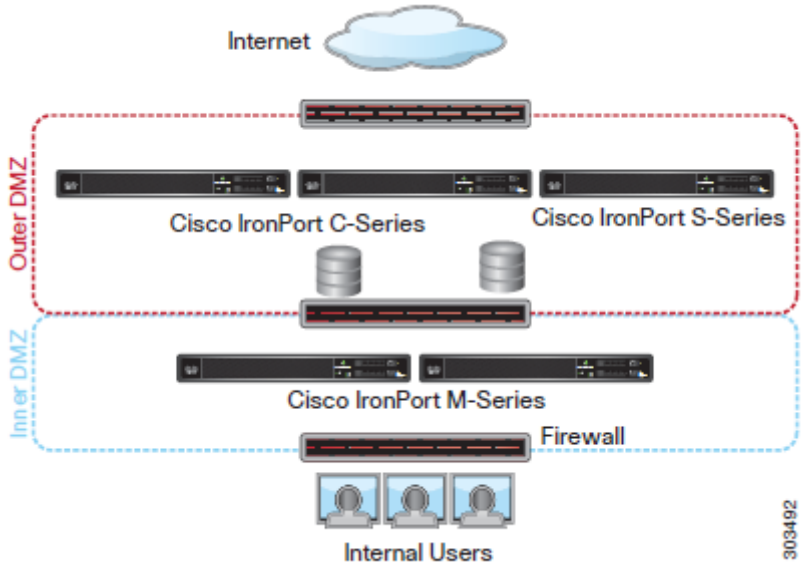
KURULUM

Kurulumu Planlayın

Cisco M170 Content Security Management Appliance, şirket politikası ayarlarını ve denetim bilgilerini izlemek için harici veya "kapalı kutu" bir konum olarak hizmet vermek üzere tasarlanmıştır. Önemli politika ve çalışma zamanı verilerini merkezileştirmek ve birleştirmek için donanımı, işletim sistemini (AsyncOS) ve destekleyici hizmetleri bir araya getirir.

Cisco M170 cihazı iç DMZ'nizde oturacak ve dış DMZ'nizdeki Cisco C Serisi ve S Serisi cihazlardan karantinaya alınmış spam alacak şekilde tasarlanmıştır. Dâhili kullanıcılar, karantinalarındaki mesajları görüntülemek ve yönetmek için Content Security Management uygulamasına erişir.

Ağ yapılandırmanızın şöyle görünmesini sağlayın:



Cihazı Rafa Kurma

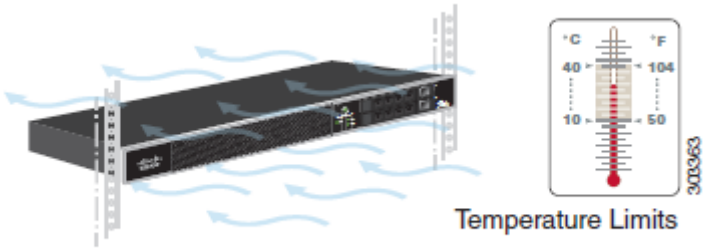
Cisco M170 Content Security Management Appliance'ı slayt raylarını veya sabit raf montaj braketlerini kullanarak takın. Bu yükleme seçenekleri hakkında daha fazla bilgi için Cisco 170 Serisi Donanım Kurulum Kılavuzu'na bakın.

Cihaz Yerleştirme

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

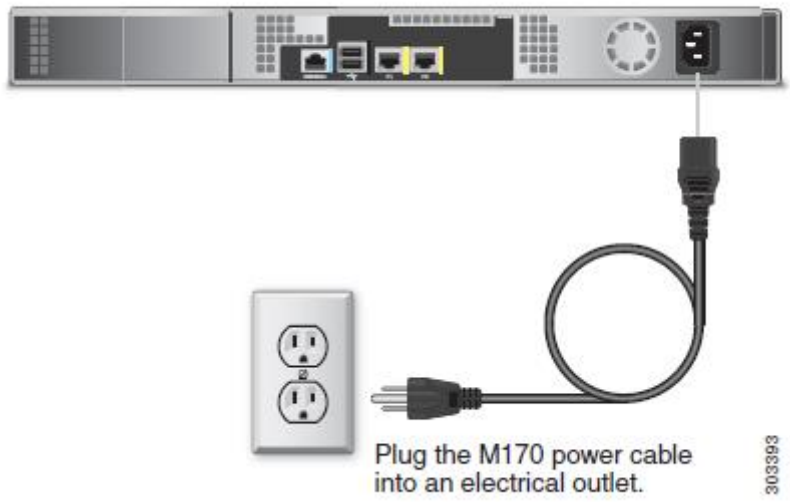
• Hava Akışı — Cihazın çevresinde yeterli hava akışı olduğundan emin olun.

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



Cihazı Takın

Güç kablosunun dişi ucunu cihazın arka panelindeki güç kaynağına takın. Erkek uçları bir elektrik prizine takın.



IP Adresinizi Geçici Olarak Değiştirin

Cisco M170'a bağlanmak için bilgisayarınızın IP adresini geçici olarak değiştirmeniz gerekir.

Not Yapılandırmayı tamamladıktan sonra bu ayarlara geri dönmeniz gerekeceğinden, geçerli IP yapılandırma ayarlarınızı not alın.

Pencereler için

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

Adım 2 Ağ ve Paylaşım Merkezi'ni çift tıklayın.

Adım 3 Yerel Ağ Bağlantısı'na ve ardından Özellikler'e tıklayın.

Adım 4 İnternet Protokolü'nü (TCP / IP) seçin ve ardından Özellikler'e tıklayın.

Adım 5 Aşağıdaki IP Adresini Kullan'ı seçin.

Adım 6 Aşağıdaki değişiklikleri girin:

• IP Adresi: 192.168.42.43

• Alt Ağ Maskesi: 255.255.255.0

• Varsayılan Ağ Geçidi: 192.168.42.1

Adım 7 İletişim kutusundan çıkmak için Tamam'a ve Kapat'a tıklayın.

Mac için

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

Adım 2Ağ'ı tıklayın.

Adım 3 Yeşil simge ile ağ yapılandırmasını seçin. Bu senin aktif bağlantın. Ardından Gelişmiş'i tıklayın.

Adım 4 TCP / IP sekmesine tıklayın ve Ethernet ayarlarından açılır listeden El İle'yi seçin.

Adım 5 Aşağıdaki değişiklikleri girin:

• IP Adresi: 192.168.42.43

• Alt Ağ Maskesi: 255.255.255.0

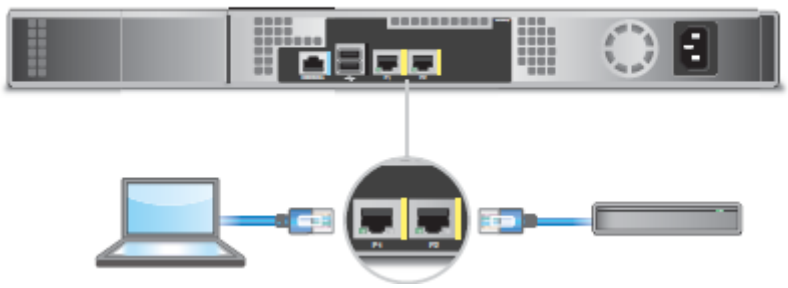
• Yönlendirici: 192.168.42.1

Adım 6 Tamam.

Alete Bağlan

Cisco M170 cihazı iki gigabit ağ portuna sahiptir: P1 ve P2.

Kurulum amaçları için, P1'e yönetim arayüzü olarak bağlanın ve gelen web trafiğini veya e-postayı P2 arayüzünde yapılandırın. Bu ayarlar ilk kurulumdan sonra değiştirilebilir.



P1: Yönetim: 192.168.42.42P1 bağlantı noktasını Ethernet kablosu kullanarak bilgisayarınıza bağlayın.

P2: Gelen web trafiği veya e-postası Ethernet kablosunu kullanarak P2 portunu ağınıza bağlayın.

Cihazı Güçlendirin

Cisco M170 cihazının ön panelindeki Açma / Kapama düğmesine basarak cihazı açın. Sistemi her açışınızda sistemin başlaması için beş dakika beklemelisiniz.

Makine açıldıktan sonra sabit bir yeşil ışık, cihazın çalıştığını gösterir.

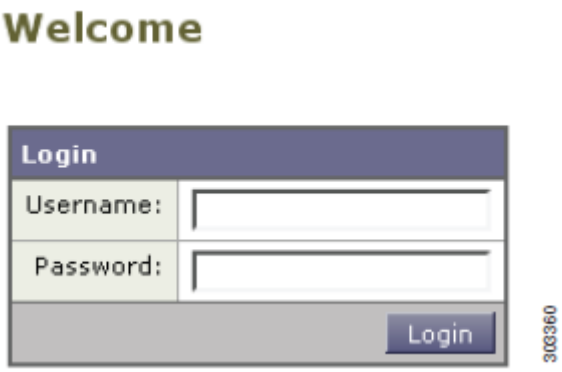
Cihazda Giriş Yap

İki arabirimden birini kullanarak Cisco M170'da oturum açabilirsiniz: web tabanlı arayüz veya komut satırı arayüzü.

Web Tabanlı Arayüz

Adım 1 Ethernet portu üzerinden web tarayıcısına erişmek için (bkz. “Cihaza Bağlan” sayfa 9), web tarayıcısına aşağıdaki URL'yi girerek Cisco M170 cihaz yönetimi arayüzüne gidin:

http://192.168.42.42



Adım 2 Aşağıdaki giriş bilgilerini girin:

• Kullanıcı Adı: admin

• Şifre: ironport

Not Ana bilgisayar adı parametresi, sistem kurulumu sırasında atanır. Bir ana bilgisayar adı (http: // ana bilgisayar adı: 8080) kullanarak yönetim arayüzüne bağlanmadan önce, cihazın ana makine adını ve IP adresini DNS sunucusu veritabanınıza eklemelisiniz.

Adım 3 Click Login'e tıklayın.

Komut satırı arayüzü

Adım 1 Seri bağlantı noktası üzerinden komut satırı arayüzü erişimi için (bkz. "Cihaza Bağlan" bölümü, sayfa 9), 9600 bit, 8 bit, eşlik yok, 1 durdurma biti (9600, 8, N, 1) ve akış kontrolü Donanım olarak ayarlanmış.

Adım 2 192.168.42.42 IP adresine bir oturum başlatın.

Adım 3 Parola ironport ile yönetici olarak oturum açın.

Adım 4 İstemde, systemsetup komutunu çalıştırın.

Sistem Kurulum Sihirbazı'nı çalıştırın

Sistem Kurulum Sihirbazı, eriştiğinizde otomatik olarak başlar.

Web tabanlı arayüzü kullanan cihaz (veya komut satırı arayüzünden systemsetup komutunu çalıştırdığınızda) ve son kullanıcı lisans sözleşmesini (EULA olarak da bilinir) görüntüler.

Adım 1 Sistem Kurulum Sihirbazı'nı başlatın.

Adım 2 Son kullanıcı lisans sözleşmesini kabul edin.

Adım 3 Kayıt bilgilerini girin.

Adım 4 Sayfa 4'teki “Doküman Ağı Ayarları” bölümünden bilgileri girin.

Adım 5 Web güvenlik ayarlarını ayarlayın.

Adım 6 Yapılandırma özeti sayfasını inceleyin.

Adım 7 Kullanıcı adı yöneticisini ve Sistem Kurulum Sihirbazı'nda ayarladığınız yeni şifreyi kullanarak cihaza tekrar giriş yapın.

Cisco M170 Content Security Management Appliance, web tarayıcınızdan bir uyarı tetikleyebilecek kendinden imzalı bir sertifika kullanır. Sadece sertifikayı kabul edebilir ve bu uyarıyı yok sayabilirsiniz.

Adım 8 Yeni yönetici şifrenizi yazın ve güvenli bir yerde saklayın.

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: 6025 ve 25 numaralı bağlantı noktaları

Diğer sistem işlevleri için, aşağıdaki hizmetler gerekli olabilir:

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

• HTTP: port 80 veya 82

• HTTPS: port 83 veya 443

• 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

• Karantina Kimlik Doğrulama: 110 (POP) ve / veya 143 (IMAP)

• SSH: 22 numaralı bağlantı noktası

• Telnet: 23 numaralı bağlantı noktası

Not 443 numaralı bağlantı noktasını açmazsanız, özellik tuşlarını indiremezsiniz.

Daha fazla bilgi için, daha fazla bilgi için Cisco AsyncOS for Content Security Management Kullanıcı Kılavuzu'ndaki "Güvenlik Duvarı Bilgileri" ekine bakın.

Uyarı Sıranızın ve yapılandırma dosyalarınızın bozulmaması için, cihazınızı Sistem Yönetimi> Kapat / Yeniden Başlat sayfasından kapatmalısınız.

Yapılandırma Özeti

Yapılandırmanızın aşağıdaki ayrıntılarını gözden geçirin.

Madde	Açıklama
Yönetim	Content Security Management cihazınızı, Sistem Kurulum Sihirbazı'nı tamamladığınızda http://192.168.42.42 veya cihazınıza atanmış olan ana bilgisayar adını girerek yönetim portundan (P1) yönetebilirsiniz. Yapılandırmanızı fabrika varsayılan ayarlarına sıfırlarsanız (örneğin, Sistem Kurulumu Sihirbazı'nı yeniden çalıştırarak), yönetim arayüzüne yalnızca P1 bağlantı noktasından erişebilirsiniz (http://192.168.42.42), böylece bir bağlantınızın olduğundan emin olun P1 portuna. Ayrıca, yönetim arabiriminizde güvenlik duvarı bağlantı noktalarını HTTP için 80 veya 82 ve HTTPS için 83 ve 443'ü açtığınızı doğrulayın.
Bilgisayar adresi	Bilgisayarınızın IP adresini, sayfa 4'teki “Doküman Ağı Ayarları” bölümünde not ettiğiniz orijinal ayarlara getirmeyi unutmayın. Sistem ayarlarınızın bir özetini Management Appliance> Centralized Services> Security Appliances sayfasından inceleyebilirsiniz.

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