AĞ GÜVENLİK CİHAZI (FİREWALL)
KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: SMA M380

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 M380
Donanım platformu	
Form faktörü	2 raf ünitesi (2RU)
Boyutlar (Y x G x D)	3,5 inç x 19 inç x 29 inç (8.9 cm. X 48.3 cm. X 73.7 cm.)
Yedekli güç kaynağı	Evet
Uzaktan güç döngüsü	Evet
DC güç seçeneği	Evet (930W)
Çalışırken değiştirilebilir sabit sürücü	Evet
Güç tüketimi	2216.5 BTU / saat
Güç kaynağı	650W
Ethernet arayüzleri	6 bağlantı noktası 1G Base-T bakır ağ arabirimi (NIC), RJ - 45
Hız (Mbps)	10/100/1000, özdevinir
Fiber seçeneği	Yok hayır
Hd boyutu	Cisco M380 Content Security Management, dört (4) 600 G HDD içerir
İşlemci	İki Intel Xeon ES-2620 Serisi işlemci (2,0 G, 6C).
Veri deposu	Sekiz (8) 4 GB DDR3-1600-MHz RDIMM DRAM

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

Başlamadan Önce

Kuruluma başlamadan önce ihtiyacınız olan öğelerin bulunduğundan emin olun. Cisco M380 ve Cisco M680 Content Security Management Appliance ile aşağıdaki öğeler bulunur:

• Hızlı Başlangıç Kılavuzu (bu kılavuz)

• Kızaklı ray takımı

• Güç kabloları (2)

• Cihazı ağınıza bağlamak için Ethernet kablosu

• Bir bilgisayarı konsol bağlantı noktasına bağlamak için RJ-45 - DB-9 kablosu

• Cisco Content Security dokümantasyon işaretçi kartı Not Cisco M680 cihazının kilitleme ön yüzü sürümünde iki adet kilitleme anahtarı bulunur. Bu anahtarları güvende tutun, çünkü eksik anahtarları değiştirmek için 4 basamaklı anahtar koduna ihtiyacınız olacaktır.

Aşağıdaki öğeleri kendiniz vermeniz gerekecektir:

• Raf kabini muhafazası (cihazın rafa monte edilmesi durumunda)

• 10/100/1000 Base TX TCP / IP LAN

• Masaüstü veya dizüstü bilgisayar

• Web tarayıcısı (veya SSH ve terminal yazılımı)

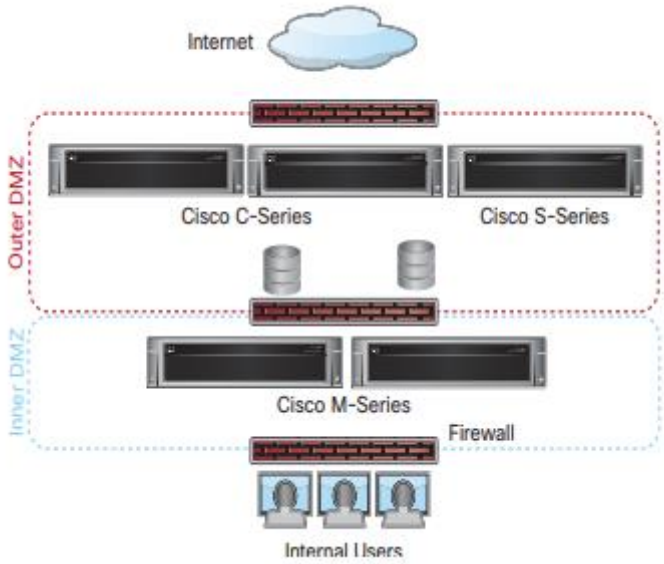
• Sayfa 4'teki “Belge Ağ Ayarları” bölümü için ağ ve yönetici bilgileri

Kurulumu Planlayın

Cisco M380 ve Cisco M680 İçerik Güvenliği Yönetim Cihazı, kurumsal politika ayarlarını ve denetim bilgilerini izlemek için harici veya "kapalı" bir konum olarak hizmet verecek şekilde tasarlanmıştır. Önemli politika ve çalışma zamanı verilerini merkezileştirmek ve birleştirmek için donanımı, işletim sistemini (AsyncOS) ve destekleyici hizmetleri bir araya getirir.

Cisco M380 ve Cisco M680, iç DMZ'nizin içine oturmak ve dış DMZ'nizdeki Cisco C Serisi ve S Serisi cihazlardan karantinaya alınmış spam almak için tasarlanmıştır. Dâhili kullanıcılar, karantinalarındaki mesajları görüntülemek ve yönetmek için Content Security Management uygulamasına erişir.

Ağ yapılandırmanızın şöyle görünmesini sağlayın:



Cihazı Rafa Kurma

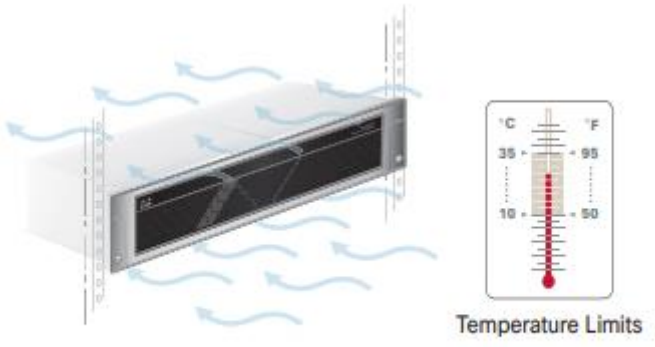
Verilen sürgü raylarını kullanarak Cisco M380 ve Cisco M680 Content Security Management Appliance'ı kurun. Cihazı rafa takma hakkında bilgi için Cisco 380 ve Cisco 680 Serisi Donanım Kurulum Kılavuzu'na bakın.

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

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

Erkek uçları bir elektrik prizine takın.

IP Adresinizi Geçici Olarak Değiştirin

Cisco M380 ve Cisco M680'e bağlanmak için, bilgisayarınızın IP adresini geçici olarak değiştirmeniz gerekir.

NOT: Yapılandırmayı tamamladıktan sonra bu ayarlara geri dönmeniz gerekeceğinden mevcut IP yapılandırma ayarlarınızı not edin.

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 ve Kapat'ı tıklayın.

Mac için

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

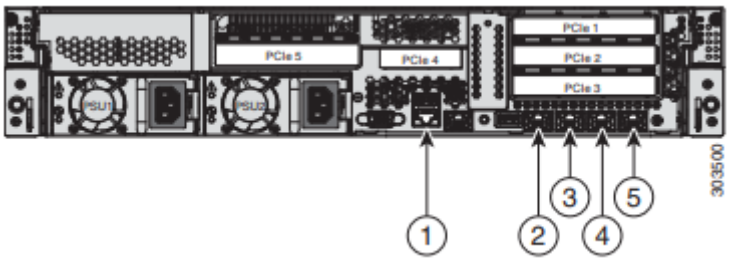
- Alt Ağ Maskesi: 255.255.255.0

- Yönlendirici: 192.168.42.1

Adım 7 Tamam'a tıklayın.

Cihaza Bağlan

Sistem kutusunda bulunan Ethernet kablosunu kullanarak dizüstü bilgisayarınızı Yönetim bağlantı noktasına bağlayın. Cisco M380 ve Cisco M680 cihazı sadece Yönetim portunu kullanır.



Madde	Port	Açıklama
1	Konsol	Bir bilgisayarı doğrudan cihaza bağlayan konsol bağlantı noktasını belirtir.
2	Yönetim arayüzü	Yalnızca yönetim kullanımıyla sınırlandırılmış Gigabit Ethernet arayüzünü gösterir. Bir RJ-45 kablosuyla bağlayın.
3	Veri 1	Gigabit Ethernet müşteri veri arayüzü Veri 1'i gösterir.
4	Veri 2	Gigabit Ethernet müşteri veri arayüzü Veri 2'yi gösterir.
5	Veri 3	Gigabit Ethernet müşteri veri arayüzü Veri 3'ü gösterir.

Not Cihazınızla bir NIC kartı sipariş ettiyseniz, bkz.

Cisco 380 ve Cisco 680 Serisi Donanım Kurulum Kılavuzu'nun PCI NIC Slot Konfigürasyonları bölümünde ayrıntılı bilgi.

Cihazı Güçlendirin

Açma / Kapama düğmesine basarak cihazı açın.

Cisco M380 ve Cisco M680'in ön paneli. Sistemi her açışınızda sistemin başlaması için beş dakika beklemelisiniz. Makine açıldıktan sonra sabit bir yeşil ışık, cihazın çalıştığını gösterir.

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.

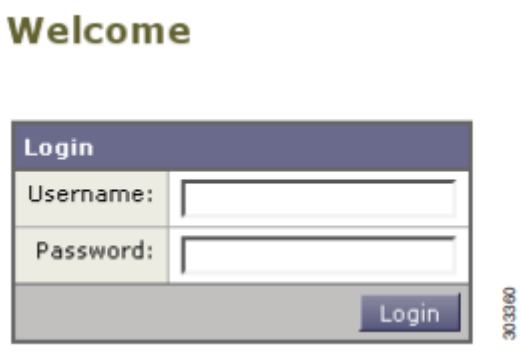
Cihazda Giriş Yap

İki arabirimden birini kullanarak Cisco M380 ve Cisco M680'de oturum açabilirsiniz: web tabanlı arayüz veya komut satırı arayüzü.

Web Tabanlı Arayüz

Adım 1 Ethernet portu üzerinden web tarayıcısına erişmek için (bkz. “Cihaza Bağlan” bölümü, sayfa 9), web tarayıcısına aşağıdaki URL'yi girerek Cisco M380 ve Cisco M680 cihaz yönetimi arayüzüne gidin:

http://192.168.42.42:8080



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 Giriş'e tıklayın.

Komut satırı arayüzü

Adım 1 Seri port üzerinden komut satırı arayüzü erişimi için (bkz. “Cihaza Bağlan” sayfa 9), 9600 bit, 8 bit, parite yok, 1 durdurma biti (9600) kullanarak komut satırı arabirimi terminal emülatörüne erişin. , 8, N, 1) ve akış kontrolü Donanım olarak ayarlanmış.

Adım 2 192.168.42.42 IP adresine bir telnet veya SSH oturumu başlatın.

Adım 3 Parola ironport ile yönetici olarak giriş yapın.

Adım 4 Komut isteminde, systemsetup komutunu çalıştırın.

Sistem Kurulum Sihirbazı'nı çalıştırın

Temel ayarları yapılandırmak ve bir dizi sistem varsayılanını etkinleştirmek için Sistem Kurulum Sihirbazı'nı çalıştırın. Cihaza web tabanlı arayüz üzerinden eriştiğinizde (veya komut satırı arayüzünden systemsetup komutunu çalıştırdığınızda) Sistem Kurulum Sihirbazı otomatik olarak başlar 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 M380 ve Cisco M680 İçerik Güvenlik Yönetimi Cihazı, 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	İçerik güvenlik yönetimi cihazınızı, http://192.168.42.42 adresini veya Sistem Kurulumu Sihirbazı'nı tamamladığınızda cihazınıza atanmış olan ana bilgisayar adını girerek yönetim portundan (Veri 1) yönetebilirsiniz. Yapılandırmanızı fabrika varsayılan ayarlarına sıfırlarsanız (örneğin, Sistem Kurulumu Sihirbazı'nı yeniden çalıştırarak), yönetim arayüzüne yalnızca Veri 1 bağlantı noktasından erişebilirsiniz (http://192.168.42.42), Veri 1 bağlantı noktasına bağlantı. 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.

Tebrikler, şimdi Cisco M380 ve Cisco M680 İçerik Güvenliği Yönetim Cihazınızı kullanmaya hazırsınız. Cihazdan daha fazla yararlanmak için aşağıdaki adımlardan bazılarını kullanmayı düşünebilirsiniz:

Güvenlik Araçları Ekleme

Yönetmek istediğiniz Cisco Email Security aygıtlarını ve Cisco Web Security aygıtlarını ekleyebilirsiniz. Cisco Security cihazlarını Cisco M380 ve Cisco M680'e eklemek için, Yönetim Araçları> Merkezi Hizmetler> Güvenlik Araçları'nı seçin.

Merkezi E-posta ve Web Raporlamayı Etkinleştirme

Cisco M380 ve Cisco M680 İçerik Güvenliği Yönetim Cihazı, hem e-posta raporlama hem de web raporlamanın yanı sıra, birden fazla E-posta ve Web Güvenliği Cihazı arasında e-posta ve web trafiğinin merkezi bir görüntüsünü sağlayan web izlemeyi de destekler.

Merkezi e-posta raporlamasını etkinleştirmek için, Yönetim Cihazı> Merkezi Hizmetler> E-posta> Merkezi Raporlama'yı seçin.

Merkezi web raporlamasını etkinleştirmek için, Yönetim Araçları> Merkezi Hizmetler> Web> Merkezi Raporlama'yı seçin.

Merkezi raporlamayı etkinleştirdikten sonra, Web ve e-posta raporlama için istatistikleri ve bilgileri Yönetim Cihazı> Merkezi Hizmetler> E-posta> Merkezi Raporlama veya Yönetim Cihazı> Merkezi Hizmetler> Web> Merkezi Raporlamaya Genel Bakış sayfasından görüntüleyebilirsiniz.

Mesaj İzleme

Mesaj İzleme hizmetini (GUI'de) kullanarak sorgular çalıştırarak mesaj gönderme ve engelleme hakkındaki ayrıntıları görüntüleyebilirsiniz.

E-posta güvenlik cihazının mesaj takibine erişmek için,

Monitör> Mesaj İzleme'yi seçin.

Planlanmış E-posta ve Web Raporlama

Cisco M380 ve Cisco M680 İçerik Güvenliği Yönetim Cihazı, E-posta veya Web Güvenliği Cihazınızdan gelen verilerden zamanlanmış raporlar oluşturmanıza olanak sağlar. Raporların günlük, haftalık veya aylık olarak çalıştırılması planlanabilir ve önceki güne, önceki yedi güne veya önceki aya ait verileri içerecek şekilde yapılandırılabilir.

Daha fazla bilgi

Cisco M380 ve Cisco M680 cihazınız için yapılandırmak isteyebileceğiniz başka özellikler de vardır. Mevcut diğer özellikler hakkında daha fazla bilgi için, Content Security Management cihazının belgelerine bakın.

Taşıma ve Nakliye Sırasında Dikkat Edilecek Hususlar

Sunucu Bilgisayarınızı taşıma ve nakliye sırasında herhangi bir hasardan kaçınmak için; Sunucu Bilgisayarınızı paketlerken, orijinal kutusunu veya paketleme malzemelerini kullanınız. Ürünü taşırken yere sert bir şekilde bırakmayın ve ürünün üzerine ağır nesneler koymayın. Bu ürüne zarar verebilir. Seyahat sırasında, Sunucu Bilgisayarı sağa sola kayabileceği genel raflara yerleştirmeyiniz. Sunucu Bilgisayarınızı düşürmeyiniz veya diğer mekanik şoklara maruz kalmamasını sağlayınız. Sunucu Bilgisayarınızı, bataryanızı ve hard-disk sürücünüzü kir, yiyecek, sıvı şeyler, aşırı sıcak, toz ve aşırı güneş ışığı gibi çevresel tehlikelerden koruyun. Sunucu Bilgisayarınızı çok farklı sıcaklık derecelerine sahip ortamlara ve/veya çok fazla nemli ortamlara götürdüğünüz zaman, Sunucu Bilgisayarınızın içinde veya üzerinde buğulanma oluşabilir. Sunucu Bilgisayarın zarar görmesini önlemek için Sunucu Bilgisayarı kullanmadan önce nemin buharlaşması için belli bir süre bekleyin.

Bilgi: Sunucu Bilgisayarınızı düşük sıcaklık sahip bir ortamdan, daha sıcak bir ortama veya yüksek sıcaktan daha serin bir ortama getirdiğinizde, güç vermeden önce oda sıcaklığına uyum sağlamasına izin verin.

Kullanım Hatalarına İlişkin Bilgiler

Sunucu Bilgisayarınızın tüm bağlantılarını kullanım kılavuzunda belirtilen şeklinde yapınız. Aslı bir bağlantı şekli Sunucu Bilgisayarınızın garanti kapsamı dışına çıkmasına neden olabilir. Sunucu Bilgisayarınızın üzerinde tadilat, onarım, oynama veya herhangi bir fiziksel müdahalede bulunmayınız. Sunucu Bilgisayarınızın barkodunun, model ve seri numarasının zarar görmemesine özen gösteriniz. Bunların okunmaması veya yıpranmış olması halinde cihazınız garanti kapsamından çıkacaktır. Sunucu Bilgisayarınızın orijinal kutusu veya ambalajı dışında ve düzgün olmayan fiziksel koşullarda saklanması. Sunucu Bilgisayarınızla bir başka ürünün beraber kurulumu, kullanımı sırasında ortaya çıkabilecek problemler, Sunucu Bilgisayarınızın garanti kapsamının dışındadır. Olağandışı fiziksel veya elektriksel koşullara, yüklemeye maruz bırakılmaması, elektrik arızaları veya kesintileri, yıldırım, statik elektrik, yangın ve diğer doğal afetler sonucu ortaya gelebilecek sorunlar ürününüzün garanti kapsamı dışındadır. İşlevinden emin olmadığınız programları, oyunları Sunucu Bilgisayarınıza yüklememeye, kaynağını ve sağlam olduğunu kesin olarak bilmediğiniz disket ve cd' leri Sunucu Bilgisayarınızda kullanmamaya gayret ediniz. Bu yolarlarla ve internet üzerinden Sunucu Bilgisayarınıza bulaşacak virüsler mevcut program ve sisteme zarar verecek ve sizi maddi zarara uğratacaktır. Sunucu Bilgisayarınızı etikette belirtilen güç tipiyle çalıştırınız. Tüm bağlantıları Sunucu Bilgisayarınız kapalı durumundayken yapınız. Sunucu Bilgisayarınız çalışırken herhangi bir bağlantıyı çıkarmaya ya da yeni bağlantılar yapmaya çalışmayınız.

 Uyarı	**ÖNEMLİ GÜVENLİK TALİMATLARI** Bu uyarı sembolü tehlike anlamına gelir. Bedensel yaralanmaya neden olabilecek bir durumdasınız. Herhangi bir ekipman üzerinde çalışmadan önce, elektrik devreleriyle ilgili tehlikelere dikkat edin ve kazaları önlemek için standart uygulamalara aşina olun. Çevirisini, bu cihazın beraberindeki çevrilmiş güvenlik uyarılarına göre bulmak için, her bir uyarı sonunda verilen bildirim numarasını kullanın.

Tüketicinin Kendi Yapabileceği Bakım, Onarım Veya Ürünün Temizliğine İlişkin Bilgiler

Temizlikten önce bu ürünü duvardaki elektrik prizinden çıkartın. Sıvı temizleyiciler yâda aerosol temizleyiciler kullanmayın. Temizlik için nemli bir bez kullanın. Sunucu Bilgisayarınızın temizliğini yaparken aşağıdaki adımları takip edin:

1. Sunucu Bilgisayarı kapatın ve bataryayı çıkartın.

2. Güç kablosunu çıkartın.

3. Nemlendirilmiş yumuşak bez kullanın. Sıvı maddeler veya aerosol temizleyiciler kullanmayın.

4. Kir veya aşındırıcı içermeyen cam temizleyiciler ve yumuşak temiz bezlerle ekranı temizleyiniz. Beze temizleyici uygulayınız, sonra ekranı üst kısmından alt kısmına doğru tek doğrultuda silin. Eğer ekran bazı kirleticiler veya yağ içeriyorsa, cam temizleyiciler yerine izoprobil alkol kullanın. Eğer Sunucu Bilgisayarınıza iyi bakarsanız oda size iyi hizmet eder. Sunucu Bilgisayarı doğrudan güneş ışığına maruz bırakmayın. Radyatör gibi ısı kaynaklarının yakınına koymayın. Sunucu Bilgisayarınızı 0°C (32°F) dan aşağı veya 50°C (122°F) yukarı sıcaklıklara maruz bırakmayın. Sunucu Bilgisayarınızı manyetik alanlara maruz bırakmayın. Sunucu Bilgisayarınızı yağmura veya rutubete maruz bırakmayın. Sunucu Bilgisayarın üstüne su veya herhangi bir sıvı damlatmayın. Sunucu Bilgisayarı aşırı zorlamaya ve titreşime maruz bırakmayın. Sunucu Bilgisayarınızı toza ve kire maruz bırakmayın. Sunucu Bilgisayarın üstüne herhangi bir nesne koymayın. Sunucu Bilgisayarınızı dengesiz veya düz olmayan zeminlere koymayın.

Güç Kablosu

Güç kablosu ile ilgili bazı bilgiler: Güç kablonuzu diğer cihazlara bağlamayın. Güç kablosunu üstüne basmayın veya üstüne ağır nesneler koymayın. Güç kablosunu insanların yürüdüğü veya gezindiği alanların uzağından geçirin. Güç kablosunu prizden çıkarırken kablodan tutup çekmeyin. Fişi tutarak prizden çıkarın. Bu işlem esnasında giriş yuvasının veya bağlantı noktasındaki metal uçların bükülmemesi için kabloyu çıkarırken düzgün bir şekilde tutunuz. Ayrıca, bir kabloyu bağlamadan önce her iki bağlayıcılarında tam olarak düzenlendiğinden ve yönlendirildiğinden emin olun. Bir elektrik priz grubuna takılan cihazların toplam akım oranı bu elektrik priz grubunun toplam akım oranını aşmamalıdır. Ayrıca bir prize takılan toplam cihaz akım oranı sigorta değerini aşmamalıdır. Güç kablosunun üzerinde hiç bir cisim olmamasına ve kablonun üzerine basılabilecek bir yerde olmamasına dikkat ediniz.

ÜRÜN HERHANGİ BİR PERİYODİK BAKIM ONARIM GEREKTİRMEMEKTEDİR.

Malın enerji tüketimi açısından verimli kullanımına ilişkin bilgiler:

Satın almış olduğunuz ürünün ömrü boyunca enerji tüketimi açısından verimli kullanımı için bakım hizmetlerinin yetkilendirilmiş sertifikalı elemanlarca yapılması, periyodik bakımlarının aksatılmaması gerekmektedir. Cihazınızın bu kullanım kılavuzunda belirtilen çevresel karakteristiklere uygun ortamlarda çalıştırılması gerekmektedir.

Bu ürün, güç tüketimini azaltacak ve ürün performansından taviz vermeden doğal kaynaklardan tasarruf etmeyi sağlayacak şekilde tasarlanmıştır.

Ürün, hem çalışma sırasında hem de aygıt kullanılmadığında toplam enerji tüketimini azaltacak şekilde tasarlanmıştır.

Güç tüketimiyle ilgili özel bilgiler, aygıtla birlikte gelen basılı belgede bulunabilir.

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