WEB GÜVENLİK CİHAZI KULLANMA KILAVUZU
MARKA: CİSCO
MODELLER: S380

Güvenlik için, ağınızın kötü amaçlı yazılımdan koruma, uygulama görünürlüğü ve kontrolü, kabul edilebilir kullanım politikası kontrolleri, içgörülü raporlama ve güvenli mobilite ihtiyacı vardır. Cisco bu korumayı tek bir platformda sunmaktadır: Cisco ® Web Güvenlik Cihazı (WSA).
Bağlantılı ve gittikçe artan mobil dünyamızda, daha karmaşık ve karmaşık tehditler doğru güvenlik çözümleri karışımını gerektirir. Cisco, işletmelerin ihtiyaç duyduğu güçlü koruma, tam kontrol ve yatırım değeri ile tüm ağ altyapısı katmanları için güvenlik sağlar. Ayrıca pazar lideri küresel tehdit istihbaratı ile birlikte geniş bir web güvenliği dağıtım seçeneği sunuyoruz. Cisco WSA, yüksek performanslı, özel bir cihazla güvenliği kolaylaştırır ve Cisco Web Güvenliği Sanal Uygulaması (WSAV) işletmelerin web güvenliğini nerede ve ne zaman ve nerede olursa olsun hızlı ve kolay bir şekilde dağıtmalarına izin verir.

Cisco WSA, kuruluşların web trafiğini güvence altına almanın ve kontrol etmenin zorluklarını ele almasına yardımcı olmak için önde gelen korumaları birleştiren ilk güvenli web ağ geçitlerinden biriydi. Daha az bakım gereksinimi, düşük gecikme süresi ve daha düşük işletme maliyetleri ile daha basit ve daha hızlı dağıtım sağlar. “Ayarla ve unut” teknolojisi, ilk otomatik politika ayarları yayınlandıktan sonra personeli serbest bırakır ve otomatik güvenlik güncellemeleri her 3 ila 5 dakikada bir ağ cihazlarına gönderilir. Esnek dağıtım seçenekleri ve mevcut güvenlik altyapınızla entegrasyon, hızla gelişen güvenlik gereksinimlerini karşılamanıza yardımcı olur.

Sanal Uygulama

Video ve diğer zengin medyaların büyümesiyle birlikte trafik, tahmin edilemez hale geldi, bu da ortalamalara ve performansın düşmesine neden oldu. Bu ve diğer hususları ele alan yöneticiler, özellikle çok uluslu kuruluşlarda donanım, uzaktan kurulum zorlukları, gümrük vergileri ve diğer lojistik sorunları satın alırken ve kurarken uzun süre dayanırlar.

Cisco WSAV, yöneticilerin ihtiyaç duydukları yerde ve zamanda güvenlik örnekleri oluşturmalarını sağlayarak, özellikle yüksek oranda dağıtılmış ağlarda web güvenliğini kullanma maliyetini önemli ölçüde azaltır. Cisco WSAV, bir VMware ESXi veya KVM hipervizörü ve Cisco Unified Computing System ™ (Cisco UCS ®) sunucuları üzerinde çalışan Cisco WSA'nın yazılım sürümüdür. İlgili SMA yazılım lisansıyla birlikte Cisco Email veya Web Security yazılım paketlerinden herhangi birini satın alarak Cisco SMAV için sınırsız bir lisans alacaksınız.
Cisco WSAV ile yöneticiler trafik artışlarına anında cevap verebilir ve kapasite planlamasını ortadan kaldırabilir. Aletler alıp göndermeye gerek yoktur; veri merkezine karmaşıklık eklemeden veya ek personel gerektirmeden yeni iş fırsatları desteklenebilir.

Özellikler ve faydalar

Talos Güvenlik İstihbaratı	Aşağıdakiler de dâhil olmak üzere en geniş görünürlük ve en büyük yer kaplayan, dünyanın en büyük tehdit algılama ağı tarafından desteklenen hızlı ve kapsamlı web koruması alın: ● Günlük 100 TB güvenlik zekâsı ● Güvenlik duvarı, IPS, web ve e-posta cihazları dâhil olmak üzere 1,6 milyon konuşlu güvenlik cihazı ● 150 milyon son nokta ● Günde 13 milyar web talebi ● dünyadaki e-posta trafiğinin% 35’i Anormallikleri analiz etmek, yeni tehditleri ortaya çıkarmak ve trafik eğilimlerini izlemek için global trafik aktivitesine 24x7 bakış sağlar. Talos, sürekli olarak her üç ila beş dakikada bir WSA güncellemeleri besleyen yeni kurallar üreterek sıfır

	saatli saldırıları önler, böylece endüstri lideri tehdit savunma saatleri ve hatta günler öncesinde rakipleri önler.
Cisco Web Kullanım Kontrolleri	Uyumluluk, sorumluluk ve verimlilik risklerini azaltmak için geleneksel URL filtrelemeyi dinamik içerik analiziyle birleştirin. Cisco'nun 50 milyondan fazla engellenen siteden oluşan sürekli güncellenen URL filtreleme veritabanı, bilinen web siteleri için istisnai kapsam sağlar ve Dinamik İçerik Analizi (DCA) motoru, bilinmeyen URL'lerin gerçek zamanlı olarak yüzde 90'ını doğru bir şekilde tanımlar; metni tarar, alaka düzeyine göre metni puanlandırır, model belge yakınlığını hesaplar ve en yakın kategori eşleşmesini döndürür. Yöneticiler ayrıca, akıllı HTTPS incelemesi için belirli kategoriler seçebilir.
Gelişmiş Kötü Amaçlı Yazılım Koruması	Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP), tüm Cisco WSA müşterileri için mevcut ek bir lisans özelliğidir. AMP, kötü amaçlı yazılım algılama ve engelleme, sürekli analiz ve geçmişe dönük uyarı vermeyi sağlayan kapsamlı bir kötü amaçlı yazılım yenen bir çözümdür. Hem Cisco hem de Sourcefire ® teknolojisinin geniş bulut güvenliği istihbarat ağlarından yararlanır. AMP, Cisco WSA'da zaten sunulan kötü amaçlı yazılım algılama ve engelleme yeteneklerini, gelişmiş dosya itibar özellikleri, ayrıntılı dosya davranışı raporlaması, sürekli dosya analizi ve geriye dönük karar uyarısı ile güçlendirir. Cisco AMP Tehdit IzgarasıKötü amaçlı yazılım örneklerini buluta göndermeye ilişkin uyumluluk veya politika kısıtlamaları olan kuruluşlar için şirket içi bir araçla kötü amaçlı yazılımdan koruma sağlar. Katman 4 Trafik Monitörü, casus yazılım "telefon ev" iletişimini algılayarak ve engelleyerek etkinlikleri sürekli olarak tarar. Tüm ağ uygulamalarını izleyerek, Layer 4 Traffic Monitor, klasik web güvenliği çözümlerini atlamaya çalışan kötü amaçlı yazılımları etkili bir şekilde durdurur. Bilinen kötü amaçlı yazılım alan adlarının IP adreslerini, engellenecek kötü amaçlı varlıklar listesine dinamik olarak ekler.
Bilişsel Tehdit Analitiği	Cisco Cognitive Threat Analytics, ağ içinde çalışan tehditlerin keşfedilmesi için gereken zamanı azaltan bulut tabanlı bir çözümdür. Davranış analizi ve anomali tespitini kullanarak bir malware enfeksiyonunun veya veri ihlali semptomlarını tanımlayarak çevre tabanlı savunmalardaki boşlukları giderir. Web Güvenliği çözümünüz için basit bir eklenti lisansıyla Cisco Cognitive Threat Analytics'ten yararlanın. Değişen tehdit ortamınızla birlikte gelişen üstün koruma kazanırken karmaşıklığı azaltın.
Uygulama Görünürlüğü ve Kontrolü (AVC)	Yüzlerce Web 2.0 ve 150.000'den fazla mikro uygulamanın kullanımını kolayca kontrol edin. Ayrıntılı politika kontrolü, yöneticilerin kullanıcıları belge yükleme veya "Beğen" düğmesini tıklatma gibi etkinliklerden engellerken Dropbox veya Facebook gibi uygulamaların kullanımına izin vermesini sağlar. WSA, ağın tamamındaki faaliyet görünürlüğünü destekler. Yeni: Müşteriler, kullanıcı başına, grup başına ve politikaya göre özelleştirilmiş bant genişliği ve zaman kotalarını kullanabilir.
Veri Kaybını Önleme (DLP)	Temel DLP için bağlam temelli kurallar oluşturarak gizli verilerin ağdan çıkmasını önleyin. Cisco WSA ayrıca, derin içerik incelemesi ve DLP politikalarının uygulanması için üçüncü taraf DLP çözümleriyle entegrasyon için Internet İçerik Uyum Protokolü'nü (ICAP) de kullanır. Cisco WSA ayrıca, WSA ile üçüncü taraf DLP çözümleri arasında yapılan trafiği şifrelemek için Secure ICAP'ı da destekler.

Dolaşım-Kullanıcı Koruması	Cisco WSA, dolaşımdaki kullanıcıları , trafiği şirket içi çözümlere yönlendiren bir VPN tüneli başlatarak web güvenliği sağlayan Cisco AnyConnect ® Güvenli Mobilite İstemcisi ile bütünleşerek korur . Cisco AnyConnect teknolojisi, erişime izin vermeden önce trafiği gerçek zamanlı olarak analiz eder. Cisco WSA, Cisco Identity Services Engine (ISE) ile de entegre edilmiştir. Bu heyecan verici gelişmeyle müşteriler talep üzerine Cisco ISE için Cisco ISE'nin gücünden faydalanabilirler. Cisco ISE entegrasyonu, yöneticilerin Cisco ISE tarafından tek oturum açma işlemi sırasında toplanan profil veya üyelik bilgilerine dayanarak Cisco WSA'da politika oluşturmasını sağlar.
Merkezi Yönetim ve Raporlama	Tehditler, veriler ve uygulamalar hakkında işlem yapılabilir bilgiler edinin. Cisco WSA, işlemleri kontrol etmek, politikaları yönetmek ve raporları görüntülemek için kullanımı kolay, merkezi bir yönetim aracı sunar. Cisco M Serisi İçerik Güvenliği Yönetim Cihazı, sanal örnekler dahil olmak üzere birden fazla cihaz ve birden fazla yerde merkezi yönetim ve raporlama sağlar. Cisco ® Web Security Raporlama Uygulaması hızla endeksler ve Cisco Web Güvenlik Araçları (WSA) ve Cisco Bulut Web Güvenliği (CWS) oluşturduğu günlükleri analiz eden bir raporlama çözümü. Bu araç, yoğun trafik ve depolama ihtiyacı olan müşterilere ölçeklenebilir raporlama sağlar. Rapor yöneticilerinin web kullanımı ve kötü amaçlı yazılım tehditleri hakkında ayrıntılı bilgi edinmelerini sağlar.
Esnek Dağıtım	Cisco WSAV, anında self servis sağlama dahil, sanal bir dağıtım modelinin ek kolaylık ve maliyet tasarrufu ile Cisco WSA ile aynı özellikleri sunar. Bir Cisco WSAV lisansıyla, şirketler, lisansı yerel olarak depolanan yeni bir Cisco WSAV sanal görüntü dosyasına uygulayarak, Internet güvenliği sanal ağ geçitlerini İnternet'e bağlanmadan dağıtabilirler. Gerekirse, birkaç web güvenliği ağ geçidini hemen dağıtmak için bozulmamış sanal görüntü dosyaları klonlanabilir. Donanım ve sanal makineleri aynı dağıtımda çalıştırın. Küçük şubeler veya uzak konumlar, Cisco WSA'nın o bölgeye donanım kurmak ve desteklemek zorunda kalmadan sağladığı korumaya sahip olabilir. Özel dağıtım, Cisco M Serisi İçerik Güvenlik Yönetimi Cihazı ile kolayca yönetilir.

Ürün Özellikleri

Tablo 1 ve 2, sırasıyla Cisco WSA performans ve donanım özelliklerini vermektedir.

Tablo 1. Cisco WSA Performans Özellikleri

	Model	Disk alanı	RAID Yansıtma	Bellek	CPU'lar
Orta Ölçekli Ofis	S380	2,4 TB (4x600 GB SAS)	Evet (RAID 10)	16 GB, DDR3	1 x 2.0 GHz, 6C

* Çözümünüzün mevcut ve öngörülen gereksinimlerinizi karşılamasını sağlamak için lütfen boyutlandırma kılavuzunu bir Cisco içerik güvenlik uzmanıyla onaylayın.

Tablo 2. Cisco WSA Donanım Özellikleri

	Cisco S380
Donanım Platformu	
Form faktörü	2RU
Boyutlar	3,5 ”x 19” x 29 ”
Yedek P / S	Evet
Uzaktan güç döngüsü	Evet
DC Güç Seçeneği	Evet (930W)
Çalışırken Değiştirilebilir H / D	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	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
İşlemci	Bir adet E5–2620 v3 işlemci
Veri deposu	Dört adet 8GB DDR4-2133 DIMM1

Tablo 3, Cisco WSAV teknik özelliklerini listeler ve Tablo 4, Cisco M Serisi İçerik Güvenliği Yönetim Cihazı için olanları listeler.

Tablo 3. Cisco WSAV

Model	**Disk**	**Bellek**	**Çekirdekler**
S000v	250 GB	4 CİGABAYT	1
S100v	250 GB	6 GB	2
S300v	1024 GB	8 GB	4
S600v	2,4 TB	24 GB	12

Sunucular		Hiper	
Cisco UCS Red Hat Enterprise Linux 7.0 Ubuntu 14.04.1 LTS		ESXi 5.0, 5.1 ve 5.5 ve 6.0 KVM: QEMU 1.5.3 KVM: QEMU 2.0.0	vmware KVM

** Sadece Web Rep, URL filtreleme, Sophos ve Webroot özelliklerine uygulanabilir. AMP, TG gibi ek özellikler bu modeli değerlendirme moduna geçirecektir.

Tablo 4. Cisco M Serisi İçerik Güvenliği Yönetim Cihazı

Model	Cisco M680	Cisco M380	Cisco M170
Kullanıcılar (yaklaşık)	10.000'in	10.000'e kadar	1.000'e kadar

Yayılma

Cisco WSA, Açık modda (proxy otomatik yapılandırma [PAC] dosyaları, Web Proxy Otomatik Bulma [WPAD], tarayıcı ayarları) veya Şeffaf modda (Web Önbellek İletişim Protokolü [WCCP], Politika-) dağıtılabilen ileri bir proxy'dir. Tabanlı Yönlendirme [PBR], yük dengeleyici). Cisco Catalyst gibi WCCP-uyumlu cihazlar, ® 6000 Serisi Anahtarlar Cisco ASR 1000 Serisi Toplama Hizmetleri Router, Cisco Integrated Services Routers ve Cisco ASA 5500-X Serisi Yeni Nesil Firewall Cisco WSA web trafiği yönlendir.
Cisco WSA, veri kaybını önleme, mobil kullanıcı güvenliği ve gelişmiş görünürlük ve kontrol gibi ek özellikler sağlamak için HTTP, HTTPS, SOCKS, yerel FTP ve HTTP trafiği üzerinden FTP proxy'si yapabilir.

Ruhsat verme

Bir Cisco WSAV lisansı, tüm Cisco Web Security yazılım paketlerinde bulunur (Cisco Web Security Essentials, Cisco Web Security Antimalware ve Cisco Web Security Premium). Bu lisans, paketteki diğer yazılım hizmetleri ile aynı terime sahiptir ve gerektiği kadar çok sanal makine için kullanılabilir.

Terime Dayalı Abonelik Lisansları

Lisanslar bir, üç veya beş yıllık dönem tabanlı aboneliklerdir.

Miktar Tabanlı Abonelik Lisansları

Cisco Web Security portföyü, cihazlara değil, bir dizi kullanıcıya göre katmanlı fiyatlandırma kullanır. Satış ve iş ortağı temsilcileri, her müşteri konuşlandırması için doğru boyutlandırmanın belirlenmesine yardımcı olabilir.

Web Güvenliği Yazılım Lisansları

Dört web güvenliği yazılımı lisansı mevcuttur: Cisco Web Security Essentials, Cisco Anti-Malware, Cisco Web Security Premium ve McAfee Anti-Malware. Her bir yazılımın ana bileşenleri aşağıdaki gibidir:

Cisco Web Güvenliği Gereklilikleri

- Cisco Talos ile Tehdit İstihbaratı
- Katman 4 trafik izleme
- Uygulama Görünürlüğü ve Kontrolü (AVC)
- Politika yönetimi
- İşlem yapılabilir raporlama
- URL filtreleme
- ICAP üzerinden üçüncü taraf DLP entegrasyonu

Cisco Anti-Malware

- Gerçek zamanlı kötü amaçlı yazılım taraması

Cisco Web Security Premium

- Web Güvenliği Gereklilikleri
- Gerçek zamanlı kötü amaçlı yazılım taraması

Gelişmiş Kötü Amaçlı Yazılım Koruması

- AMP, kötü amaçlı yazılım algılama ve engelleme yeteneklerini dosya itibarı puanlaması ve engellemesi, statik ve dinamik dosya analizi (sanal alan) ve tehditlerin sürekli analizi için dosya retrospektifiyle artırır.

Bilişsel Tehdit Analitiği

· CTA, yeni tehditleri bağımsız olarak tanımlamak, gördüklerini öğrenmek ve zaman içinde uyum sağlamak için gelişmiş istatistiksel modelleme ve makine öğrenmeye dayanır.

McAfee Anti-Malware

- McAfee gerçek zamanlı kötü amaçlı yazılım taraması, tek bir alakart lisans olarak kullanılabilir.

Yazılım Lisans Sözleşmeleri

Cisco Son Kullanıcı Lisans Sözleşmesi (EULA) ve Cisco Web Güvenliği Eki Son Kullanıcı Lisans Sözleşmesi (SEULA), her bir yazılım lisansı satın alımında verilmektedir.

Yazılım Abonelik Desteği

Tüm Cisco Web Security lisansları, iş için kritik uygulamaları kullanılabilir, güvenli ve en üst düzeyde performansta tutmak için gerekli yazılım abonelik desteğini içerir. Bu destek, müşterilere, satın alınan yazılım aboneliğinin tam süresi boyunca aşağıdaki hizmetleri sağlar:

- Uygulamaların en güncel özellik setinde optimum performans göstermesini sağlamak için yazılım güncellemeleri ve büyük güncellemeler
- Hızlı ve özel destek için Cisco Teknik Yardım Merkezi'ne (TAC) erişim
- Şirket içi uzmanlığı geliştirmek ve genişletmek ve iş çevikliğini artırmak için çevrimiçi araçlar
- Ek bilgi ve eğitim fırsatları için ortak öğrenme

Hizmetler

Tablo 5, Cisco Web Security servislerini listeler.

Tablo 5. Cisco Web Güvenlik Hizmetleri

Cisco Markalı Servisler	Cisco Güvenlik Planlama ve Tasarımı: Sağlam bir güvenlik çözümünün hızlı ve düşük maliyetli bir şekilde kullanılmasını sağlar. Cisco Web Güvenliği Konfigürasyonu ve Kurulumu: Uygulanacak cihazları kurarak, yapılandırarak ve test ederek web güvenliği risklerini azaltır: ● Kabul edilebilir kullanım politikası denetimleri ● İtibar ve kötü amaçlı yazılım filtreleme ● Veri güvenliği ● Uygulama görünürlüğü ve kontrolü Cisco Güvenlik Optimizasyonu Hizmeti: Güvenlik tehditlerini, tasarım güncellemelerini, performans ayarlamalarını ve sistem değişikliklerini ele almak için gelişen bir güvenlik sistemini destekler.
Ortak / Ortak Hizmetler	Ağ Aygıtı Güvenlik Değerlendirmesi: Ağ altyapısı güvenliğindeki boşlukları belirleyerek sertleştirilmiş bir ağ ortamının korunmasına yardımcı olur.

	Akıllı Bakım: Güvenli görünürlükten ağ performansını elde etmek için elde edilebilecek istihbarat sağlar Ek hizmetler: Cisco iş ortakları, planlama, tasarım, uygulama ve optimizasyon yaşam döngüsü boyunca çok çeşitli değerli hizmetler sunar.
Cisco Finansmanı	Cisco Capital ® , finansman çözümlerini iş ihtiyaçlarına göre uyarlayabilir. Cisco teknolojisine daha erken erişin ve iş avantajlarını daha erken görün.

KURULUM

Kurulumu Planlayın

Ağınızdaki Cisco S380 Web Güvenlik Cihazını nasıl yapılandıracağınıza karar verin.

Cisco S380 tipik olarak istemcilerle İnternet arasındaki ağda ek bir katman olarak kuruludur.

Cihazı nasıl dağıttığınıza bağlı olarak, istemci trafiğini cihaza yönlendirmek için bir Katman 4 (L4) anahtarına veya bir WCCP yönlendiricisine ihtiyacınız olabilir veya gerekmeyebilir.

Dağıtım seçenekleri şunları içerir:

• Şeffaf Proxy - L4 anahtarlı Web proxy'si

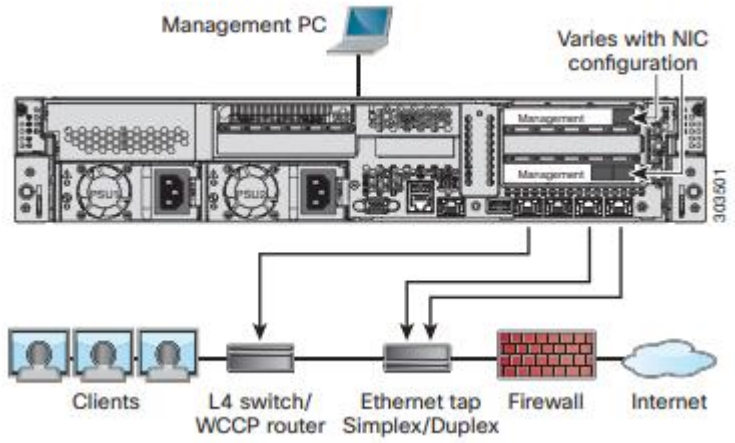
• Şeffaf Proxy - WCCP yönlendiricili Web proxy'si

• Açık İletimli Proxy - Bir ağ anahtarına bağlantı

• L4 Trafik Monitörü - Ethernet bağlantısı (tek taraflı veya çift taraflı)

- Simpleks Modu: T1 Limanı tüm giden trafiği alır ve T2 Limanı gelen tüm trafiği alır.

- Dubleks Modu: T1 Limanı tüm gelen ve giden trafiği alır.



Not Gerçek istemci IP adreslerini izlemek için, L4 trafik monitörü her zaman güvenlik duvarı içinde ve NAT'tan önce yapılandırılmalıdır (Ağ Adresi Çevirisi).

Cihazı Rafa Kurma

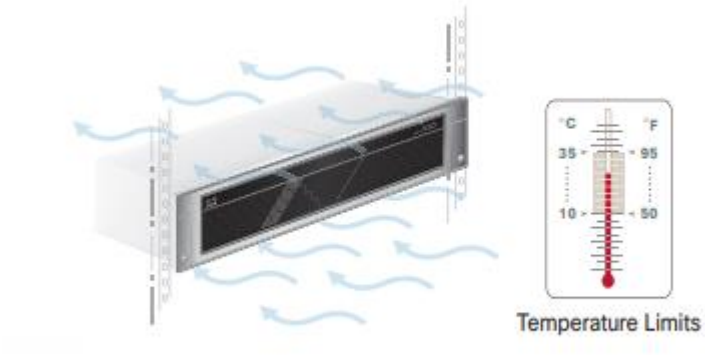
Verilen sürgü raylarını kullanarak Cisco S380 Web Güvenlik Cihazı'nı kurun. Cihazı rafa takma hakkında bilgi için Cisco 380 Serisi Donanım Kurulum Kılavuzu'na bakın.

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.



Cihazın fişini 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 S380'e bağlanmak için, bilgisayarınızın IP adresini geçici olarak değiştirmeniz gerekir.

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

Pencereler için

Adım 1 Sistem kutusunda bulunan Ethernet kablosunu kullanarak dizüstü bilgisayarınızı Yönetim bağlantı noktasına bağlayın. Cisco S380 cihazı sadece Yönetim portunu kullanır. Sayfa 8'deki "Kurulumu Planlayın" bölümüne bakın.

Adım 2 başlat menüsüne gidin ve Denetim Masası'nı seçin.

Adım 3 Ağ ve Paylaşım Merkezi'ni çift tıklatın.

Adım 4 Yerel Ağ Bağlantısı'na tıklayın ve ardından Özellikler'e tıklayın.

Adım 5 İnternet Protokolü'nü (TCP / IP) seçin ve ardından Özellikler'e tıklayın.

Adım 6 Aşağıdaki IP Adresini Kullan'ı seçin.

Adım 7 Aşağıdaki değişiklikleri girin:

- IP Adresi: 192.168.42.43

- Alt Ağ Maskesi: 255.255.255.0

- Varsayılan Ağ Geçidi: 192.168.42.1

Adım 8 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.

Alete Bağlan

Ethernet kablolarını Cisco S380 cihazının arka panelindeki uygun bağlantı noktalarına takın.

• Proxy portları P1 ve P2 olarak etiketlenmiştir.

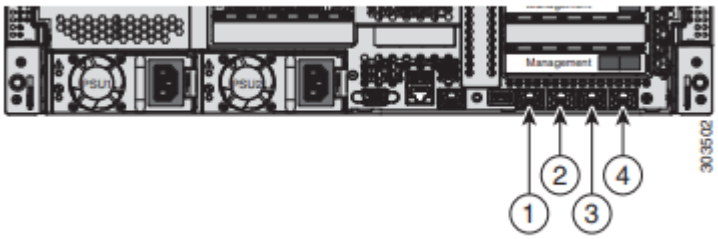
- Yalnızca P1 etkin: Yalnızca P1 etkin olduğunda, gelen ve giden trafik için ağa bağlayın.

- P1 ve P2 etkin: Hem P1 hem de P2 etkin olduğunda, P1'i dâhili ağa ve P2'yi İnternete bağlamanız gerekir.

• Trafik izleme portları T1 ve T2 olarak etiketlenmiştir.

- Simpleks musluk: T1 ve T2 bağlantı noktaları; İnternet için hedeflenen tüm paketler için bir kablo (T1) ve İnternet'ten gelen tüm paketler için bir kablo (T2).

- Çift yönlü kademe: Port T1; Tüm gelen ve giden trafik için tek bir kablo.



Madde	Port	Açıklama
1	P1	Proxy bağlantı noktasını belirtir. Hem gelen hem de giden trafik için P1'i ağa bağlayın.
2	P2	Proxy bağlantı noktasını belirtir. Hem P1 hem de P2 etkinleştirildiğinde, P1'i dâhili ağa ve P2'yi İnternete bağlamanız gerekir. P1 ve P2, L4 anahtarına, WCCP yönlendiricisine veya ağ anahtarına bağlanabilir.
3	T1	Dubleks Ethernet musluğu için trafik izleme portu T1'i gösterir: Tüm gelen ve giden trafik için bir kablo.
4	T2	Trafik izleme portunu gösterir. Simplex Ethernet musluğu: T1 ve T2 portları. İnternet için hedeflenen tüm paketler için bir kablo (T1) ve İnternet'ten gelen tüm paketler için bağlanabilir (T2).

Not Cihazınızla bir NIC kartı sipariş ettiyseniz, Cisco 380 Serisi Donanım Kurulum Kılavuzu'nun PCI NIC Yuvası Yapılandırmaları bölümündeki ayrıntılı bilgilere bakın.

Cihazı Güçlendirin

Cisco S380'in 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.

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 kontrol cihazının senkronize edilmesine izin verecek şekilde tasarlanır.

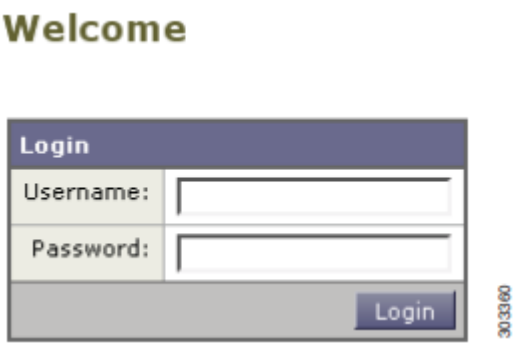
Cihazda Giriş Yap

İki arabirimden birini kullanarak Cisco S380'e giriş yapabilirsiniz: web tabanlı arayüz veya komut satırı arayüzü.

Web Tabanlı Arayüz

Adım 1 Ethernet portu üzerinden web tarayıcısına erişmek için (bkz. "Cihaza Bağlan" bölümü, sayfa 13), bir web tarayıcısına aşağıdaki URL'yi girerek 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" bölümü, sayfa 13), 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 S380 Web Güvenlik 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.

Web güvenlik cihazı aşağıdaki bağlantı noktalarında dinleyebilmelidir:

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

• HTTP: 80 numaralı bağlantı noktası

• HTTPS: 443 numaralı bağlantı noktası

• Yönetim erişimi: 8443 (HTTPS) ve 8080 (HTTP) bağlantı noktaları

• SSH: 22 numaralı bağlantı noktası

Web güvenlik cihazı, aşağıdaki bağlantı noktalarında giden bir bağlantı kurabilmelidir:

• DNS: 53 numaralı bağlantı noktası

• 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

• SMTP: 25 numaralı bağlantı noktası

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

Yapılandırma Özeti

Madde	Açıklama
Yönetim	Web güvenlik cihazını, http://192.168.42.42:8080 girerek veya Sistem Kurulum Sihirbazı'nı tamamladıktan sonra yönetim arayüzüne atanan IP adresini kullanarak yönetim portundan (Yönetim portu) yönetebilirsiniz. Yapılandırmanızı fabrika varsayılan ayarlarına sıfırlarsanız (örneğin, Sistem Kurulumu Sihirbazı'nı yeniden çalıştırarak), yönetim arabirimine yalnızca Yönetim portundan erişebilirsiniz (http://192.168.42.42:8080), Yönetim portuna bir bağlantı. Ayrıca, yönetim arabiriminizde güvenlik duvarı bağlantı noktalarını 80 ve 443'ü açtığınızı doğrulayın.
Veri	Sistem Kurulum Sihirbazı'nı çalıştırdıktan sonra, cihazdaki en az bir bağlantı noktası ağdaki istemcilerden web trafiğini alacak şekilde yapılandırılmıştır: yalnızca M1; M1 ve P1; M1, Pl ve P2; Sadece P1; veya P1 ve P2. **Not** Web proxy'sini açık ileri modda yapılandırdıysanız, istemci makinelerdeki uygulamaların, M1 veya P1 için veriler için yapılandırılmış IP adresini kullanarak web trafiğini web güvenlik cihazının web proxy'sine açıkça iletecek şekilde yapılandırılması gerekir.
Trafik İzleyicisi	Sistem Kurulum Sihirbazı'nı çalıştırdıktan sonra, bir veya her iki L4 trafik monitörü portu (yalnızca T1 veya her ikisi de T1 ve T2), tüm TCP portlarında trafiği dinleyecek şekilde yapılandırılır. L4 trafik monitörü için varsayılan ayar yalnızca monitördür. Kurulum sırasında veya sonrasında, L4 trafik izleyicisini şüpheli trafiği izleyecek ve engelleyecek şekilde yapılandırabilirsiniz.
Bilgisayar adresi	Bilgisayarınızın IP adresini, sayfa 11'deki "IP Adresinizi Geçici Olarak Değiştirin" bölümünde not ettiğiniz orijinal ayarlara getirmeyi unutmayın.

	Not Sistem ayarlarınızın bir özetini Sistem Yönetimi> Yapılandırma Özeti 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