



İNTERNET GÜVENLİK CİHAZI (FİREWALL)

Türkçe Tanıtım ve Kullanma Kılavuzu

MARKA: CISCO

MODEL

ASA5506W-X



TEKNİK ÖZELLİKLERİ

Ağ	
Bağlantı Teknolojisi:	Telli
Veri Bağlantı Protokolü:	Gigabit Ethernet, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n
Özellikler:	Fanless, Firewall koruması, VLAN desteği, VPN desteği
Form faktörü:	Masaüstü
Limanlar Miktarı:	8
Tür:	Güvenlik cihazı
Kablosuz İletişim Kuralı:	802.11 / b / g / n
Sağlanan Arayüz	
Bağlayıcı Türü:	RJ-45
Adet:	1
Tür:	1000Base-T (yönetim)
Bağlayıcı Türü:	Tip A
Tür:	USB 2.0
Tür:	Mini USB
Tür:	Konsol
Adet:	8
Tür:	1000BASET
Hizmet	
Destek Ayrıntıları Tam Sözleşme Süresi:	90 gün
Destek Ayrıntıları Dahil Hizmetler:	Peşin parça değişimi
Destek Ayrıntıları Tip:	Sınırlı garanti
Çeşitli	
Uyumlu Standartlar:	AS / NZS 60950, CAN / CSA C22.2 No. 60950, CISPR 22 Sınıf A, CISPR 24, CNS 13438, EN 300386, EN 301.489.1, EN 301.489.17, EN 301.489.24, EN 301.489.4, EN 301.489.7, EN 60950, EN 61000-3-2, EN 61000-3-3, EN55022, EN55024, IEC 60950, UL 60950,
Şifreleme Algoritması:	AES, Üçlü DES
Kabine	
Şasi Dahili Aygıtlar:	Kablosuz erişim noktası
Çevresel Parametreler	
Nem Aralığı Çalışma:	10 -% 90 (yoğuşmasız)
Maksimum Çalışma Sıcaklığı:	40 ° C
Minimum Çalışma Sıcaklığı:	0 ° C
Başlık	
Marka:	Cisco
Uyumluluk:	PC
Ülke Kitleri:	Kuzey Amerika
Üretici firma:	Cisco Sistemleri
Model:	Firepower Tehdit Savunması ile 5506W-X

	Paketli Miktar:	1
	Ürün hattı:	Cisco ASA
	Güç Aygıtı	
	Gerekli Sıklık:	50/60 Hz
	Nominal Gerilim:	AC 120/230 V
	Tür:	Harici güç adaptörü
	Servis desteği	
	Tür:	90 gün garanti
	Hizmet ve Destek Ayrıntıları	
	Tepki Süresi:	10 gün
	Sabit Disk Sürücüsü	
	Kapasite:	50 GB
	Kapasite	
	Tür:	Eşzamanlı oturumlar
	Değeri:	20000 (maksimum 50000)
	Tür:	Cisco AnyConnect Premium / Apex VPN eşleri
	Değeri:	2 (maksimum 50)
	Tür:	IPSec VPN eşleri
	Değeri:	10 (50'ye yükseltilebilir)
	Tür:	Sanal arabirimler (VLAN'lar)
	Değeri:	5 (30'a yükseltilebilir)
	PERFORMANS	
	Tür:	İnceleme çıktısı
	Değeri:	750 Mb / sn
	Tür:	Çok protokollü güvenlik duvarı çıktı
	Değeri:	300 Mbps
	Tür:	Bağlantı oranı
	Değeri:	Saniyede 5000 bağlantı
	Tür:	Uygulama denetimi (AVC) çıktı
	Değeri:	250 Mbps
	Tür:	Uygulama kontrolü (AVC) ve IPS çıktı
	Değeri:	125 Mb / sn
	Tür:	VPN çıktısı (3DES / AES)
	Değeri:	100 Mb / sn
	Tür:	Uygulama kontrolü (AVC) veya IPS boyutlandırma çıktıları

Değeri:	90 Mb / sn
Boyutlar ve Ağırlık	
Derinlik:	19.992 cm
Yükseklik:	4.369 cm
Ağırlık:	1,82 kg
Geniřliđi:	23.444 cm
Flash Bellek	
Yüklü Boyutu:	8 GB
Sabit sürücü	
Form faktörü:	mSATA
Yüklü Miktar:	1
Tür:	SSD
Veri deposu	
Yüklü Boyutu:	4 CİGABAYT

*** Periyodik bakım gerektirmemektedir ve ürüne tüketici kendi başına herhangi bir müdahalede bulunmamalıdır.

KULLANIM SIRASINDA İNSAN VE ÇEVRE SAĞLIđI AÇISINDAN TEHLİKELİ VEYA DİKKAT EDİLMESİ GEREKEN NOKTALAR İLE İLGİLİ UYARILAR:

Ana bilgisayar kasası genişleme yuvasına takılan kenar bađlayıcısı dışında, ařađıdaki tabloda X milimetre (mm) ve Y milimetre (mm) olarak listelenen boşluk ve atlama mesafeleri, kartlarla takılan tüm genişleme kartları da dâhil olmak üzere, ana bilgisayarın diđer parçaları arasında korunmalıdır.

Tablo: Voltaja Göre Atlama ve Boşluk Mesafeleri:

Ana Bilgisayarın Diđer Parçaları ya da Genişleme Kartı Tarafından Kullanılan veya Üretilen Voltaj (Vrms¹ veya VDC²)	Atlama (Y mm)³	Boşluk (X mm)
50'ye kadar	2.4 (3.8)	2.0
125'e kadar	3.0 (4.8)	2.6
250'ye kadar	5.0 (8.0)	4.0
300'e kadar	6.4 (10.0)	4.0

- 1Vrms = kök ortalama kare voltaj
- 2VDC =volt doğru akım
- 3Parantez içinde olmayan atlama mesafeleri, cihaz normal ofis ortamında kurulduğunda uygulanır.
- Parantez içindeki daha büyük olan mesafeler, cihaz, nem ve yoğunlaşma nedeniyle toz ve diđer türde kirlenmelerin elektrik iletebileceđi bir ortamda kurulduğunda uygulanır. Bu yüksek neme sahip bölgelerde geçerlidir.

- Tablo için aşağıdaki noktaları göz önünde bulundurun:
- Boşluk mesafeleri, havada iki nokta arasında ölçülen en küçük mesafe olarak tanımlanır (yani, görüş hattı)
- Atlama mesafeleri, iki nokta arasındaki bir yalıtkanın yüzeyinin bir tarafından öbür tarafına ölçülen en düşük mesafe olarak tanımlanır (yani, yalıtkanın dış hattını izleyerek)
- Şimşek etkinliği sırasında sistem üzerinde çalışmayın ve kabloları takıp çıkarmayın.
- Güç kablosu bağlıken güç kaynağına dokunmayın. Bir güç anahtarına sahip olan sistemlerde, güç anahtarı kapalı ve güç kablosu bağlı olduğunda bile, güç kaynağı içinde hat voltajı bulunur. Bir güç anahtarına sahip olmayan sistemlerde, güç kablosu bağlı olduğunda güç kaynağının içinde hat voltajı bulunmaz.
- Bir kasa üzerinde ya da güç kaynaklarının yakınında çalışmadan önce, AC birimlerindeki güç kablosunu fişten çekin; DC birimlerdeki akım kesicide gücün bağlantısını kesin.
- Açma/kapama anahtarı olan bir sistemde çalışmadan önce, gücü kapatın ve güç kablosunu fişten çekin.
- Bu ürün, binanın kısa devre (aşırı akım) korumasının kurulmasına dayanır. Faz iletkenleri (tüm akımı taşıyan iletkenler) için 120 VAC, 15A ABD (240VAC, 10A uluslararası) oranlarından daha büyük bir sigorta ya da akım kesici olmadığından emin olun.
- Aygıt, TN güç sistemleriyle çalışmak üzere tasarlanmıştır.
- Bu birim, erişimin yasaklandığı bir bölgede kurulacak şekilde tasarlanmıştır. Erişimin yasaklandığı bölge, yalnızca hizmet personelinin özel bir araç, kilit ve anahtar ya da başka bir güvenlik ögesi kullanarak erişebileceği ve bölgeden sorumlu yetkili tarafından denetlenen yerdir.
- AC bağlı birimler, güç kablosu topraklamasına ek olarak kalıcı bir toprak bağlantısına sahip olmalıdır. NEBS uyumlu topraklama bu gerekliliği karşılar.
- Bu ürünün en son imhası, tüm ulusal yasalara ve düzenlemelere uygun olarak gerçekleştirilmelidir.
- Güç hatlarına bağlı olan bir cihaz üzerinde çalışmadan önce, takılarınızı (yüzükler, kolyeler ve saatler dahil) çıkarın. Metal nesnelere, güç ve toprağa bağlandıklarında ısınır ve ciddi yanıklara neden olabilir ya da metal nesnelere kaynatarak yapıştırabilir.
- Yalnızca eğitimli ve uzman personele bu cihazı kurma veya değiştirme izni verilmelidir.
- Ethernet 10/100BaseT, G.SHDSL, seri, konsol ve yardımcı bağlantı noktaları güvenlik aşırı düşük voltaj (SELV) devreleri içerir. BRI devrelerine, telefon-ağ voltajı (TNV) devreleri gibi davranılır. SELV devrelerini, TNV devrelerine bağlamaktan kaçınınız.
- Elektrik şokundan kaçınmak için, telefon-ağ voltaj (TNV) devrelerine güvenli aşırı düşük voltaj (SELV) devreleri bağlamayın. LAN bağlantı noktaları SELV devreleri içerir ve WAN bağlantı noktaları TNV devreleri içerir.
- Bazı LAN ve WAN bağlantı noktalarının her ikisi de RJ-45 fişleri kullanır. Kabloları bağlarken dikkatli olun.
- BRI kablolarında tehlikeli ağ voltajları bulunur. BRI kablosunun bağlantısını keserken, olası elektrik şokundan kaçınmak için önce AccessPro kartından uzak olan ucun bağlantısını kesin. Güç kapalı olsa bile, BRI bağlantı noktası (RJ-45 fişi) bölgesindeki sistem kartında tehlikeli ağ voltajları bulunur.
- ISDN bağlantıları, kullanıcının teması açısından erişilmez voltaj kaynakları olarak düşünülmüştür. Herhangi bir genel telefon operatörü (PTO) tarafından sağlanan cihaz veya bağlantı donanımını kurcalamayın ya da açmayın. Herhangi bir sabit kablo bağlantısı (çıkarılmayan, yalnızca bir kez takılan fişler dışında) yalnızca PTO ekibi ya da uygun şekilde eğitim görmüş mühendisler tarafından yapılmalıdır.

- Yöneltecinin gücü Açık ya da Kapalı, nasıl olursa olsun, WAN bağlantı noktalarında tehlikeli ağ voltajı bulunur. Elektrik şokundan kaçınmak için, WAN bağlantı noktalarının yakınında çalışırken dikkatli olun. Kablo bağlantılarını keserken, yönelteciden uzak olan uçtaki bağlantıyı önce kesin.
- Elektrik şokundan kaçınmak için yönelteciye gücü Açıkken ya da ağ kabloları takılıyken, bir WAN arabirim kartını 2 yuvalı bir modüle yerleştirmeyin.
- Aşağıdaki prosedürlerden herhangi birini gerçekleştirirmeden önce, üzerinde çalışacağınız doğrultucunun DC gücünün Kapalı olduğundan emin olun. O doğrultucunun gücünün Kapalı olduğundan emin olmak için, doğrultucuya hizmet veren güç besleme panelinin ön tarafındaki akım kesiciyi bulun, anahtarı OFF konumuna getirin ve anahtarı OFF konumunda bantlayın.
- T1/E1 bağlantısı, kullanıcının teması açısından erişilemez bir voltaj kaynağı olarak düşünülmüştür. Herhangi bir genel telefon operatörü (PTO) tarafından sağlanan cihaz veya bağlantı donanımını kurcalamayın ya da açmayın. Herhangi bir sabit kablo bağlantısı (çıkarılamayan, yalnızca bir kez takılan fişler dışında) yalnızca PTO ekibi ya da uygun şekilde eğitim görmüş mühendisler tarafından yapılmalıdır.
- Kasayı açmadan önce, telefon-ağ voltajlarıyla temastan kaçınmak için, telefon-ağ kablolarının bağlantısını kesin.
- Yöneltecinin gücü Açık ya da Kapalı nasıl olursa olsun, BRI S/T, BRI U, CT1/PRI-CSU, CE1/PRI-B, CE1/PRI-U bağlantı noktalarında tehlikeli ağ voltajı bulunur. Elektrik şokundan kaçınmak için, bu bağlantı noktalarının yakınında çalışırken dikkatli olun. Kablo bağlantılarını keserken, yönelteciden uzak olan uçtaki bağlantıyı önce kesin.
- DC güç kaynağının kablolamasını tamamladıktan sonra, akım kesici anahtar tutamacından bandı kaldırın ve akım kesicinin tutamacını ON konumuna getirerek gücü yeniden sağlayın.
- Bu ürün, binanın kısa devre (aşırı akım) korumasının kurulmasına dayanır. Tüm akımı taşıyan iletkenlerde 60 VDC, 15A oranlarından daha büyük olmayan bir UL Listelenmiş ya da Sertifikalı sigorta veya akım kesici kullanıldığından emin olun.
- Resim, DC güç kaynağı uçbirim bloğunu gösterir. Gösterildiği gibi, kablolama ucunda uygun mandalları kullanarak ya da mandalsız şekilde, DC güç kaynağının kablolarını döşeyin. Düzgün kablolama dizisi, toprak toprağa, pozitif pozitive ve negatif negativedir. Toprak kablolarının her zaman en önce bağlanacağını ve en son kesileceğini unutmayın.
- Bükülü kablo kullanıldığında, kapalı döngü ya da yukarı çevrilmiş mandallı kürek tipi gibi onaylanan kablolama sonlandırıcıları kullanın. Bu sonlandırıcılar, kablolar için uygun boyutta olmalı ve yalıtıcıyla iletkenin her ikisini de sıkıştırmalıdır.
- Toprak iletkenini asla bozmayın ya da cihazı uygun olarak kurulmuş bir toprak iletkeni olmadan çalıştırmayın. Uygun topraklamanın olduğu konusunda şüphe duyuyorsanız, uygun elektrik inceleme yetkilisine ya da bir elektrikçiye başvurun.
- Bu birimi bir rafa monte ederken ya da servis verirken bedensel yaralanmaları önlemek için, sistemin dengeli durduğundan emin olmak amacıyla özel önlemler almalısınız. Aşağıdaki ana hatlar, güvenliğinizi garantilemek için sağlanmıştır:
 - ** Raftaki tek birimse, bu birim rafın en altına monte edilmelidir.
 - ** Bu birimin montajı rafı kısmen doldurduğunda, en ağır bileşen rafın en altında olacak şekilde, rafı aşağıdan yukarıya doğru yükleyin.
 - ** Rafta sabitleme aygıtları varsa, birimi rafa monte etmeden ya da birime servis vermeden önce, sabitleyicileri kurun.

BAKIM, ONARIM VE KULLANIMDA UYULMASI GEREKEN KURALLAR:

- Arıza durumumda lütfen Yetkili Servisi arayın. Birimi kurarken, toprak bağlantısı en önce yapılmalı ve en son kesilmelidir. Herhangi bir kapağı çıkarmadan önce, ana bilgisayarın kasasıyla güç kaynağının bağlantısını her zaman kesin.
- Herhangi bir kapağı çıkarmadan önce, ana bilgisayarın kasasının tüm analog devreleriyle ya da Temel Erişim ISDN'lerle (uygulandığı yerlerde) bağlantısını her zaman kesin. Doğrudan ya da diğer aparatlar yoluyla: "Güvenlik Uyarısı-Kullanım için yönergelere bakın" işaretli bağlantı noktalarıyla işaretli olan ya da olmayan bağlantı noktalarının kendi aralarında bağlanması, ağ üzerinde tehlikeli koşullar meydana getirebilir ve böyle bir bağlantı yapılmadan önce, yetkili bir mühendisten tavsiye alınmalıdır.

KULLANIM HATALARINA İLİŞKİN BİLGİLER:

- a) Sistemi güç kaynağına bağlamadan önce kurulum talimatlarını okuyunuz.
- b) Birim kurulurken toprak bağlantısı her zaman en önce yapıp en son çözülmelidir.
- c) Cihaz çalışırken bağlantı kabloları çözülmemelidir.
- d) Aşırı nemli, aşırı sıcak ve soğuk ortamlarda kullanmaktan kaçınınız.
- e) Bu veya bağlı ekipmanın genel amaçlı bir çıkışa yanlış bağlantılandırılması tehlikeli bir duruma sebebiyet verebilir.
- f) Cihazı sökmeden önce muhakkak güç anahtarından kapatınız. Cihazı yalnızca güç anahtarından açıp kapayınız. Cihazı amacı dışında kullanmayınız.

TAŞIMA VE NAKLİYE SIRASINDA UYULMASI GEREKEN KURALLAR:

- a) Araca indirme-bindirme ve taşıma sırasında maksimum dikkat gösterilmelidir.
- b) Araca yükleme sırasında ambalajın tamamen kapalı olduğundan ve hasar görmemiş olduğundan emin olunuz.
- c) Üst üste 10 koliden fazla istiflemeyiniz.
- d) Nakliye sırasında Uluslararası Nakliyeciler Birliği Tarafından açıklanan yönetmeliklere tamamen uyulmalıdır.
- e) Nakliye sırasında ortam sıcaklığı $-10^{\circ}/+80^{\circ}$ arasında bulunmalıdır.

TÜKETİCİNİN YAPABİLECEĞİ BAKIM-ONARIM VEYA ÜRÜNÜN TEMİZLİĞİNE İLİŞKİN BİLGİLER:

Güç ve Soğutma Sistemlerinin Sorunlarının Giderilmesi

Sorunu belirlemek için aşağıdakileri öğeleri kontrol edin:

*Güç anahtarı AÇIK (ON) konumundayken (I) ve güç LED lambası yanıyorken fanın işlediğinden emin olun. İşlemiyorsa fanı kontrol edin.

*Router kısa bir süre sonra kapanırsa, çevresel koşulları kontrol edin. Termal kaynaklı kapanmayla sonuçlanacak şekilde router fazla ısınmış olabilir. Sıcaklığın işletim sıcaklığı aralığında olduğundan emin olun.

*Router başlamazsa ancak güç LED lambası yanıyorsa, güç kaynağını kontrol edin.

*Router sürekli ya da arada sırada yeniden başlıyorsa, işlemci veya yazılımla ilgili bir sorun olabilir ya da DRAM SIMM'lerden biri düzgün takılmamış olabilir.

Bağlantı Noktaları, Kablolar ve Bağlantıların Sorunlarının Giderilmesi

Sorunu belirlemek için aşağıdakileri öğeleri kontrol edin:

*Router bir bağlantı noktasını algılamazsa, kablo bağlantısını kontrol edin.

*Güç anahtarı AÇIK (ON) konumundayken (I) güç LED lambasının yandığından emin olun.

Yanmıyorsa güç kaynağını ve güç kablosunu kontrol edin.

*Sistem başlıyorsa ancak konsol ekranı donmuşsa, konsolun ayarlarının 9600 baud, 8 veri biti, parite yok ve 2 durma biti olduğundan emin olun.

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, 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, aygıtle birlikte gelen basılı belgede bulunabilir.

TÜKETİCİNİN SEÇİMLİLİK HAKLARI

Malın ayıplı olduğunun anlaşılması durumunda tüketici, 6502 sayılı Tüketicinin Korunması Hakkında Kanununun 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 olmadığı, 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.

İTHALATCI FİRMA:

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

İMALATCI ADRESİ:

CISCO SYSTEMS, INC.

170 WEST TASMAN

DRIVE,

SAN JOSE, CA 95134-1706 USA

<http://www.cisco.com>

TEL: 408526-4000

800553-NETS (6387)

FAKS: 408526-4100

FirePOWER Hizmetleri Yetenekleri ve Kapasiteleri ile Cisco ASA 5506W-X

Özellik	FirePOWER Hizmetleri ile Cisco ASA 5506W-X	
Üretilen iş:	250 Mbps	
Uygulama Kontrolü (AVC)		
Üretilen iş:	125 Mb / sn	
Uygulama Kontrolü (AVC) ve IPS		
Maksimum eşzamanlı oturumlar	20.000; 50000 ¹	
Saniyede Maksimum Yeni Bağlantı Sayısı	5000	
Desteklenen uygulamalar	3.000'den fazla	
URL kategorileri	80+	
Kategorilenen URL sayısı	280 milyonun üstünde	
Merkezi yapılandırma, günlüğe kaydetme, izleme ve raporlama	Çok Aygıtlı Cisco Güvenlik Yöneticisi (CSM) ve Cisco Firepower Yönetim Merkezi	
Cihaz Üzerinde Yönetim	ASDM (sürüm 7.3 veya üstü gerekir)	ASDM

Özellik	FirePOWER Hizmetleri ile Cisco ASA 5506W-X	
Duruma dayalı denetim işlemi (maksimum ¹)	750 Mb / sn	
Duruma dayalı denetim işlemi (çok protokollü ²)	300 Mbps	
Üçlü Veri Şifreleme Standardı / Gelişmiş Şifreleme Standardı (3DES / AES) VPN çıktı ³	100 Mb / sn	
Kullanıcılar / düğümler	Sınırsız	
IPsec site-yerinde VPN eşleri	10; 50 ⁴	
Cisco AnyConnect Plus / Apex VPN maksimum eş zamanlı bağlantı ⁵	50 ⁵	
Sanal arabirimler (VLAN'lar)	5; 30 ⁴	
Güvenlik bağlamları ⁵ (dahil, maksimum)	N / A	
Yüksek kullanılabilirlik ⁴	Güvenlik Plus Lisansı gerektirir; Aktif/ Bekleme	

Tümleşik Kablosuz Erişim Noktası	N / A
(WiFi teknik ayrıntıları için bkz. Cisco AP 702 veri sayfası)	
Genişletme yuvası	N / A
Kullanıcı tarafından erişilebilen Flash	Yok hayır
USB 2.0 portları	USB portu tipi 'A', Yüksek Hız 2.0
Tümleşik G / Ç	8 x 1 Gigabit Ethernet (GE)
Genişletme G / Ç	N / A
Yönetim kapısı tahsisatı	Evet (FirePOWER Hizmetleri ile paylaşılmak üzere), 10/100/1000
Seri bağlantı noktaları	1 RJ-45 ve Mini USB konsolu
Katı hal sürücüsü	50 GB mSata 6
Bellek	4 CİGABAYT
Sistem flaşı	8 GB
Sistem veri yolu	Multibüs mimarisi

ÇALIŞMA PARAMETRELERİ

Sıcaklık	32 ila 104 ° F (0 ila 40 ° C)									
Bağıl nem	Yüzde 90 yoğuşmasız									
Rakım	0 ila 10.000 ft (3048 m) için tasarlanmış ve test edilmiştir									
Akustik	Fanless	Fanless	Fanless	41,6 A ağırlıklı desibel (dBA)	41,6 dBA tipi	64,2 dBA Maksimu m	64,2 dBA Maksimu m	64,2 dBA Maksimu m	67,9 dBA Maksimu m	67,9 dBA Maksimu m
Gürültü	0 dBA	0 dBA	0 dBA	67,2 dBA Maksimu m	67,2 dBA maksimum m					

ÇALIŞMAYAN PARAMETRELER

Sıcaklık ⁷	-13 ila 158°F (-25 ila 70°C)
Bağıl nem	Yoğunlaşmayan yüzde 10 ila 90
Rakım	0 ila 15.000 ft (4572 m) için tasarlanmış ve test edilmiştir

GÜÇ GİRİŞİ

AC menzil voltajı	Dış, 90 ila 240 volt alternatif akım (VAC)
AC normal hat voltajı	90 ila 240 VAC
AC akım	N / A
AC frekansı	50/60 Hz
Çift güç kaynakları	Yok
DC yerel hat voltajı	N / A
DC uluslararası hat voltajı	N / A
DC akımı	N / A

ÇIKTI

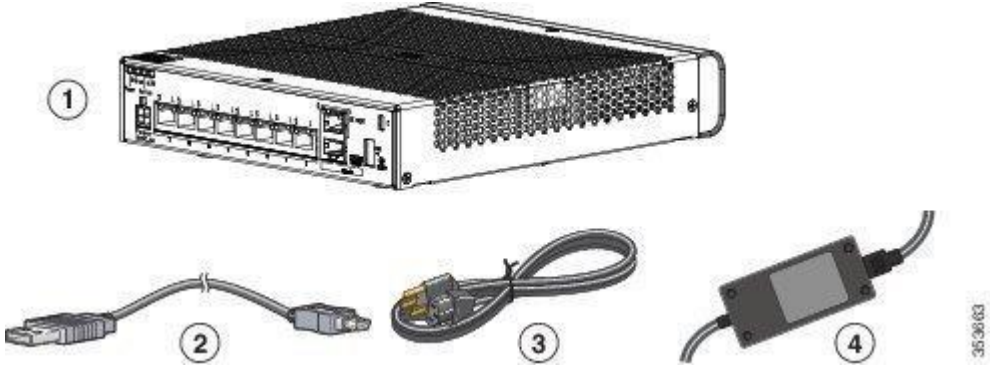
Denge durumu	12V @ 2.5A
Maksimum	
Tepe	12V @ 5A
Maksimum	
Isı dağılımı	103 İngiliz termik ünitesi (Btu) / saat
Form faktörü	Masaüstü, rafa monte edilebilir
Boyutlar	1,72 x 7,871 x 9,23 inç
(Y x G x D)	(4.369 x 19.992 x 23.444 cm)
Ağırlık (AC güç kaynağı ile)	4 lb (1.82 kg)

Cisco ASA5506W-XSerisi Hızlı Başlangıç Kılavuzu

1. Paket İçeriği

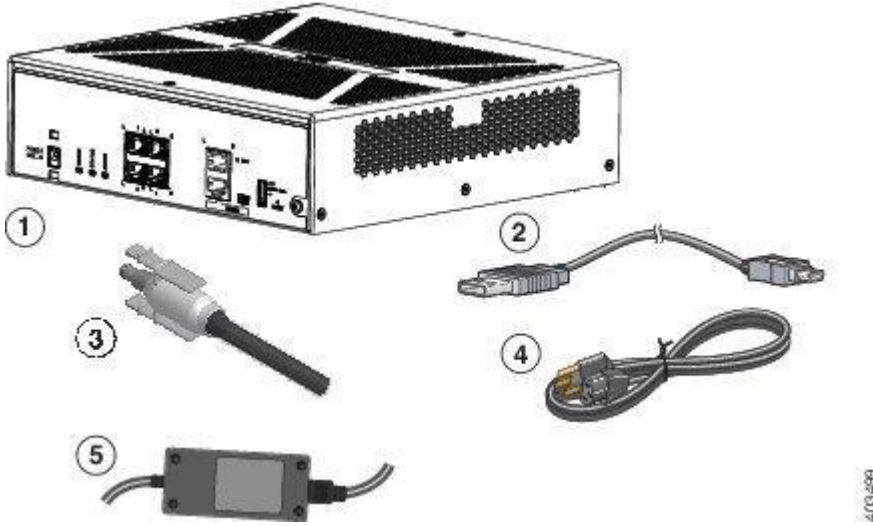
Bu bölüm, kasanın paket içeriğini listeler. İçeriğin değiştirilebileceğini ve tam içeriğinizin ek veya daha az öge içerebileceğini unutmayın.

ASA5506W-Xve 5506W-X



1	ASA5506W-Xveya ASA 5506W-X	2	USB Konsol Kablosu (Tip A'dan Tip B)
3	Güç kablosu	4	Güç kaynağı

ASA 5506H-X



1	ASA 5506W-Xşasi	2	USB Konsol Kablosu (Tip A'dan Tip B)
3	Güç kablosu tutma	4	Güç kablosu
5	Güç kaynağı		

2. Lisans Gereklilikleri

ASA Lisansları

ASA 5506W-X, sipariş ettiğiniz sürüme bağlı olarak **Base** veya **Security Plus** lisansını içerir. Ayrıca kullanıma uygunsa, Güçlü **Şifreleme (3DES / AES)** lisansı ile önceden kurulmuş olarak gelir. İsteğe bağlı olarak **AnyConnect Plus** veya **Apex** lisansı satın alabilirsiniz.

Elle Güçlü Şifreleme lisansını (ücretsiz) talep etmeniz gerekiyorsa, <http://www.cisco.com/go/license> adresini ziyaret edin .

Temel lisansından Security Plus lisansına yükseltmek veya bir AnyConnect lisansını satın almak istiyorsanız, bkz. <Http://www.cisco.com/go/ccw> . Ayrıca bkz. [Cisco AnyConnect Sipariş Kılavuzu](#) ve [AnyConnect Lisansı Sık Sorulan Sorular \(SSS\)](#) . Daha sonra, lisans etkinleştirme anahtarını edinebilmeniz için Ürün Yetkilendirme Anahtarı (PAK) içeren bir e-posta alacaksınız. AnyConnect lisansları için, aynı kullanıcı oturumları havuzunu kullanan birden çok ASA'ya uygulayabileceğiniz çoklu kullanımlı bir PAK alırsınız.

Not: Lisanslama için kullanılan seri numarası, donanımınızın dışında basılı olan şasi seri numarasından farklıdır. Şasi seri numarası teknik destek için kullanılır ancak lisanslama için değildir. Lisans seri numarasını görüntülemek için, **show version | grep Seri** komutu veya **ASDM Yapılandırması> Aygıt Yönetimi> Lisanslama Etkinleştirme Anahtarı** sayfasına bakın.

ASA FirePOWER Lisansları

ASA FirePOWER modülü ASA'dan ayrı bir lisanslama mekanizması kullanır. Lisans önceden yüklenmiş değildir, ancak kutuda, aşağıdaki lisanslar için bir lisans etkinleştirme anahtarı edinmenizi sağlayan bir çıktıda bir PAK bulunur:

- **Kontrol ve Koruma Kontrol** aynı zamanda "Uygulama Görünürlük ve Kontrol (AVC)" veya "Uygulamalar" olarak da bilinir. Koruma "IPS" olarak da bilinir. Bu lisanslar için etkinleştirme anahtarına ek olarak, bu özellikler için otomatik güncellemeler için "kullanım hakkı" aboneliklerine de ihtiyacınız vardır.

Kontrol (AVC) güncellemeler Cisco destek sözleşmesine dâhildir.

Koruma (IPS) güncellemeleriniz IPS abonelik satın gerektirir <http://www.cisco.com/go/ccw> .

Bu abonelik, Kuralı, Motor, Güvenlik Açığı ve Coğrafi Konum güncelleştirmelerini içermektedir. **Not:** Bu kullanım hakkı olan abonelik ASA FirePOWER modülü için bir PAK / lisans etkinleştirme anahtarı oluşturmaz veya bunları gerektirmez; yalnızca güncellemeleri kullanma hakkını sağlar. Satın alabileceğiniz diğer lisanslar şunları içerir:

- **Gelişmiş Malware Koruması (AMP)**
- **URL Filtreleme**

Bu lisanslar, ASA FirePOWER modülü için bir PAK / lisans etkinleştirme anahtarı üretir.

Daha fazla bilgi için [Cisco Firepower System Özellik Lisansı'na](#) bakın.

Denetim ve Koruma lisanslarını ve diğer isteğe bağlı lisansları yüklemek için [Lisansları Yükleme](#) konusuna bakın.

3. ASA 5506W-X Kablosuz Eriřim Noktası

ASA 5506W-X, ASA'ya entegre bir Cisco Aironet 702i kablosuz eriřim noktası içerir. Eriřim noktası, ASA'ya GigabitEthernet 1/9 arabirimi üzerinden dahili olarak baėlanır. Tüm wifi istemcileri GigabitEthernet 1/9 aėına aittir. ASA güvenlik politikası, wifi aėının diėer arabirimlerdeki tüm aėlara nasıl eriřebileceėini belirler. Eriřim noktası herhangi bir harici arabirim veya geçiř baėlantı noktası içermiyor.

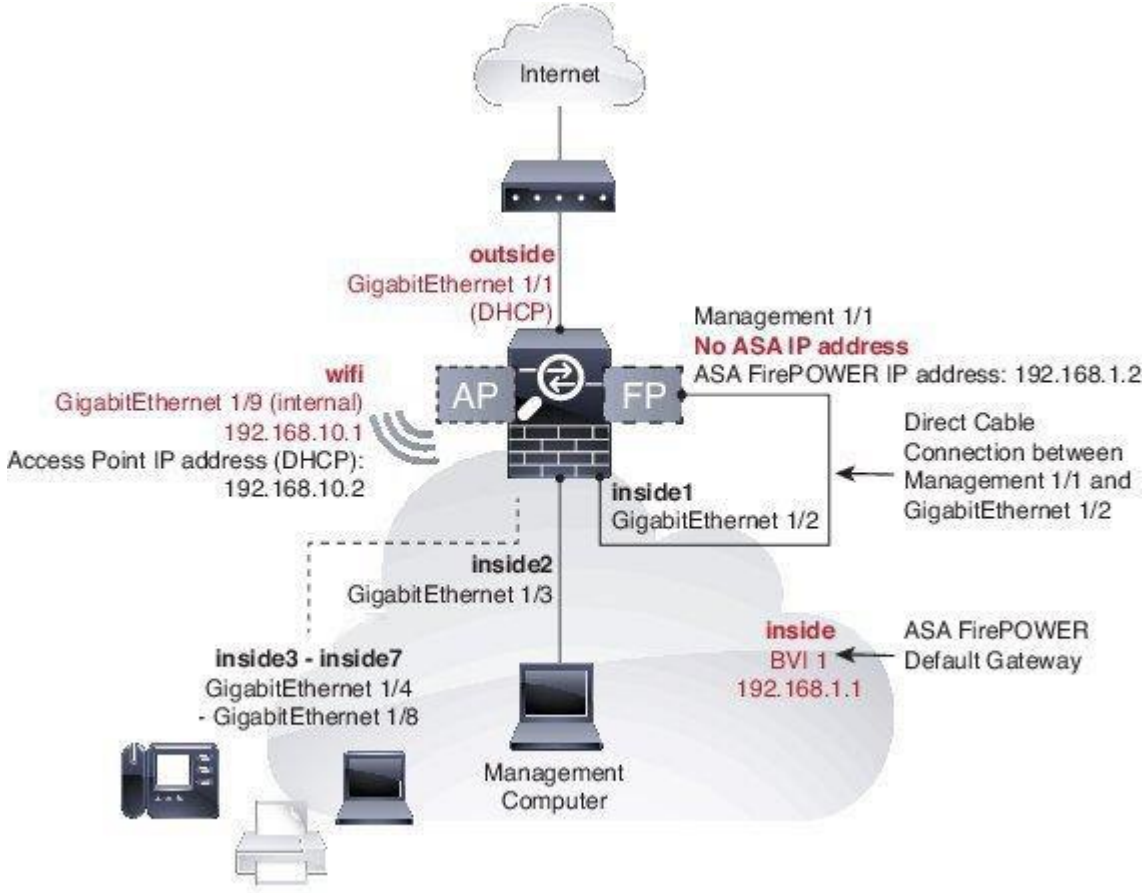
Eriřim noktası, baėımsız aygıt yönetimini mümkün kılan *özerk bir* Cisco IOS görüntüsünü içerir. ASA 5506W-X'i bir Cisco Birleřik Kablosuz Aėı'na eklemek ve bir kablosuz LAN denetleyicisi kullanmak istiyorsanız, hafif resmi yükleyebilirsiniz. Hafif resmin birleřik modda kullanılmasıyla ilgili daha fazla bilgi için Cisco Kablosuz Kontrol Yapılandırma Kılavuzu'ndaki Esnek Eriřim Noktalarını Hafif Moda Dönüřtürme bölümüne bakın.

- Desteklenen eriřim noktası yazılımı için bkz. Cisco ASA Uyumluluėu.
- Kablosuz LAN denetleyicisinin kullanılmasıyla ilgili ayrıntılar için Cisco Kablosuz LAN Denetleyicisi Yazılımı belgelerine bakın .
- Kablosuz eriřim noktası donanım ve yazılımı ile ilgili ayrıntılar için Cisco Aironet 700 Serisi belgelerine bakın .

4. ASA 5506W-X'i Aėınıza Daėıtın

ASA 9,7 ve Daha Sonra

Ařaėıdaki řekilde, ASA FirePOWER modülü ve dâhili kablosuz eriřim noktası (ASA 5506W-X) ile ASA5506W- Xiçin önerilen aė kurulumu gösterilmektedir. Bu daėıtım, harici ve wifi arabirimlerinin hepsini içeren bir iç köprü grubu içerir; böylece bu arabirimleri harici bir anahtara alternatif olarak kullanabilirsiniz.



Varsayılan yapılandırma, aşağıdaki davranışla yukarıdaki ağ dağıtımını etkinleştirir.

- GigabitEthernet 1/1 **dışında**, DHCP'den IP adresi **içinde** , 192.168.1.1'e (ASA 5506W-X için 1/4 ile GigabitEthernet 1/2) 1/8 elemanı arayüzleri üzerinden GigabitEthernet 1/2 köprü grubu
- (ASA 5506W-X) **wifi** GigabitEthernet 1/9, 192.168.10.1
- **iç** -> **dış** trafik akışı
- **iç** -> **içindeki** üye arayüzleri için trafik akışının
- (ASA 5506W-X) **wifi** <-> **iç** , **wifi** -> **dış** trafik akışı
- **DHCP** istemcileri için **dahili** ve **wifi** . Erişim noktası kendisi ve tüm istemcileri ASA'yı DHCP sunucusu olarak kullanmaktadır.

• **Yönetim 1/1 ASA FirePOWER modülüne** aittir. Arayüz Yukarı, *ancak aksi durumda ASA'da yapılandırılmamış*. Daha sonra ASA FirePOWER modülü, bu arabirimi, **ağdaki ASA'ya erişmek** ve iç arabirimi **İnternet geçidi** olarak kullanmak için kullanılabilir.

Not: Do not ASA yapılandırmasında Bu arabirim için bir IP adresi yapılandırın.

Yalnızca FirePOWER yapılandırmasında bir IP adresi yapılandırın. Sen olmalıdır

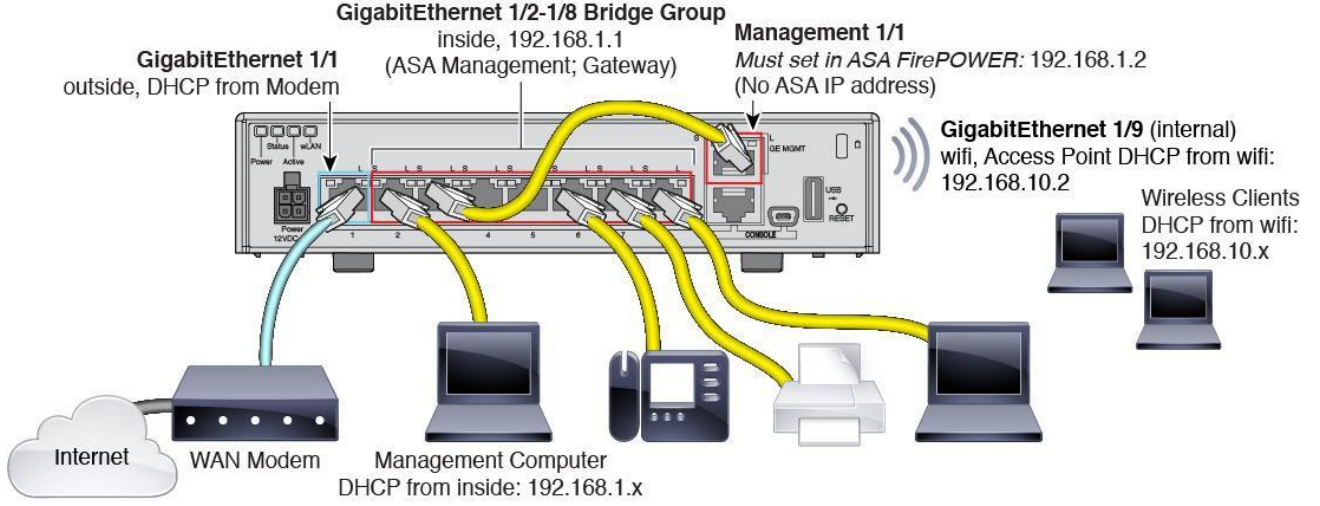
tamamen ASA ayrı olarak bu arabirimin düşünün yönlendirme açısından.

- **İç** arayüz ve **wifi** arayüzü üzerinde **ASDM erişimi**
- **NAT: İç**, kablosuz ve yönetim dışından gelen tüm trafik için Arayüz PAT'si.

Not: İç şebekede ayrı bir yönlendirici kurmak isterseniz, yönetim ile içeriden

gidebilirsiniz. Bu durumda, Management 1 / 1'de ASA ve ASA FirePOWER modüllerini uygun konfigürasyon değişiklikleri ile yönetebilirsiniz.

Prosedür



1. Kablo Yönetimini 1/1 (ASA FirePOWER modülü için) doğrudan aşağıdakilerden birine yapın: GigabitEthernet 1/2 through GigabitEthernet 1/8.

Not: Yönetim ağının yalnızca ASA FirePOWER modülüne ait olan ayrı bir aygıt gibi davranması nedeniyle içerde ve yönetim aynı ağda bağlanabilir.

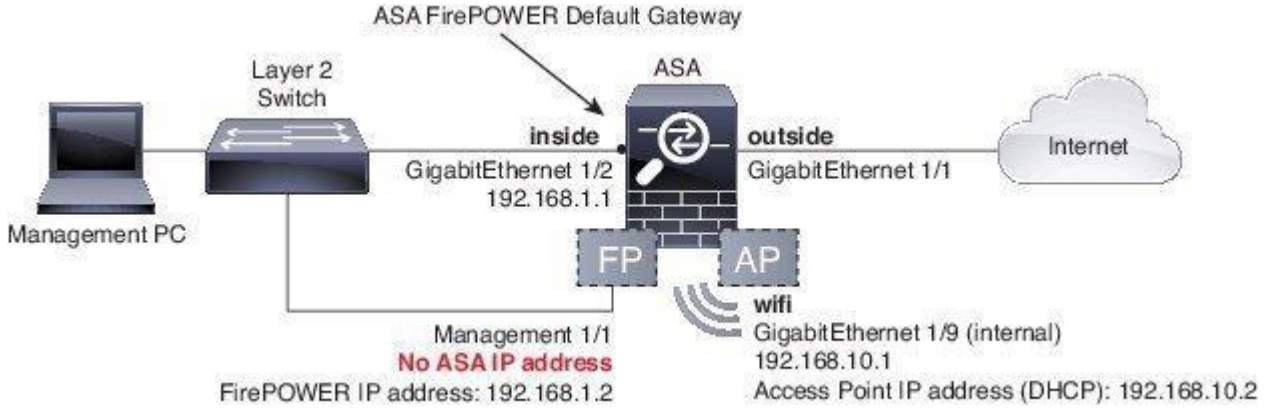
2. Bilgisayarınızı GigabitEthernet 1/2 ile GigabitEthernet 1/8 (ASA 5506W-X için GigabitEthernet 1/2 - 1/4) arasından birine bağlayın.

3. Kablo GigabitEthernet 1/1 (dış) WAN cihazınıza, örneğin kablo modeminize.

Not: Kablo modem 192.168.1.0/24 veya 192.168.10.0/24 üzerinde bir dış IP adresi sağlıyorsa, farklı bir IP adresi kullanmak için ASA yapılandırmasını değiştirmeniz gerekir. Arayüz IP adresleri, HTTPS (ASDM) erişimi ve DHCP sunucusu ayarları Başlangıç Sihirbazı kullanılarak değiştirilebilir. ASDM'ye bağlı olduğunuz IP adresini değiştirirseniz, sihirbazı tamamladığınızda bağlantı kesilirsiniz. Yeni IP adresine tekrar bağlanmalısınız.

ASA 9.6 ve Daha Önce

Aşağıdaki şekilde, ASA FirePOWER modülü ve yerleşik kablosuz erişim noktası (ASA 5506W-X) ile ASA5506W-X için önerilen ağ kurulumu gösterilmektedir:



Not: Dağıtımınızda ayrı bir dahili anahtar kullanmanız gerekir.

Varsayılan yapılandırma, aşağıdaki davranışla yukarıdaki ağ dağıtımını etkinleştirir.

- GigabitEthernet 1/1 **dışında**, DHCP'den IP adresi
- **İçeride** GigabitEthernet 1/2, 192.168.1.1
- (ASA 5506W-X) **wifi** GigabitEthernet 1/9, 192.168.10.1
- **iç** -> **dış** trafik akışı
- (ASA 5506W-X) **wifi** <-> **iç**, **wifi** -> **dış** trafik akışı
- **DHCP** istemcileri için **dahili** ve **wifi**. Erişim noktası kendisi ve tüm istemcileri ASA'yı DHCP sunucusu olarak kullanmaktadır.

• **Yönetim 1/1 ASA FirePOWER modülüne** aittir . Arayüz Yukarı, *ancak aksi durumda ASA'da yapılandırılmamış*. Daha sonra ASA FirePOWER modülü, bu arabirimi, **ağdaki ASA'ya erişmek** ve iç arabirimi **İnternet geçidi** olarak kullanmak için kullanabilir.

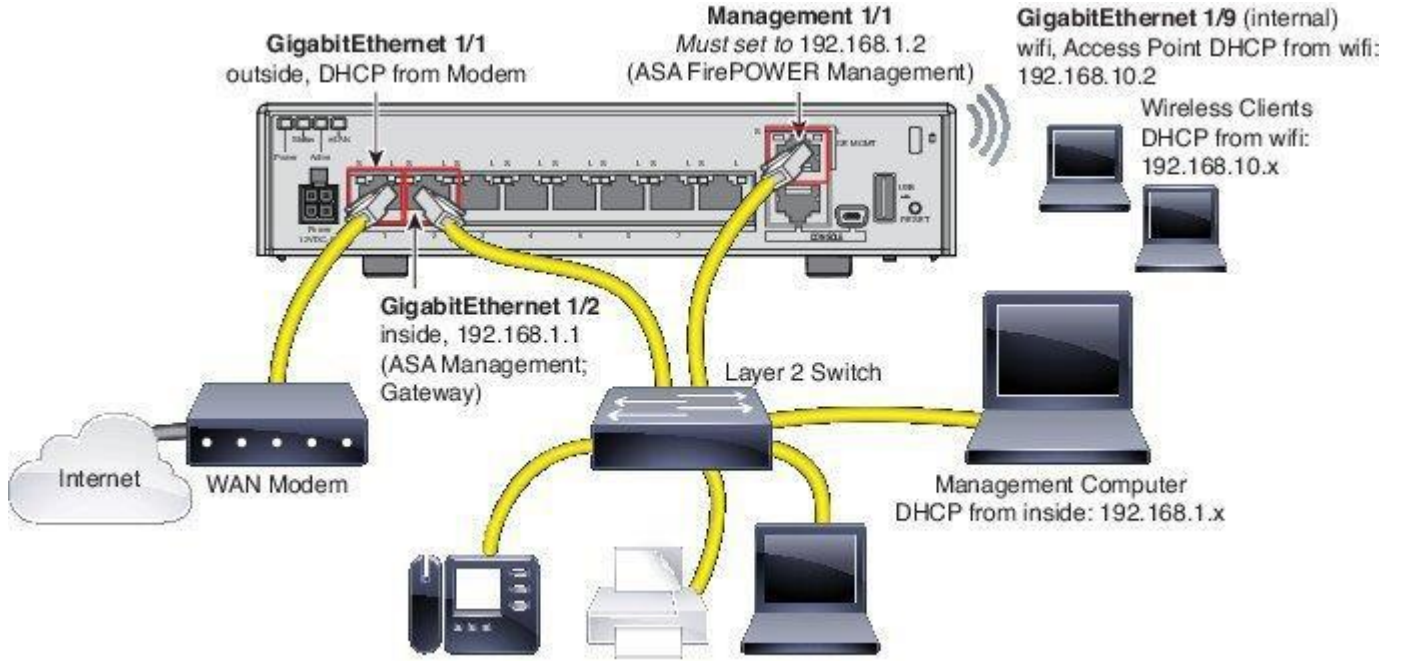
Not: Do not ASA yapılandırmasında Bu arabirim için bir IP adresi yapılandırın. Yalnızca FirePOWER yapılandırmasında bir IP adresi yapılandırın. Sen olmalıdır **tamamen ASA ayrı olarak bu arabirimin düşünün** yönlendirme açısından.

- **İç** arayüz ve **wifi** arayüzü üzerinde **ASDM erişimi**
- **NAT: İç**, kablosuz ve yönetim dışından gelen tüm trafik için Arayüz PAT'si.

Not: İç şebekede ayrı bir yönlendirici kurmak isterseniz, yönetim ile içeriden gidebilirsiniz.

Bu durumda, Management 1 / 1'de ASA ve ASA FirePOWER modüllerini uygun konfigürasyon değişiklikleri ile yönetebilirsiniz.

Prosedür



1. Aşağıdakileri Katman 2 Ethernet anahtarına bağlayın:

- Gigabit Ethernet 1/2 arabirimi (içeride)
- Yönetim 1/1 arabirimi (ASA FirePOWER modülü için)
- Bilgisayarınız

Not: Yönetim ağının yalnızca ASA FirePOWER modülüne ait olan ayrı bir aygıt gibi davranması nedeniyle içeride ve yönetim aynı ağda bağlanabilir.

2. Kablo GigabitEthernet 1/1 (dışarıda) WAN cihazınıza, örneğin kablo modeminize.

Not: Kablo modem 192.168.1.0/24 veya 192.168.10.0/24 üzerinde bir dış IP adresi sağlıyorsa, farklı bir IP adresi kullanmak için ASA yapılandırmasını değiştirmeniz gerekir. Arayüz IP adresleri, HTTPS (ASDM) erişimi ve DHCP sunucusu ayarları Başlangıç Sihirbazı kullanılarak değiştirilebilir. ASDM'ye bağlı olduğunuz IP adresini değiştirirseniz, sihirbazı tamamladığınızda bağlantı kesilirsiniz. Yeni IP adresine tekrar bağlanmalısınız.

5. ASA'yı Açın

1. Güç kablosunu ASA'ya takın ve bir elektrik prizine takın.
Güç kablosunu taktığınızda güç otomatik olarak açılır. Güç düğmesi yok.
2. ASA'nın arkasındaki Güç LEDini kontrol edin; Yeşilse cihaz açık durumda.
3. ASA'nın arkasındaki Durum LEDini kontrol edin; Yeşil yeşil olduktan sonra, sistem açılış teşhisini geçti.

6. Kablosuz Erişim Noktasını (ASA 5506W-X) etkinleştirin.

ASA 5506W-X kablosuz erişim noktası varsayılan olarak devre dışıdır. Erişim noktası GUI'sine bağlanın, böylece kablosuz radyoları etkinleştirebilir ve SSID ve güvenlik ayarlarını yapılandırabilirsiniz.

Sen başlamadan önce

Bu yol, varsayılan yapılandırmayı kullanmanızı gerektirir.

Prosedür

1. Ağın içindeki ASA'ya bağlı bilgisayarda, bir web tarayıcısı açın.
2. **Adres alanına girin <http://192.168.10.2>**. Kullanıcı adı ve şifre girmeniz istenir.
Not: Erişim noktasına erişemiyorsanız ve ASA varsayılan yapılandırmaya sahipse ve diğer ağ sorunları bulunmuyorsa, erişim noktası varsayılan yapılandırmasını geri yüklemek isteyebilirsiniz. ASA CLI'ye erişmeniz gerekir (ASA konsol bağlantı noktasına bağlanın veya ASDM kullanarak Telnet veya SSH erişimini yapılandırın). ASA CLI'den, **hw-module module wlan kurtarma yapılandırmasını girin**. Erişim noktasını daha da gidermeniz gerekiyorsa, **session wlan console** komutunu kullanarak erişim noktası CLI'ye bağlanın.
3. **Cisco kullanıcı** adını ve **Cisco** şifresini girin. Erişim noktası GUI görünür.
4. Sol tarafta, **Kolay Kurulum> Ağ Yapılandırması seçeneğini** tıklayın.
5. **Radyo Yapılandırma** alanı, her biri için **Radyo 2.4 GHz** ve **Radyo 5GHz** bölümleri, aşağıdaki parametreleri ayarlamak ve tıklayın **uygula** her bölüm için:
 - **SSID**
 - **Beacon'da SSID yayınlama**
 - **Evrensel Yönetici Modu: Devre dışı bırak**
 - **Güvenlik** (seçtiğiniz)
6. Sol tarafta **Özet'i** tıklatın ve ana sayfadaki **Ağ Arayüzleri** altından 2.4 GHz radyo için hotlink'i tıklatın.
7. **Ayarlar** sekmesi tıklayın.
8. İçin **Etkin Radyo** ayarı, tıklayın **Enable** radyo düğmesini ve ardından **Uygula** sayfanın alt kısmında.
9. 5 GHz telsizi tekrarlayın.
10. Daha fazla bilgi için aşağıdaki el kitaplarına bakın:
 - Kablosuz LAN denetleyicisinin kullanılmasıyla ilgili ayrıntılar için bkz. [Cisco Kablosuz LAN Denetleyicisi Yazılımı belgeleri](#).
 - Kablosuz erişim noktası donanımı ve yazılımı hakkında ayrıntılı bilgi için [Cisco Aironet 700 Serisi belgelerine bakın](#).

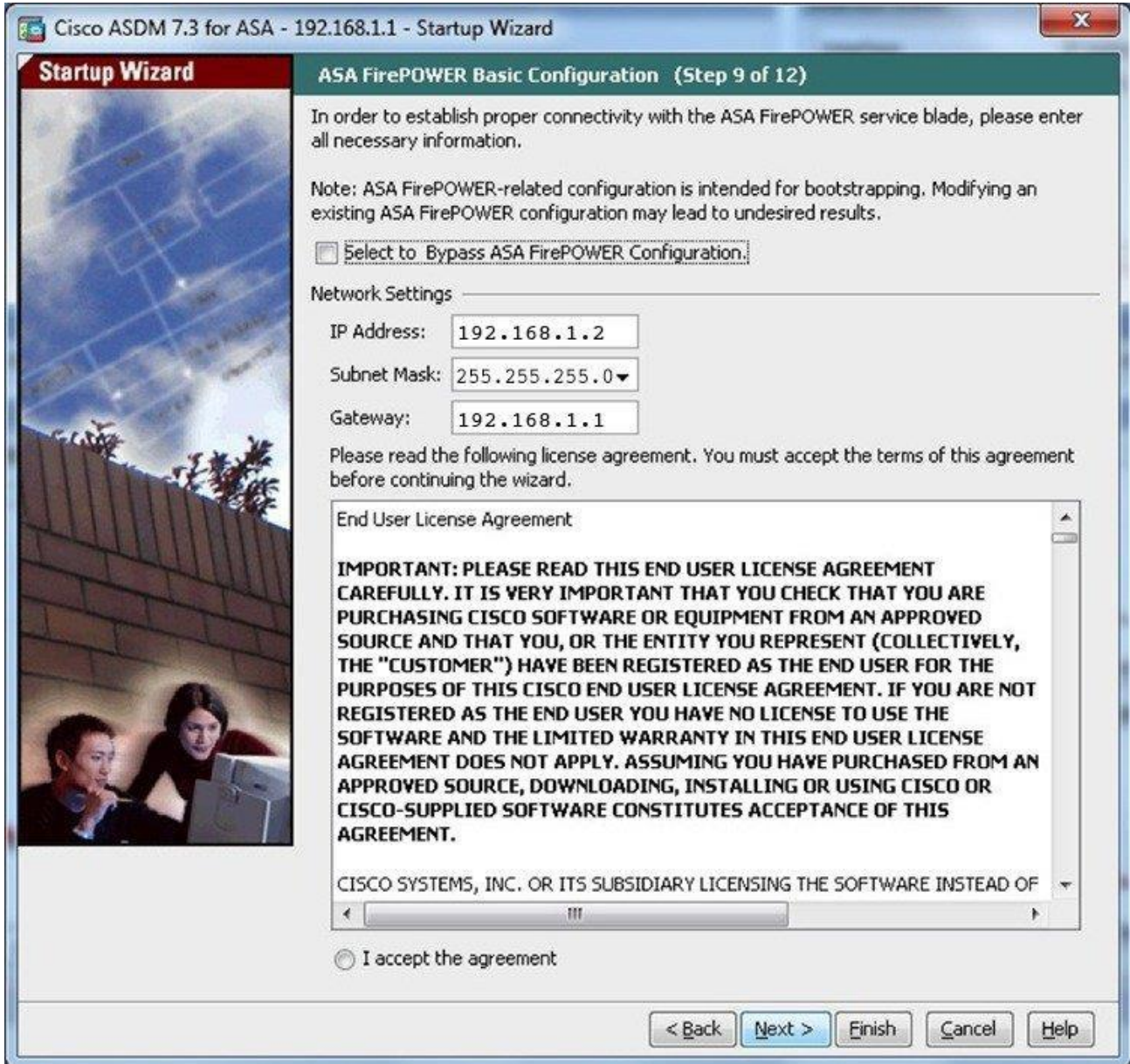
7. ASDM'yi başlatın

[ASDM'yi çalıştırmak için gereksinimler için Cisco.com'daki ASDM sürüm notlarına bakın](#) .

Bu prosedür ASA FirePOWER Modülünü yönetmek için ASDM'yi kullanmak istediğinizi varsaymaktadır. Firepower Management Center'ı kullanmak istiyorsanız, modül CLI'ye bağlanmanız ve kurulum komut dosyasını çalıştırmanız gerekir; bkz [ASA Firepower hızlı başlangıç kılavuzu](#).

Prosedür

1. ASA'ya bağlı bilgisayarda bir web tarayıcısı açın.
2. Adres alanına aşağıdaki URL'yi girin: <https://192.168.1.1/admin>. **Cisco ASDM** web sayfası açılır. Yönetim bilgisayarınızı bir kablosuz istemci olarak ASA'ya bağladıysanız, <https://192.168.10.1/admin> adresinden ASDM'ye erişebilirsiniz.
3. Mevcut seçeneklerden birini tıklayın: **ASDM Launcher yükleyin, ASDM on veya Çalıştır Başlatma Sihirbazı çalıştırın**
4. Seçtiğiniz seçeneğe göre ASDM'yi başlatmak için ekrandaki yönergeleri izleyin. **Cisco ASDM-IDM Launcher** görünür.
ASDM Başlatıcıyı Kur'u tıkladıysanız, bazı durumlarda ASA için bir kimlik sertifikası ve ASDM için Bir Kimlik Belgesi Takma göre ASA FirePOWER modülü için ayrı bir sertifika yüklemeniz gerekir.
5. Kullanıcı adı ve parola alanlarını boş bırakın ve Tamam'ı **tıklatın**. Ana ASDM penceresi görüntülenir.
6. Yüklü ASA FirePOWER modülünün IP adresini girmeniz istenirse, iletişim kutusunu iptal edin. İlk önce Başlangıç Sihirbazını kullanarak modül IP adresini doğru IP adresine ayarlamanız gerekir.
ASDM, ASA arka paneli üzerinden ASA FirePOWER modülünün IP adres ayarlarını değiştirebilir; ancak ASDM modülü daha sonra yönetmek için ASDM, modülüne (ve yeni IP adresine) Yönetim 1/1 ara yüzünde ağ üzerinden erişebilmelidir. Önerilen dağıtım, modül IP adresi iç ağda olduğu için bu erişimi sağlar. ASDM, IP adresini ayarladıktan sonra modülde erişemiyorsa, bir hata göreceksiniz.
7. **Sihirbazlar> Başlangıç Sihirbazını** seçin.
8. İsteddiğiniz şekilde ek ASA ayarlarını yapılandırın veya **ASA FirePOWER Temel Yapılandırma** ekranına gelene kadar ekranları atlayın.



Varsayılan yapılandırmayla çalışmak için aşağıdaki değerleri ayarlayın:

- **IP Adresi** -192.168.1.2
- **Alt Ağ Maskesi** -255.255.255.0
- **Ağ geçidi** -192.168.1.1

9. Anlaşmayı kabul ediyorum'u tıkladıktan sonra sihirbazı tamamlamak için İleri'yi veya Son'u tıkladın.
10. ASDM'den çıkın ve ardından yeniden başlatın. Giriş sayfasında **ASA FirePOWER** sekmelerini görmelisiniz.

8. Diğer ASDM Sihirbazlarını ve Gelişmiş Yapılandırmayı Çalıştırın

ASDM, güvenlik ilkenizi yapılandırmak için birçok sihirbaz içerir. Mevcut tüm sihirbazlar için **Sihirbazlar** menüsüne bakın.

ASA'nızı yapılandırmaya devam etmek için [Cisco ASA Series Dokümantasyonunda Seyrüsefer'deki yazılım sürümü için mevcut dokümanlara bakın.](#)

9.ASA FirePOWER Modülünü Yapılandırma

Lisansları yüklemek, modül güvenlik ilkesini yapılandırmak ve modüle trafik göndermek için ASDM'yi kullanın.

Not: Alternatif olarak, ASA FirePOWER modülünü yönetmek için FirePOWER Management Center'ı kullanabilirsiniz. Daha fazla bilgi için [ASA FirePOWER Modülü Hızlı Başlangıç Kılavuzu'na](#) bakın.

Lisansları Yükle

Kontrol ve koruma lisansları varsayılan olarak sağlanır ve kutunuzdaki bir çıktıya Ürün Yetkilendirme Anahtarı (PAK) dâhil edilir. Ek lisanslar sipariş ettiyseniz, e-postanızdaki bu lisanslar için PAK'lara sahip olmanız gerekir.

1. Yapılandırma> ASA FirePOWER Yapılandırması> Lisanslar'ı seçip Yeni Lisans Ekle'yi tıklatarak kasanız

için Lisans Anahtarı edinin.

Lisans Anahtarı en üstte; örneğin, 72: 78: DA: 6E: D9: 93: 35.

2. Lisans portalını başlatmak için Lisans Al'ı tıklatın.

Alternatif olarak, tarayıcınızda

<http://www.cisco.com/go/license> adresine gidin .

3. Yeni Lisans Al alanına virgülle ayrılmış PAK'ları girin ve Tamamla'yı tıklatın.

4. Diğer alanların arasında Lisans Anahtarı ve e-posta adresi istenir.

5. Ortaya çıkan lisans etkinleştirme anahtarını, web sitesi ekranından veya sistemin otomatik olarak gönderdiği lisans e-postasına eklenmiş zip dosyasından kopyalayın.

6. ASDM Yapılandırması> ASA FirePOWER Yapılandırması> Lisanslar> Yeni Lisans Ekle ekranına geri dönün.

7. Lisans etkinleştirme anahtarını Lisans kutusuna yapıştırın.

8. Metni doğru şekilde kopyaladığınızdan emin olmak için Lisansı Doğrula'yı ve ardından doğrulamadan sonra Lisansı Gönder'i tıklayın.Lisans Sayfasına Geri Dön düğmesini tıklatın.

ASA FirePOWER Güvenlik İlkesini yapılandırma

1. ASA FirePOWER güvenlik ilkesini yapılandırmak için Yapılandırma> ASA FirePOWER Yapılandırmasını seçin.

Bilgi için ASDM'deki ASA FirePOWER sayfalarını kullanın. Herhangi bir sayfadaki Yardım'ı tıklatabilir veya ilkeleri yapılandırmayla ilgili daha fazla bilgi edinmek için Yardım> ASA FirePOWER Yardım Konularını seçebilirsiniz.

Ayrıca bkz. [ASA FirePOWER modülü yapılandırma kılavuzu](#).

ASA Güvenlik İlkesini Yapılandırma

1. Modüle trafik göndermek için Yapılandırma> Güvenlik Duvarı> Hizmet İlkesi Kurallarını seçin.

2. Ekle> Hizmet İlkesi Kuralı Ekle'yi seçin.

3. Belirli bir arabirime ilkeyi uygulamak veya küresel uygulamak ve tıklamayı seçin **İleri**.
4. Trafığı eşleştirmeyi yapılandırın. Örneğin, **herhangi bir Trafığı** eşleştirebilir, böylece gelen erişim kurallarınızdan geçen tüm trafik modüle yönlendirilir. Veya limanlar, ACL (kaynak ve hedef ölçütleri) veya mevcut bir trafik sınıfına dayalı daha katı ölçütler tanımlayabilirsiniz. Diğer seçenekler bu politika için daha az kullanışlıdır. Eğer trafik sınıfı tanımını tamamladıktan sonra tıklayın **İleri**.
5. Kural Eylemleri sayfasında **ASA FirePOWER İnceleme** sekmesini tıklayın.
6. Kontrol **Bu trafik akışı için ASA ateş gücünü etkinleştirme** onay kutusunu.
7. Yılında ise **ASA FirePOWER Kart Başarısız** alanı, aşağıdakilerden birini tıklayın:
 - **İzin trafiği** - Modül kullanılmıyorsa ASA'yı tüm trafiğe izin vermek için, beklenmedik şekilde ayarlar.
 - **Trafığı kapat** -A modülü kullanılmıyorsa, tüm trafiği engellemek için ASA'yı ayarlayın.
8. (İsteğe bağlı) Modüle trafik için yalnızca salt okunur bir kopyasını göndermek için **Monitörü yalnızca** kontrol edin, örn. Pasif mod.
9. **Son'u** ve ardından **Uygula'yı** tıklayın.

KURULU M

Kurulumun Nasıl Yapılacağını Gösterir Bağlantı Şeması ile Bağlantı ve Kurulum ile İlk Çalıştırılmasının Kimler Tarafından Yapılması (Kullanıcı, Teknik Servis) Gerektiğine İlişkin Bilgiler:

Esnek Konuşlandırma

Mevcut birçok çeşitli grupta BLKR teknolojilerinin parçası olarak Cisco ASA5506W-X Güvenlik Duvarları IPv4 ve IPv6 çeşitli ağ ortamlarında konuşlandırılabilir.

ASA5506W-X içerisindeki geniş oranda performans ve arayüz konfigürasyonları ayrıt, kampüs (yerleşke) ve veri merkezi boyunca etkili izinsiz girişi önleme ile paralel olmayan esnekliği başarmanıza imkân tanımaktadır (olanaklı kılmaktadır).

enable you to achieve effective izinsiz girişi önleme ile unparalleled flexibility throughout the ayrıt, campus, and veri merkez.

- Cisco ASA5506W-X Güvenlik Duvarları içine katılmış bir BLKR konfigürasyonunda sık değişen bir IDS konfigürasyonu, veya hem içindeki hem de değişken eş zamanlı olarak konuşlandırılabilir.

- IPv4 ve IPv6 ağları üzerinde kritik varlıklarınız maksimum konuşlandırma esnekliği ve daha düşük mülkiyet maliyeti için tek bir adet Cisco ASA5506W-X Güvenlik Duvarları ile korunmaktadır.

Cisco ASA5506W-X Güvenlik duvarları IPv6 veya hibrid IPv4 ve IPv6 ağlarına aktarma (sistemi geçirmeyi) düşünen veya planlayan müşteriler için yatırım koruma sağlamaktadır.

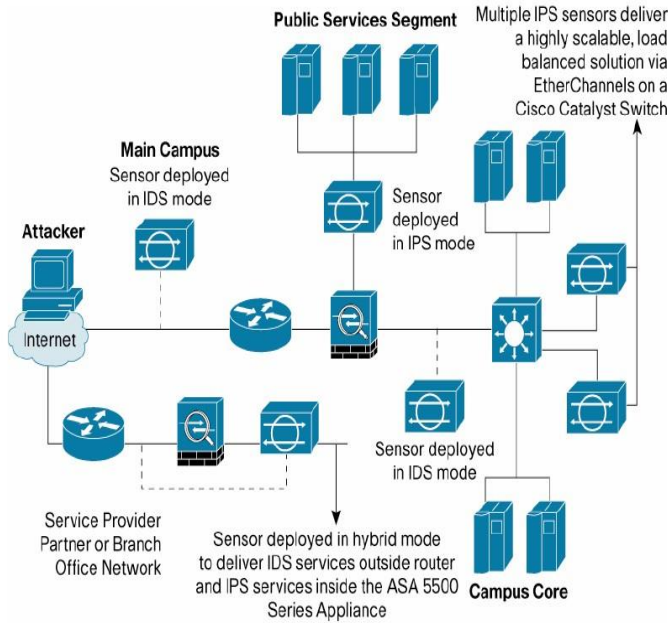
- Erişim aygıtları in the Cisco ASA5506W-X içerisindeki erişim aygıtları bakır tel ve fiber Gigabit Ethernet, ve 10 Gigabit Ethernet arayüzleri teknik özelliklerine sahip çeşitli çoklu-arayüz konfigürasyonlarında mevcuttur.

Aynı zamanda mantıksal (lojik) yapılandırabilirsiniz ve kolaydan karmaşığa kadar bütün konuşlandırma gereksinimlerinize cevap vermek üzere esnekliği tasarlamınıza izin vererek sizin VLAN ortamınızla izinsiz girişi önlemenizi gerçekleştirmektedir.

- Cisco BLKR teknolojileri sanal güvenlik duvarlarıyla aynı zamanda hem konfigürasyon hem de güvenlik duvarı durumunu sanallaştırmanızı olanaklı kılan endüstri-öncü sanallaştırma teknik özelliklerine sahiptir.

Şekil 1 de gösterildiği üzere güvenlik duvarları bilgisayar kurtlarını ve virüslerin etkin bir biçimde durdurmak üzere güvenlik görünürlüğünün gerekli olduğu hemen hemen bütün kuruluşlardaki ağ dilimlerinde (segmentlerinde) yer alabilmektedir.

Şekil 1. Cisco ASA5506W-X Güvenlik duvarları için Konuşlandırma Senaryoları



Dağıtım Performansı

Cisco ASA5506W-X Güvenlik duvarları, uygulamalar ve ağ kullanımının geniş ölçüdeki zorluklarını karşılamak üzere tasarlanmıştır. Günümüzdeki işletmelerde uygulamalar daha önce olmadığı biçimde interneti kullanmaktadır.

IP üzerinden Ses, e-ticaret, duraksız video iletimi ve Web 2.0 daha yüksek verimlilik ve çalışanların işbirliğini olanaklı kılmaktadır.

Bu ağa bağlı uygulamalar bağlantı hızları, aynı zamanda oluşan bağlantılar, akış uzunluğu ve hareket ölçüsü vesaire gibi kaynaklarda farklı ortaya çıkmaktadır ve talepleri değişmektedir.

Bir performans perspektifinden seri-ateş, hafif ağırlıktaki bağlantılarla belirli bir yere yerleştirilen yüksek derecede ticari ortamlarda belli bir noktada birleşen içerik özelliğine sahip ortam zengin özellikleri değişen uygulama spektrum türleri vardır.

Cisco BLKR teknolojisi hem “ortam-zengin” ve hem de “ticari” ortamlarda çeşitli metrik sistem gruplarında değerlendirmekte olup,

Sizin gerçek-dünya ortamınızdaki benzersiz özelliklere dayalı olarak tam ve gerçek BLKR performansı beklemenize imkân vermektedir.

Medya-Zengin

Medya-zengin ortamlar içerik (kapsam) tarafından nitelendirilmektedir. Popüler web sitelerin çoğunda görülene içerik video içeriği ve dosya transferlerini yaptığı şekilde spektrumun ortam zengin ucuna rastlamaktadır. Eğer ortamınız geniş miktarlardaki ortam veri ve birleşik, üç boyutlu olaylara erişimle yönlendiriliyorsa ortamınız medya açısından daha zengin bir ortamdır.

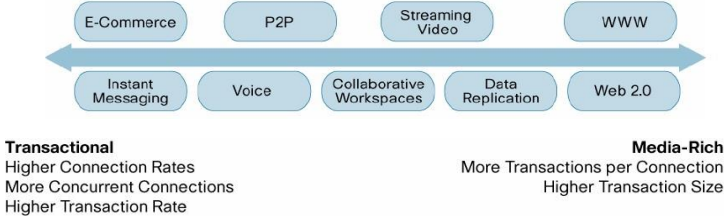
Ticari

Ticari ortamlar bağlantılarla tanımlanmaktadır.

E-ticaret ortam biçimlerinin birçoğu acil mesajlaşma ve seste olabildiği gibi spektrum sonuna rastlamaktadır. Eğer ortam bağlantı-yoğun uygulamalar ve küçük hareket ölçüleriyle yürütülüyorsa sizin ortamınız daha ticari olmaktadır.

Şekil 2 medya-zengin ve ticariler arasındaki spektrumu göstermektedir.

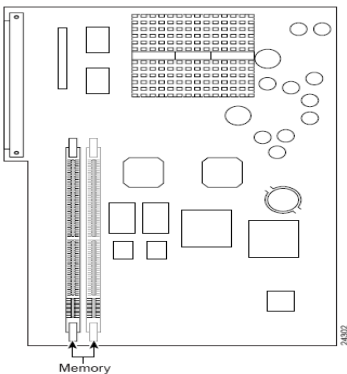
Şekil 2. Network Ortam Spektrumu: Ticari ile Medya-Zengin



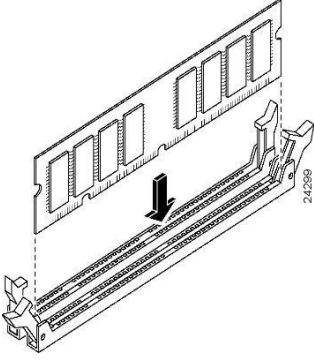
Gerekli Araçlar ve Ekipman:

Sıradan bir router kurulumu için aşağıdaki araçlar ve parçalar gereklidir:

- *2 numara PhillBLKR tornavida
- *düz uçlu tornavidalar: küçük (0.476 cm) ve orta (0.625 cm)
- *Elektrostatik boşalma önleyici bilezik.
- *Rafların dirseklerini router'a sabitlemek için vidalar.
- *WAN ve LAN bağlantı noktalarına bağlantı için kablolar (yapılandırmaya göre):
- *Bir Ethernet bağlantı noktasına bağlantı için Ethernet 10BaseT kablosu (dâhildir).
- *Bir Fast Ethernet bağlantı noktasına bağlantı için Ethernet 10/100BaseT kablosu (dâhildir).
- *Token Ring bağlantı noktası için bir Token Ring lob kablosu
- *Ethernet (LAN) bağlantı noktalarına bağlantı için Ethernet 10BaseT Hub ya da bir ağ arabirim kartına sahip PC.
- *9600 baud, 8 veri biti, parite yok ve 2 durma biti için yapılandırılmış konsol uçbirimi (bir ASCII uçbirimi ya da öykünme programını çalıştıran bir PC uçbirimi). Otomatik Kurulum prosedürünü kullanmıyorsanız bir uçbirim gerekir.
- *İsteğe bağlı) Uzak yönetim erişimi amacıyla yardımcı bağlantı noktasına yapılacak bağlantı için



modem.



Çabuk Kurulum Kartı: Windows NT Sunucusu için CiscoGüvenli BLKR 2,4.

Not: İlk Önce Beni Oku üzerindeki talimatları daha önceden takip ettiğinizden emin olunuz: Windows NT Sunucu Temin edilen Çalıştırılan kart için CiscoGüvenli BLKR 2.4.

! Uyarı: Eğer kurulan CiscoGüvenli BLKRnin önceki versiyonuna sahipseniz, yeni versiyonu kurmadan önce verinizi diğer makinaya yedekleyiniz Kurulum ile herhangi bir probleminiz varsa, benioku dosyasında veya sürüm notlarında ve tekrar-çalıştır kurulumda tanımlanan CiscoGüvenli BLKR CD-ROM üzerinde kurulu Clean.exe dosyasını çalıştırınız.

Yazılımın Kurulumu

Not: Kurulumu çalıştırmadan önce bütün Windows programlarını kapatınız.

1. Üzerinde CiscoGüvenli BLKRYi kurduğunuz makinaya yerel sistem yöneticisi olarak giriş yapınız.

Not: Mevcut uzaktan erişim yöneticisine yöneticinin kontrol hakkı verildiği müddetçe yeni bir uzaktan erişim yöneticisi uzaktan yakından oluşturulabilmektedir.

2. CiscoGüvenli BLKR CD-ROMunu sizin CD-ROM sürücünüze yerleştiriniz. Kurulum pencereleri açılmaktadır.

3. **Install**'e tıklayınız. Yazılım Lisans Anlaşma Penceresi açılır.

4. Yazılım Lisans Anlaşmasını okuyunuz; lisanslama şartlarını ve koşullarını kabul etmek için **Accepti** tıklayınız. Hoş geldiniz penceresi açılır.

5. **Nexti** tıklayınız. Başlamadan Önce pencere açılır.

6. Karşılaman her bir koşulu doğrulayınız, sonra her bir parça için kontrol kutusunu tıklayınız. **Nexti** tıklayınız. (Listelenen parçalar hakkında daha fazla bilgi için **Explain**'e tıklayınız. Eğer herhangi bir koşul karşılanmıyorsa Kurulumdan çıkmak için **Canceli** tıklayınız.) Eğer bu yeni bir kurulum ise Adım9'a geçiniz.

7. (Seçmeli) Eğer CiscoGüvenli BLKR daha önceden kurulu ise, Önceki Kurulum Penceresi açılmaktadır. Önceki versiyonu silmek isteyip istemediğinizi Kurulum sorar ve mevcut veritabanı bilgisini saklar. Mevcut veriyi saklamak için şuna tıklayınız:

Yes, keep existing veribase

Yeni bir veritabanı kullanmak için kontrol kutusunu temizleyiniz.

Next'e tıklayınız. Kontrol kutusunu kontrol ettiyseniz, Kurulum mevcut konfigürasyonu yedekler. Kurulum eski dosyaları siler. Dosyalar silindiğinde **OK**'e tıklayınız.

8. Eğer Kurulum mevcut bir konfigürasyon bulduğunda, konfigürasyonu getirtmek isteyip istemediğinizi sorar.

Mevcut konfigürasyonu saklamak için şuna tıklayınız:

.Yes, import konfigürasyon

Yeni bir konfigürasyon kullanmak için, kontrol kutusunu temizleyiniz.

Next'e tıklayınız.

9. Destinasyon Lokasyon Seçimi penceresi açılır.

Varsayılan dizindeki yazılımı kurmak için **Next**'e tıklayınız. Farklı bir dizin kullanmak için **Browse**'a tıklayınız ve kullanacağınız dizini giriniz.

Eğer dizin mevcut değilse kurulum size dizini oluşturmak isteyip istemediğinizi sorar. **Yes**'e tıklayınız. *Kimlik kanıtlama Veritabanı Konfigürasyon* penceresi açılmaktadır.

10. Click the seçenek button(s) for the kimlik kanıtlama veritabanı(s) to be used by CiscoGüvenli tarafından kullanılacak kimlik kanıtlama veritabanı(ları) için seçenek düğme(ler)ini tıklayınız:

Check the CiscoSecure BLKR Veribase only (default)

Also check the Windows NT User Veribase

Eğer birinci seçeneği seçerseniz kimlik kanıtlama için sadece CiscoGüvenli BLKR veritabanını kullanacaktır; eğer ikinci seçeneği seçerseniz CiscoGüvenli BLKR her iki veritabanını da kontrol edecektir.

11. (Seçmeli) Windows NT Kullanıcı Yöneticisinde açıkça belirtildiniz sadece şu kullanıcıların çeviri erişimi kısıtlamak için şuna tıklayınız:

Yes, reference "Grant dialing permission to user"

setting Next'e tıklayınız. Ağ Erişim Sunucu Detayları

penceresi açılır.

12. Şu bilgiyi tamamlayınız. (*Before You Start: CiscoSecure BLKR 2.4 for Windows NT Sunucu Getting Started* çabuk başvuru kartını gözden geçiriniz.)

Kullanılan Doğrulama Kullanıcıları—Güvenlik protokolü tipi kullanılacaktır. TACBLKR+ (Cisco) varsayılmaktadır.

Erişim Sunucu İsmi—NASın ismi CiscoSecure BLKR servisleri için kullanılıyor olacaktır. **Erişim Sunucu IP Adresi**—NASın IP adresi CiscoSecure BLKR servisleri kullanılıyor olacaktır. **Windows NT Sunucu IP Adresi**—Bu Windows NT sunucusunun IP adresidir.

TACBLKR+ veya RADIUS Anahtarı—NAS ve CiscoSecure BLKRinin ortak gizli anahtarı. Bu şifreler NAS ve CiscoGüvenli BLKR arasındaki düzgün fonksiyon ve iletişimi sağlamak için aynı olmalıdır. Ortak gizli anahtarlar büyük ve küçük harfe duyarlıdır. Kurulum CiscoSecure BLKR dosyalarını düzenlemektedir ve Sistem Kütüğünü güncellemektedir.

13. **Next**'e tıklayınız. Arayüz Konfigürasyon penceresi açılmaktadır. Arayüz Konfigürasyon seçenekleri etkisiz kılınmaktadır. Listelenen seçeneklerin tümü veya herhangi bir kontrol kutusunu tıklayınız.

Not: Bu parçaların konfigürasyon seçenekleri eğer sadece seçilir kılınmış ise CiscoSecure BLKRde gösterilmektedir. Arayüz Konfigürasyonundaki bu ve ilave seçeneklerin tümünü veya herhangi birini seçilir kılabilir veya seçilemez kılabilirsiniz.: Gelişmiş Seçenekler penceresi.

14. **Next**'e tıklayınız. Aktif Servis Gözetim penceresi açılır. CiscoSecure BLKR gözetim servisi olan CSMon'u seçilir kılmak için, **Enable Log-in Gözetim** kontrol kutusunu kontrol ediniz ve daha sonra giriş süreci testi geçemediğinde yürütmek için betiği seçiniz:

Düzeltilici Faaliyet Yok—CiscoSecure BLKR çalışırken olduğu gibi bırakınız.

Sistemi yeniden başlatma—Çalışan CiscoGüvenli BLKR üzerindeki sistemi yeniden başlatın.

Hepsini Tekrar Başlatma—(varsayılan) Tüm CiscoGüvenli BLKR servislerini tekrar başlatınız.

RADIUS/TACBLKR+ Protokolünü Tekrar Başlatma—RADIUS ve/veyaTACBLKR+ protokolünü tekrar başlatınız

Eğer bir sistem hatası olursa aynı zamanda kendi arayüzünüzü geliştirebilirsiniz. Daha fazla bilgi için **Online Documentation** bakınız.

Yönetici olayları meydana geldiğinde CiscoSecure BLKR bir e-posta mesajı oluşturması için **Enable Mail Notifications** kontrol kutusunu kontrol ediniz sonra aşağıdaki bilgiyi giriniz:

SMTP Posta Sunucusu—İsmi ve gönderilen posta sunucusunun tanım kümesini(domain) giriniz; örneğin, *server1.company.com*

Mail account to notify—Amaçlanan alıcının tam e-posta adresini giriniz. Örneğin, *msmith@company.com*

15. **Next**'e tıklayınız. CiscoSecure BLKR Servisi Başlatma penceresi açılmaktadır. Eğer Setup'tan bir NAS konfigüre etmek istemiyorsanız **Next**'e tıklayınız ve "Completing Setup" bölümüne geçiniz.

Şimdi tek bir NAS'I konfigüre etmek için şuna tıklayınız:

Yes, I want to configure Cisco IOS now **Next**'e tıklayınız.

NAS Konfigürasyonu

1. Eğer **Yes, I want to conşekil Cisco IOS now** seçtiyseniz Seçilir Kılınan Gizli Şifre Penceresi açılmaktadır. Seçilir kılınmış şifreye ilave olarak kullanılabilen bir seçmeli Seçilir kılınan Gizli şifre giriniz. **Next**'e tıklayınız. Erişim Sunucusu Konfigürasyon penceresi açılmaktadır.

2. **Next**'e tıklayınız. NAS Konfigürasyon penceresi açılır. Kaydırma penceresindeki bilgiyi gözden geçiriniz. Bu bilgi NAS için minimum Cisco IOS AAA konfigürasyon gereksinimidir.

3. Aşağıdaki seçeneklerden birini seçiniz:

NAS Detayları penceresinde girdiğiniz IP adresine Telneti **Telnet Now?** Tıklayınız.

NAS konfigürasyonu otomatik olarak panoya kopyalanmaktadır ve doğrudan doğruya NAS konfigürasyon dosyasına yapıştırılabilmektedir. Daha fazla bilgi için Cisco IOS dökümantasyonuna bakınız.

Örnek konfigürasyonu kopyalamak için **Print**'e tıklayınız. Telneti NASa kopyalamadan önce basılmış kopyeyi gözden geçiriniz. .

Bir NASı konfigüre etmeksizin devam etmek için **Next**'e tıklayınız.

Kurulumu Tamamlamak

1. CiscoSecure BLKR Servis Başlatma penceresi açılır. Aşağıdaki seçeneklerden birini veya bir kaçını kontrol ediniz:

Yes, I want to start the CiscoSecure BLKR Servis now

Not: CiscoGüvenli BLKR web-tabanlı arayüzüne erişmek için Servis çalışıyor olmalıdır.

Yes, I want Setup to launch the CiscoGüvenli BLKR Administrator from my browser following installation

Yes, I want to view the readme file

Not: “readme file” ilave önemli bilgi içermektedir.

2. **Next**'e tıklayınız. Kurulum Tamamlama penceresi açılmaktadır.

3. **Finish**'e tıklayınız. CiscoSecure BLKR'nin kurulumu tamamdır. Windows NT masaüstünde BLKR Admin etiketli bir simge yaratılmaktadır. Tarayıcınız ile ilişkin CiscoSecure BLKR programına kısayoldur. Adım 1deki “başlatma” seçeneğini seçtiyseniz tarayıcınız başlayacaktır ve CiscoSecure BLKR açılır. Eğer adım 1deki “benioku” seçeneğini seçtiyseniz benioku dosyası açılır.

CiscoSecure BLKR Bařlatmak

CiscoSecure BLKR bařlatmak iin BLKR Admin iin URL ile bir tarayıcı bařlatmak iin BLKR Admin ikonuna ift tıklayınız veya řunu giriniz:

http://IP address:2002

Örneęin:

http://172.16.0.1:2002

Not: Her bir uzaktan eriřim yöneticisi uzaktan eriřim yönetici eriřim izinine sahip olmalıdır.

Aędaki BLKR'yi yerleřtirmek iin

Yönergeler Tanıtımı

Bu doküman bir řirket aęındaki Windows NT/2000 iin CiscoSecure Eriřim Kontrol Sunucusunu (BLKR) konuřlandırma iin planlama, tasarı ve uygulama pratiklerini ele almaktadır. Aę topolojisi, kullanıcı tabanlı seenekler, eriřim gereksinimlerini, harici veri tabanları entegrasyonu ve BLKRnin olanakları hakkında aık oturumları ihtiva etmektedir. Bu doküman ierisindeki bilgi BLKR versiyonları 2.6 ve 3.0 tabanlıdır.

BLKR Konuřlandırmasını Etkileyen Faktörler

BLKR'nin İřletim aęı iine nasıl konuřlandıracaęı hususunu etkileyen BLKRA faktörlerinin sayısı:

- Aę topoloji
- Uzaktan-eriřim politikası
- Güvenlik politikası
- İdari eriřim politikası
- Veri tabanı
- Kullanıcıların Sayısı
- Veri tabanı tipi
- Aę hızı ve güvenilirlięi

Kimlik kanıtlama, Yetkilendirme, ve Sayıřım

Cisco Güvenli BLKR, Windows NT/2000 iin bir kimlik kanıtlama, yetkilendirme, ve sayıřım (AAA) eriřim kontrolü sunucusudur. BLKR baęımsız üç set güvenlik fonksiyonlarını uyumlu řekilde konfigürasyonu iin bir yapısal çereve olan AAA vasıtasıyla aę eriřim sunucusuna eriřim kontrolü saęlamaktadır.

AAA aşağıdaki servislerin gerçekleştirilmesi için modüler bir yol sağlamaktadır:

- Kimlik kimliklama—Seçilen güvenlik protokolüne belki şifrelemeye bağlı olarak giriş ve şifre iletişimi, davet ve yanıt, mesajlaşma desteği içeren kullanıcıları saptayan yöntem sağlamaktadır.
- Yetkilendirme—Tek-zamanlı yetkilendirme veya kullanıcı hesap listesi ve profili başına her bir servis için yetkilendirme, kullanıcı grupları için destek ve IP desteği, Ağlar arası Paket Santrali (IPX), AppleTalk Uzaktan Erişim(ARA) ve Telnet içeren uzaktan erişim kontrolü yöntemi sağlamaktadır.
- Sayışım—Kullanıcı kimlikleri, başlama ve durdurma zamanları, uygulanmış komutlar sayısı (Noktadan Noktaya Protokol [PPP], paketlerin sayısı ve byte(sekiz ikil) gibi) içeren Faturalama, hesapların incelenmesi ve raporlama için kullanılan toplanan ve gönderilen güvenlik sunucusu bilgisi yöntemini sağlamaktadır.

BLKR AAA servisleri için iki adet ayrı protokol kullanılmaktadır: Uzaktan erişim Kimlik kimliklama Dahili- Çevirme Kullanıcı Servisi (RADIUS) ve Uçbirim Erişim Denetleyici Erişim Kontrolü Sistemi (TACBLKR+).

Livingston (şimdiki adıyla Lucent) da geliştirilen RADIUS AAA desteği için endüstri standardı olarak düşünülmüştür. Haziran 1996da RADIUS protokol şartnamesinin Taslak 5 Internet Tasarım Görev Kuvvetine(IETF) sunulmuştur.

RADIUS şartname (RFC2865) ve RADIUS sayışım standardı (RFC2866) şu an önerilen standart protokolleridir.

BLKR aynı zamanda RFC2868 (Tünel Protokol Desteği için RADIUS Öznitelikleri) desteklemektedir. IETF önerilen standartlarının metni aşağıdaki URL'lerde mevcuttur:

- <http://www.faqs.org/rfcs/rfc2865.html>
- <http://www.faqs.org/rfcs/rfc2866.html>
- <http://www.faqs.org/rfcs/rfc2868.html>

RADIUS tek bir adımda kimlik kimliklama and yetkilendirme sağlamaktadır. Kullanıcı ağa bağlandığı zaman NAS bir kullanıcı ismi ve bir şifre için bilgi isteminde bulunur. NAS bu durumda isteği BLKR'ye gönderecektir. NAS erişim kısıtlamaları ve kullanıcı başına konfigürasyon bilgisini içerebilmektedir.

RADIUS sunucu kimlik kimliklama onay statüsü ve herhangi bir ilgili erişim bilgi mevcudiyetini döner.

TACBLKR+ Cisco Sistemleri tescilli AAA protokolüdür. İlk başta TACBLKR olarak Minnesota Üniversitesinde özgün şekilde C. Finseth tarafından arz edilmiştir..

TACBLKR+ kimlik kimliklama, yetkilendirme ve sayışım adımlarını ayırmaktadır. Bu mimari yetkilendirme ve sayışım için hala TACBLKR+ kullanabilen ayrı kimlik kimliklama çözümlerini olanaklı kılmaktadır.

Bir oturum esnasında eğer ilave yetkilendirme kontrolüne ihtiyaç olursa erişim sunucusu kullanıcı belirli bir komutu kullanmak için verilmiş izni kullanmasını ya da kullanmamasını belirleyen bir TACBLKR+ sunucusuyla kontrol etmektedir. Bu RADIUSa mukayesen erişim sunusunda yürütülebilen komutların üzerinde daha geniş kontrol sağlamaktadır ve kimlik kimliklama mekanizmasından yetkilendirme sürecini ayırıştırır.

Örneğin, TACBLKR+ ile Kerberos Protokol kimlik kanıtama ve TACBLKR+ yetkilendirme ve sayışımını kullanmak mümkündür. Bir NAS kimlik kanıtlamayı Kerberos sunucuya geçtiğinde TACBLKR+ kimlik kanıtama mekanizmasını kullanarak NAS'ı tekrar doğrulama zorunluğu olmaksızın bir TACBLKR+ sunucusundan yetkilendirme bilgisi istemektedir.

Bir Kerberos sunucusu üzerinde kimlik kanıtlamayı başarılı şekilde geçtiğini ve sunucunun bundan sonra yetkilendirme bilgisini sağladığını NAS TACBLKR+ bilgilendirir.

TACBLKR+ ve RADIUS'un etraflıca mukayesesi bu web sayfasından bulunabilmektedir:
<http://www.cisco.com/warp/public/480/10.html>

PPP veya sanal özel ağlar (VPNler) gibi ağ erişimini sağlarken RADIUS genellikle tavsiye edilmektedir. Bir ağ erişim protokolü kadar fonksiyonel olmasına rağmen TACBLKR+ komut filtreleme gibi daha kapsamlı destek kabiliyetinden dolayı NAS erişimi için tavsiye edilmektedir.

Ağ Topolojisi

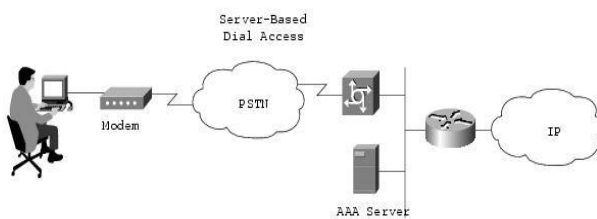
Şirket ağının nasıl konfigüre edildiği muhtemelen BLKR'nin nasıl konuşlandırılacağı konusunda en önemli tek faktördür. AAA ilk önce hesaba katıldığında ağ erişimi ya doğrudan LAN'a bağlantılı aygıtlarıyla veya modem vasıtasıyla erişime ulaşan uzaktan erişim aygıtlarıyla kısıtlanmaktadır.

Günümüzde şirket ağları kompleks olabilmektedir ve şifreleme teknolojileri sayesinde geniş çapta coğrafi olarak dağılabilmektedir.

Çevirim Erişimi

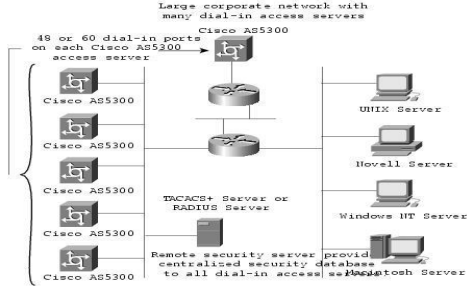
Çevirim erişimin geleneksel modelinde (bir PPP bağlantısı) bir modem veya Bütünleşik Servisler Dijital Ağ(ISDN) bağlantı kullanan bir kullanıcı bir NAS vasıtasıyla intanete erişimi onaylamaktadır. Kullanıcılar küçük bir işletmede tek bir NAS ile bağlantı kurabilmektedir veya birçok coğrafi olarak dağıtılmış erişim sunucuları seçeneğine sahip olabilmektedir. Küçük bir LAN ortamında (Şekil 1) tek bir BLKR genellikle NASa dahili olarak kurulmaktadır ve bir güvenlik duvarı ve NAS ile dışardan erişime karşı korunmaktadır. Bu ortamda kullanıcı veritabanı genellikle küçüktür ve AAA için erişim gerektiren az aygıt vardır ve veritabanı kopyalama yedekleme olarak ikinci bir BLKR ile sınırlıdır.

Şekil 1. Küçük LAN Ortamı:



Daha geniş bir çevirim ortamında yedekleme ile tek bir BLKR kurulumu da uygundur (Şekil 2). Bu konfigürasyonun uygunluğu ağ ve sunucu erişim atalet süresine bağlıdır. Bu senaryoda bir yedekleme BLKR eklemek tavsiye edilmektedir.

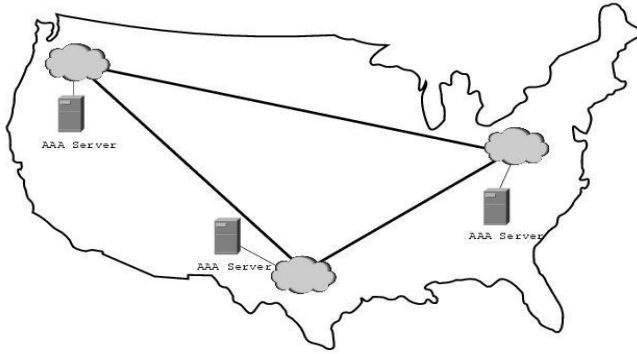
Şekil 2. Geniş Çevirim Ağı:



Coğrafi olarak dağıtılmış geniş bir ağda (Şekil 3) erişim sunucuları bir şehrin farklı kısımlarında, farklı şehirlerde veya farklı kıtalarda yerleştirilebilmektedir. Merkezi bir BLKR ağ atalet süresi mesele değilse çalışabilmektedir. Fakat uzun mesafelerdeki bağlantı güvenilirliği problemlere sebep olabilmektedir. Bu durumda yerel BLKR kurulumları merkezi bir sunucuya tercih edilebilmektedir. Eğer bitişik veri gereksinimi lüzumlu ise o zaman bir merkezi sunucudan veri tabanı kopyalama veya senkronizasyonu lüzumlu olabilmektedir. Bu ayrıca harici veri tabanların kullanımıyla (NT veya kimlik kanıtlama için kullanılan Hafif Ağırlıktaki Dizin Erişim Protokolü [LDAP] gibi) ile güçleştirilebilmektedir.

İlave güvenlik düzeyleri ağı ve WAN boyunca iletilen kullanıcı bilgisini korumak için gerekebilmektedir. Bu topoloji ve güvenlik faktörlerini birleştirmektedir. Bu durumda bölgeler arasındaki şifreli bağlantıya ilaveten gösterilmektedir.

Şekil 3. Coğrafi olarak Dağıtılmış Ağ:



Kablosuz Ağ

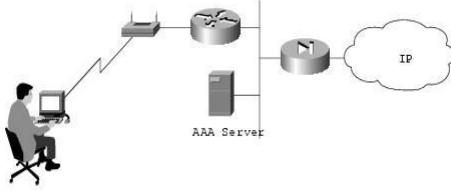
Kablosuz ağ AAA'ya göre yenidir. Cisco Aironet[®] serisi gibi kablosuz erişim noktası (AP) gezgin istemciler için LAN'a köprülü bir bağlantı sağlamaktadır. Kimlik kanıtlama AP'ye erişim kolaylığından dolayı tamamıyla zorunludur. Başkalarının gizli konuşmalarını gizlice dinleme kolaylığı yüzünden iletişimlerde şifreleme aynı zamanda bir gereksinimdir. Bunun gibi hatta güvenlik çevirim senaryosundan daha büyük bir rol oynamaktadır ve bu ilerde detaylı olarak ele alınacaktır.

Ölçeklendirme kablosuz ağda ciddi bir sorun olabilmektedir. "Kablolu" LAN'dakine benzer şekilde kablosuz LAN'ın (WLAN) mobilite faktörü çevirim ağı olarak benzer öneme sahiptir. "Kablolu" LAN'den farklı olarak bununla birlikte WLAN daha kolayca genişletilebilmektedir. WLAN teknolojisi bir AP vasıtasıyla bağlanan kullanıcıların sayısında fiziksel limitlere sahip olmamasına rağmen AP'lerin sayısı çabucak büyüyelebilmektedir. Çevirim ağıyla olduğu gibi WLAN tüm kullanıcıların tam erişimine izin vermek üzere bütünüyle tasarlanabilmektedir veya siteler, binalar,

zeminler veya odalar arasındaki farklı alt ağlara sınırlı erişim sağlayabilmektedir.

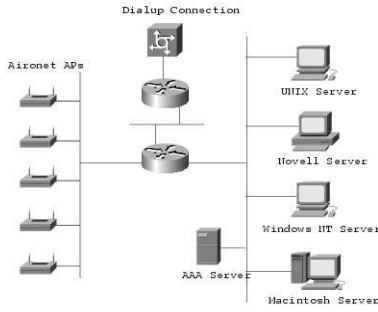
Bu WLAN'larla birlikte eşsiz bir sonuç yetiştirmektedir: AP'ler arasında "roam(dolaşım)" için bir kullanıcı kapasitesi.

Şekil 4. Basit WLAN:



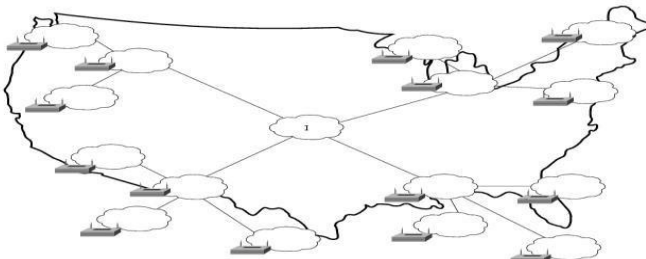
Basit bir WLAN'da tek bir AP kurulabilmektedir (Şekil 4). Sadece tek bir AP olduğu için birincil sorun güvenlidir. Bu ortamda genellikle küçük bir kullanıcı tabanı ve endişelenecek az ağ aygıtı vardır. Ağ üzerindeki diğer aygıtlara AAA servisleri sağlamak BLKR üzerindeki herhangi bir önemli ilave yüke neden olmayacaktır.

Şekil 5. Yerleşke WLAN:



Bir WLAN içinde geniş bir bina veya yerleşke ortamında AP'lerin birkaçı konuşlandırıldığında (Şekil 5) BLKR'nin nasıl konuşlandırılacağı hakkında kararlar daha karmaşık olmaktadır. Şekil 5 aynı LAN üzerindeki bütün AP'leri göstermesine rağmen yönlendiriciler ve anahtarlar vasıtasıyla bağlanan LAN boyunca dağıtılabilmektedir. WLAN'ların daha geniş coğrafi dağıtımında BLKR konuşlandırma çevirim LAN'ların geniş bölgesel dağıtımına benzerdir (Şekil 3). Bu özellikle bölgesel topoloji yerleşke WLAN olduğu zaman doğrudur. Bu model WLAN'lar daha çok basit WLAN'a benzeyen küçük sitelerin birçoğunda WLAN'lar konuşlandırıldığı zaman değişmeye başlar(Şekil 4). Bu model şehir veya eyalet boyunca ulusal veya evrensel olarak küçük mağaza zincirlerine uygulanabilir(Şekil 6).

Şekil 6. Küçük Sitelerin Geniş Konuşlandırması:



Şekil 6 modelinde, BLKR'den kimlik analizi kararı, tüm ağdaki kullanıcıların herhangi bir AP'de

erişime ihtiyaç duyup duymadığına veya sadece bölgesel veya yerel ağ erişimine ihtiyaç duyup duymadığına bağlıdır. Bu faktör, birlikte verilerle birlikte, yerel veya bölgesel BLKR kuruluşlarının gerekip gerekmediğini ve nasıl bir devamlılık sürdürüldüğünü kontrol eder. Bu çok büyük dağıtım modelinde, Güvenlik de daha karmaşık hale geliyor

VPN Kullanarak Uzaktan Erişim

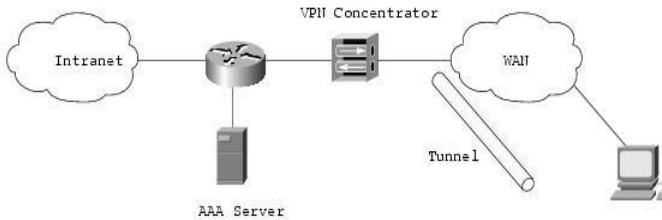
VPN'ler Internet veya dış Internetler (extranetler) gibi üçüncü parti ağlar üzerinden uçtan uca güvenli özel ağ bağlantıları kurmak üzere organizasyonlara izin vermek için gelişmiş şifreleme ve tünelden gönderme kullanmaktadır(Şekil 7).

Bir VPN aşağıdaki avantajları içermektedir:

- **Maliyet Tasarrufu**—VPN teknolojisiyle üçüncü parti ağlarını manivela ederek organizasyonlar artık bağlı kiralananmış veya Frame Relay(Çerçeve Aktarıcı) hatlar kullanmak zorunda değildir ve pahalı 800-hatlı veya uzak mesafeli çağrılarda kaynak tüketen modem bankaları yerine yerel bir Internet Servis Sağlayıcısı (ISP) vasıtasıyla ortak ağlarına uzaktan erişim kullanıcılarıyla bağlanabilmektedirler.
- **Güvenlik**—VPN'ler yetkisiz erişimden veriyi koruyan gelişmiş şifreleme ve kimlik kanıtama protokollerini kullanarak en yüksek seviyede güvenlik düzeyi sağlamaktadır.
- **Ölçeklenebilirlik**—VPN'ler şirketlere ISP'lerin içerisindeki uzaktan erişim altyapılarını kullanma olanağı vermektedir. Bu yüzden şirketler önemli altyapı eklemeksizin hemen hemen sınırsız miktarda kapasite ekleyebilmektedir.
- **Geniş bantlı Teknolojiyle Uyumluluk**—

VPNler önemli esneklik ve verimlilik sağlarken ortak ağlarına erişimi elde ettiklerinde DSL ve kablo gibi yüksek hız, geniş bantlı bağlantılılık avantajlarını mobil çalışanlarına, telecommuternlara (bilgisayar bağlantısı aracılığıyla iletişim kurarak evde çalışan insanlara) ve mesai çalışanlarına sağlamaktadır.

Şekil 7. Basit VPN Konfigürasyonu:



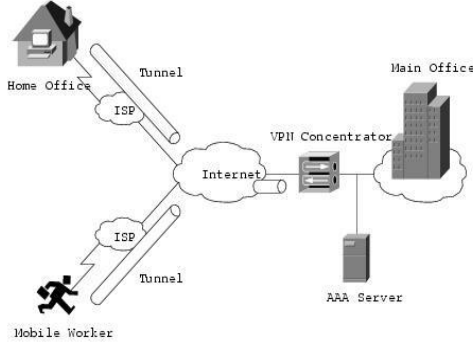
İki tip ağa erişim VPN'leri vardır:

Siteden Siteye VPN'ler—Internet gibi genel bir ağ üzerinden uzaktan erişim ofisleri ve merkezi ofisler gibi çoklu sabit siteler arasında geniş-ölçekli şifreleme sağlayarak klasik WAN genişletmektedir.

Uzaktan-Erişim VPNs—VPN istemci yazılımı vasıtasıyla bir servis sağlayıcısı gibi üçüncü bir parti ağı boyunca kendi ortak ağları ve mobil veya uzaktan erişim kullanıcıları arasında güvenli, şifreli bağlantılara izin vermektedir.

Genellikle siteden siteye VPN'ler tipik bir WAN bağlantısı olarak değerlendirilebilmektedir ve güvenli başlangıç bağlantısına AAA genellikle kullanmak üzere konfigüre edilmemektedir. Bununla birlikte uzaktan- erişim VPN'ler bununla birlikte klasik uzaktan erişim-bağlantı teknolojisine benzerdir (modem veya ISDN) ve etkili şekilde AAA modelini kullanarak kendilerine katkıda bulunmaktadır (Şekil 8).

Şekil 8. Şirket VPN Çözümü:



Aşağıdaki web sayfasında daha kapsamlı VPN çözümlerinin uygulaması mevcuttur:

http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

Uzaktan-Erişim Politikası

Uzaktan erişim geniş bir kavramdır. Genel olarak kullanıcının LAN'a veya LAN'dan dışardaki öz kaynaklara (diğer deyişle, Internet) nasıl bağlanacağını tanımlamaktadır. Bu bağlantı birkaç yolda meydana gelmektedir.

Yöntemler fakat sadece bunlarla sınırlı olmayan çevirim, ISDN, kablosuz köprüler ve güvenli Internet bağlantıları içermektedir. Her bir yöntem avantajlara ve dezavantajlara sahiptir ve AAA servisleri sağlayarak kendi meydan okumasını sağlamaktadır.

Bu sıkıca uzaktan-erişim politikasını ağ topolojisine bağlamaktadır. Bu erişim yöntemine ilaveten spesifik ağ yönlendirme(erişim listeleri), günün her saatinde erişim, NAS erişim üzerindeki kişisel kısıtlamalar(erişim kontrol listeleri) gibi diğer kararları içermektedir ve böylece aynı zamanda BLKR'nin nasıl konuşlandırılacağını etkilemektedir.

Uzaktan-erişim politikaları bir ISDN veya Genel Anahtarlı Telefon Ağı (PSTN) üzerinden çeviren bir mobil kullanıcıları veya bilgisayar bağlantısı aracılığıyla iletişim kurarak insanların evlerinde çalışanlar için uygulanabilmektedir. Bu gibi politikalar BLKR ile ortak yerleşkede ve erişim sunucusunda (AS5300, VPN çoğullayıcı vesaire) yürütülmektedir. Şirket ağı içindeki uzaktan-erişim politikaları kablosuz erişim için bireysel çalışanlar için erişimi kontrol edebilmektedir.

BLKR uzaktan-erişim politikası kullanıcıların uzaktan erişimini yetkilendirme ve merkezi kimlik kanıtlamayı kullanarak kontrolü sağlamaktadır. BLKR veri tabanı bütün kullanıcı ID'lerini, şifrelerini ve ayrıcalıklarını sağlamaktadır. BLKR erişim politikaları erişim kontrol listeleri şekliyle veya spesifik dönemlerde veya spesifik erişim sunucuları üzerinde erişim izni vererek veya Cisco AS5300 Ağ Erişim Sunucusu gibi (ACL'ler) ağ erişim sunucularına indirilebilmektedir.

Uzaktan-erişim politikası tüm ortak güvenlik politikasının parçasıdır.

Güvenlik Politikası

Cisco Sistemleri en az aşağıdaki politikaları tanımlaması gereken bir güvenlik politikası geliştiren ağı destekleyen her bir organizasyonu tavsiye etmektedir:

- Hazırlık
- Kullanım politika deyimlerini atamak
- Bir Risk Analizini Yönetmek
- Tam bir güvenlik takım yapısı Kurmak
- Önleme
- Güvenlik Değişikliklerini Onaylama
- Ağınızın Gözetim Güvenliği
- Cevap Verme
- Güvenlik ihlalleri
- Restorasyon
- Gözden Geçirme

Güvenlik politikası üzerine uygun birkaç doküman aşağıdaki URL'lerde yer almaktadır:

<http://www.cisco.com/warp/public/126/secpol.html>

http://www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/deesp_wp.htm

http://www.cisco.com/univercd/cc/td/doc/product/yazılım/ios121/121cgcr/secur_c/scdovertv.htm

İdari Erişim Politikası

Bir ağı yönetmek bir ölçek işidir. Ağ aygıtlarına idari erişim için bir politika sağlamak doğrudan ağın ölçüsüne ve bunu sağlayan yöneticilerin sayısına bağlıdır. NAS üzerindeki yerel kimlik kanıtlama yerine getirilebilmektedir. Ağ yönetim araçları kullanımı geniş ağlara yardım edebilmektedir fakat eğer yerel kimlik kanıtlama her bir aygıt üzerinde kullanılıyorsa politika genellikle NAS üzerinde tek bir girişten oluşacaktır. Bu yeterli aygıt güvenliğini yükseltmez. BLKR kullanımı merkezi bir yönetici veri tabanı ve tek bir lokasyonda eklenebilen veya silinebilen yöneticiler için imkân sunmaktadır.

TACBLKR+ NAS idari erişimini kontrol etmek için tavsiye edilen bir NAS yöneticisinin aygıt erişiminin komut kontrolü başına (komut filtreleme) kapasitesinden dolayı AAA protokol seçeneğidir. Kimlik kanıtlama kabulü esnasında yetkilendirme bilgisinin tek-zamanlı transferinden dolayı RADIUS bu amaç için pek yeterli değildir.

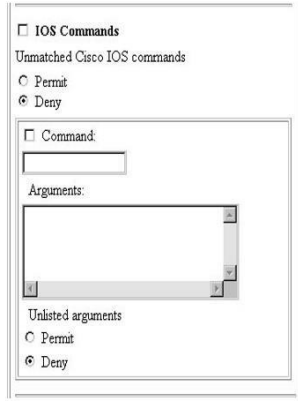
Erişimin türü aynı zamanda önemli bir noktadır. Eğer NAS'a farklı idari erişim düzeyleri olaksa veya yöneticilerin bir altseti belirli sistemlere sınırlandırılacaksa zorunlu olarak yöneticileri sınırlamak üzere BLKR komut ve NAS filtreleme ile birlikte kullanılabilir.

Yerel kimlik kanıtlama kullanmak bir aygıt üzerinde giriş yok (daha önce ele alındığı gibi) veya kontrol erişimine ayrıcalık düzeyleri kullanarak idari erişim politikasını sınırlamaktadır. Ayrıcalık düzeyleri vasıtasıyla erişimi kontrol etmek kullanışsızdır ve ölçeklenebilir değildir.

NAS üzerinde deęişen spesifik komutların ayrıcalık düzeylerini gerektirmektedir ve spesifik ayrıcalık düzeyleri kullanıcı girişı için tanımlanmaktadır. Komut ayrıcalık düzeyi düzenleyerek aynı zamanda daha çok problemlere yol açmak oldukça kolaydır. BLKR üzerindeki komut filtrelemeyi kullanmak deęişen kontrollü komutların ayrıcalık düzeyini gerektirmez. NAS ayrıştırılacak BLKR'ye komut gönderir ve BLKR komutu kullanmak için yönetici izine sahip olup olmayacağını kararlaştırır(Şekil 9). AAA kullanımı, BLKR üzerindeki herhangi bir yöneticiye AAA için konfigüre edilen herhangi bir NAS üzerinde kimlik kanıtlamaya izin verdiğiinden NAS filtreleme her NAS temeli üzerinde bu aygıtlara erişimi sınırlandırmak için kullanılabilir.

Birkaç ağ aygıtlarıyla küçük bir ağ sadece onu yönetmek için bir veya iki bireye gereksinim duyabilmektedir. Aygıt üzerindeki yerel kimlik kanıtlama genellikle yeterlidir. Eğer kimlik kanıtlamanın sağlayabildiğinden daha çok kontrol gerekirse yetkilendirmenin bazı yöntemleri gerekmektedir. Başlarda ele alındığı üzere ayrıcalık düzeylerini kullanan erişimi kontrol etmek kullanışsızdır. BLKR bu problemi azaltmaktadır.

Şekil 9. Komut Filtreleme Konfigürasyonu



Yönetilen büyük sayıdaki aygıtlarla büyük şirket ağlarında BLKR'nin kullanımı sanal bir gereksinim olmaktadır. Aygıtlarının birçoğunun yönetimi erişim düzeylerini çeşitlendirmekle daha çok sayıda yöneticilere gereksinim duymaktadır

Yerel kontrolün kullanımı yöneticileri ve aygıtlar deęişirken gereken konfigürasyon deęişiklerini tam takip etmeye çalışırken karışıklık yaratacaktır. CiscoWorks gibi ağ yönetim araçlarının kullanımı bu ağır yükü hafifletmeye yardım eder fakat sağlanan güvenlik yine de önemli bir noktadır.

BLKR rahatlıkla 10,000 kullanıcıya kadar idare edebildiği için BLKR'nin desteklediği yöneticilerin sayısı bir mesele deęildir.

Eğer AAA desteği için RADIUS kullanan daha geniş bir uzaktan erişim popülasyonu(evreni) varsa ortak bilgi teknoloji takımı (IT) yönetici takımı için TACBLKR+ kimlik kanıtlamayla ilgili ayrı bir BLKR sistemi dikkate alınmalıdır. Bu genel kullanıcı popülasyonunu idari takımdan izole edecektir ve yanlışlıkla ya da kazaren ağ aygıtlarına erişimi olasılığını azaltacaktır. Eğer uygun bir çözüm deęilse uzaktan erişim ağına erişmek için RADIUS ve idari girişler için (shell/exec) TACBLKR+ kullanarak ağ aygıtları için yeterli güvenlik sağlamaktadır.

İdari ve Genel Kullanıcıları Ayırmak

Genel ağ kullanıcılarını ağ aygıtları erişiminden alıkoymak önemlidir. Bir genel kullanıcı sistemi bozmayı planlamasa bile yanlışlıkla veya kazara erişim ağ erişimine tesadüfi bozulmasına neden olabilir. Genel kullanıcıları idari kullanıcılardan ayırmak AAA ve BLKR'nin alanına girer.

Böyle bir ayrımı gerçekleştirmenin en kolay ve tavsiye edilen yöntemi genel uzaktan erişim kullanıcısı için RADIUS ve idari kullanıcı için TACBLKR+ kullanmaktır. Muhtemelen bir yönetici aynı zamanda uzaktan erişim ağına genel bir kullanıcı gibi erişmek ihtiyacı duyduğunda ortaya çıkacak bir meseledir.

BLKR ile problem çıkmaz. BLKR'de yönetici hem RADIUS hem de TACBLKR+ konfigürasyonlarına sahip olabilir. Yetkilendirme kullanarak RADIUS kullanıcılar izin verilen protokol olarak kurulu PPP (veya diğer ağ erişim protokolü)ne sahip olabilmektedir. Shell(exec) erişimine izin vermek için TACBLKR+ altında sadece yönetici konfigüre edilmelidir.

Örneğin, eğer yönetici genel bir kullanıcı olarak ağa bağlanıyorsa NAS, RADIUSu belgeleme ve onaylama protokolü olarak kullanmaktadır ve PPP protokolü yetkilendirilmektedir. İçinde eğer aynı yönetici konfigürasyon değişiklikleri yapmak için ağ aygıtına uzaktan yakından bağlanıyorsa aygıt kimlik kanıtlama ve yetkilendirme için TACBLKR+ protokolünü kullanacaktır. Bu yönetici TACBLKR+ altındaki kabuk izniyle BLKR üzerinde konfigüre edilebildiği için ilgili aygıtı bağlanmak üzere yetkilendirilecektir. Bu BLKR üzerinde NAS'ın bir tanesi RADIUS ve diğer TACBLKR+ için olmak iki ayrı konfigürasyona sahip olmasını gerektirmez. Cisco IOS® Yazılımı altında bir NAS konfigürasyon örneği sağlanmaktadır.

Örnek 1—PPP ve Shell Girişlerini Ayırmak için Örnek Cisco IOS Konfigürasyonu

```
aaa new-model
tacBLKR-server host <ip-
address> tacBLKR-server key
<secret-key> radius-server host
<ip-address> radius-server key
<secret-key>
aaa authentication ppp default group radius
aaa authentication login default group tacBLKR+
local aaa authentication login console none
aaa authorization ağ default group radius
aaa authorization exec default group tacBLKR+ none
aaa authorization command 15 default group tacBLKR+
none username <user> password <password>
line con 0
login authentication no_tacBLKR
```

Tersine eğer bir genel kullanıcı bir ağ aygıtına kendi uzaktan erişim girişini kullanmaya çalıştığında BLKR kullanıcının ismini ve şifresini kontrol edecek ve onaylayacaktır fakat yetkilendirme süreci başarısızlığa uğrayacaktır çünkü kullanıcı aygıtı shell/exec erişimine izin veren ehliyete sahip olmayacaktır.

Veritabanı

Topolojik önemi bir yana veritabanı BLKR için konuşlandırma kararları ile ilişkili en etkili faktörlerden biridir. Kullanıcı tabanı ölçüsü, ağ boyunca kullanıcıların dağıtımı, erişim gereksinimleri ve veri tabanı tipi olmak üzere kullanılan tümü BLKR'nin nasıl kullanıldığına katkıda bulunur.

Kullanıcıların Sayısı

BLKR 80,000 ile 100,000 arasındaki kullanıcıları rahatça yönetmek üzere şirket ortamı için tasarlanmıştır. Bu genellikle bir şirket için yeterli olandan daha fazladır. Bu sayıyı aşan bir ortamda kullanıcı tabanı tipik olarak geniş çapta coğrafi dağıtılmaktadır ve birden fazla BLKR konfigürasyonunu kullanmak üzere kendine eklemektedir.

"Ağ Topoloji" bölümünde ele alındığı gibi uzaktan erişim bölgelerini yönetmek için tek bir BLKR konuşlandırmak ağ atalet süresi ve güvenilirliğinden dolayı mantıklı olmayacaktır. Bir WAN hatası kimlik kimlik kimlik sunucusunun kaybından dolayı yerel bir ağı erişilmez hale getirecektir.

Bu önemli noktaya ek olarak tek bir BLKR'yi idare eden kullanıcıların sayısını azaltmak verilen herhangi bir zamanda meydana gelen girişlerin sayısını azaltarak veya kendi veri tabanı üzerindeki yükü düşürerek performansı geliştirmektedir.

Kimlik kimlik kimlik Tipi

BLKR kimlik kimlik kimlik seçenekleri sayısını desteklemektedir. BLKR'nin mevcut versiyonları altında seçenekler yerel BLKR veri tabanı kullanımı, harici veri tabanı yoluyla uzaktan erişim kimlik kimlik kimlik veya BLKR yerel veri tabanı ile ilgili veri tabanı yönetim sistemi (RDBMS) uzaktan erişim bir senkronizasyon içermektedir. Tablo 1 çeşitli seçenekleri ve mevcut teknik özellikleri göstermektedir.

Tablo 1. BLKR Veritabanı Seçmeli					
Kimlik kimlik kimlik Yöntem	Teknik özellikler				
	Clear Text	PAP	CHAP	MS-CHAP	Grup Gönderimi
Yerel	X	X	X	X	X
NT/2000 AD	X	X		X	X
Novell NDS	X	X			X
Soysal LDAP	X	X			X
ODBC	X	X	X	X	X
RDBMS-Senkronizasyon kullanan RDBMS	X	X	X	X	X
Andaçlı Sunucu (OTP)	X	X			
MCIS	X	X	X	X	X
Uzaktan erişim AAA Sunucusu	X	X	*	*	

* Eğer uzaktan erişim AAA sunucusu tarafından destekleniyorsa.

Her bir veri tabanı seçeneği ölçeklenebilirlik ve performans ile ilgili olarak kendi avantajları kadar sınırlamalara sahiptir.

Uzaktan erişim AAA Sunucusu (Proxy):

Proxy(Vekil) otomatik olarak kimlik kanıtama talebini bir NASdan diğer AAA sunucusuna iletmek üzere BLKRye olanak sağlamaktadır. Talep başarılı şekilde onaylandığında uzaktan erişim AAA sunucusu üzerindeki kullanıcı için konfigüre edilen yetkilendirme ayrıcalıkları NAS üzerindeki oturum için kullanıcı görüntü bilgisinin uygulandığı yere, orijinal BLKRye geri devredilmektedir. Tanımlı yerel veritabanında konfigüre edilmesi gereken kullanıcıların sayısını en aza indirgeyerek BLKRnin kullanımını genişletebilen çok güçlü bir araçtır. Örneğin, grup bilgisi yerel BLKR üzerinde sağlanmak zorunda değildir. Diğer avantajı ise organizasyon BLKR ile sınırlı değildir. Diğer sağlayıcıların AAA ürünleri kullanılabilir. Bir mahzuru kullanıcı kendi ismini daha önceden tanımlı bir dizgi ile beraber sağlamalıdır (örneğin, "mary.smith@ortak.com," "@ortak.com" sunucunun Dağıtım Tablosunda diğer spesifik BLKR ile ilişkili olarak tanımlı bir karakter dizisidir.) Diğer dezavantajı ise NAS filtreleme icra edilirken problem yaratmasıdır. İletilen BLKR'nin NAS IP adresi talebi oluşturan NAS'ın IP adresinden daha çok kullanılmaktadır.

Ağ Hızı ve Güvenilirliği:

Aynı zamanda ağ atalet süresini ilgilendiren ağ hızı ve ağ güvenilirliği BLKR'nin nasıl konuşlandırılacağı konusunda önemli bir rol oynamaktadır. Kimlik kanıtlamadaki gecikmeler istemci tarafında veya NASTa zaman aşımalarıyla sonuçlanmaktadır. Global olarak dağılmış kuruluş gibi geniş, yayılmış ağlar için genel kural her bir bölgede en az BLKR konuşlandırmasına sahip olmaktır. Eğer siteler arasındaki güvenilir yüksek- hızlı bir bağlantı birleşmiş değilse bu yeterli olmayabilir. VPNler tartışmasında bahsedildiği üzere link sağlamak için Internet kullanarak şirketlerin çoğu günümüzde sitelerde arasında güvenli VPN bağlantısı kullanıyor. Bu para ve zaman tasarrufu sağlar fakat bu sağlanacak T1 linkine ve bir tahsis edilmiş çerçeye hız ve güvenilirlik sağlamaz. Eğer kimlik kanıtama iş fonksiyonelliği sağlamak için tıpkı kablosuz LAN ile bağlı yazar kasaları olan bir mağaza örneğinde olduğu gibi kritik ise WAN bağlantısının bir BLKRye uzaktan erişim kaybı dönüm noktası olabilir. Aynı mesele BLKR tarafından kullanılan harici bir veritabanına uygulanabilmektedir. Veritabanı güvenilir ve zamanında erişimi kesinleştirmek üzere BLKR kuruluma yeterli derecede yakın konuşlandırılmalıdır. Bir yerel BLKR'yi uzaktan erişim bir veritabanıyla kullanmak uzaktan erişim bir BLKR kullanmak gibi aynı problemlere sebep olabilmektedir.

Bu senaryodaki olası diğer problem bir kullanıcının kullanıcı ismi doğrulanmadığında bir mesaj almaktan çok zaman aşımı problemleriyle karşı karşıya kalmasıdır. NAS BLKR ile kontak kurabilebilecektir fakat BLKR cevap için bir süre bekleyecektir ya da hiçbir şekilde cevap almayacaktır. Eğer BLKR uzaktaysa NAS zaman aşımına uğrayacak ve kullanıcıyı doğrulamak için alternatif bir yöntem deneyecektir fakat sonraki durumda muhtemelen kullanıcının istemci programı ilk önce zaman aşımına uğrar.

Gözden Geçirilmesi

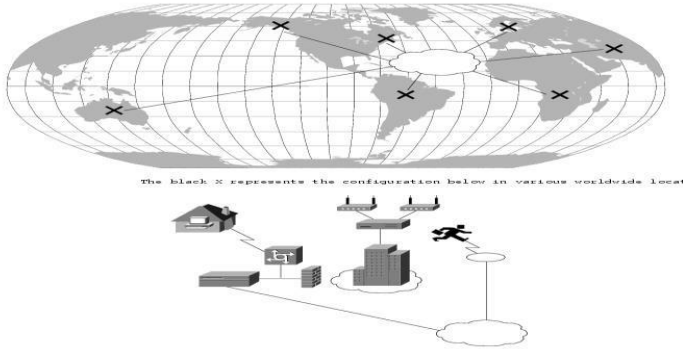
BLKR'nin nasıl konuşlandırılacağını yönlendiren faktörler yakından birbirine bağlıdır. Ağ topolojisi yakından ağ hızına ve güvenilirliğine bağlıdır. Erişim ve güvenlik politikaları ağ topolojisine ve veritabanı meselelerine bağlıdır. Hemen hemen herhangi bir kombinasyon mümkündür.

AAA ilk kez tasarlandığında ana amaç çevirim servisleri vasıtasıyla kullanıcı erişim için merkezi kontrol noktası sağlamaktı. Kullanıcı tabanı olarak gelişti ve erişim sunucularının lokasyonlarını AAA sunucusunun gerektirdiği daha çok kapasiteyle geniş çapta dağıtabilmekteydi. Bölgesel daha sonra global olarak gereksinimler yaygınlaştık. Günümüzde BLKR iç çevirim erişimi, dış çevirim erişimi, kablosuz, sanal LAN (VLAN) erişimi, güvenlik duvarları, VPN çoğullayıcıları ve idari kontrolü sağlamak üzere gerekmektedir.

Liste büyümeye devam etmektedir. Ağlar devralama ve birleşme yoluyla birleştiğinden çoklu veritabanları gittikçe kullanılmaktadır. Geniş, dağıtılmış, karışık bir ortama sahip olmak mümkündür. Çevirim ve VPN yoluyla bir uzaktan erişim kombinasyonu kablosuzla yerel erişim popüler olmaya başlamıştır. VLAN kimlik kanıtı ile karışık yerel erişim kontrolü ekleyerek kompleks bir intranet ortaya çıkmaktadır. Şekil 11 şirket ağının nasıl kompleks olabileceğini göstermektedir. Bu ortamlar çoklu BLKR konuşlandırma gerektirmektedir.

Şekil 11. Dünya Konuşlandırma Şeması:

Bu topolojideki harici veritabanlarını dahil etme veritabanı sunucusunun en uygun çoklu kurulum konuşlandırmasını zorunlu kılmaktadır. Eğer farklı veritabanları kullanımında ise yönetici farklı formatlara yer sağlamak için BLKRYi bölgesel olarak konfigüre etmek zorunda olacaktır. Örneğin, Kuzey Amerika LDAP kullanıyorsa ise Asya NDS kullanıyor ise Kuzey Amerika'daki BLKR ilk önce LDAP veritabanını kontrol etmelidir. Bu aynı zamanda Asya'daki NDS veritabanını kontrol etmek üzere konfigüre edilebilmektedir fakat bu veritabanına daha az talep olacağından harici veritabanı konfigürasyonundaki liste daha uzun olabilmektedir. Tersine de Asya'daki BLKR için geçerlidir. Eğer bölgeler ortak bir veritabanı paylaşıyorsa senkronize kurulumlar her bir bölgede konumlanmalıdır ve kendi BLKR'leri tarafından hizmet verilmelidir. Merkezi olarak yönetilen tek birleşik bir veritabanı durumunda bölgeler boyunca çoklu BLKR ve veritabanı kurulumları tavsiye edilmektedir. Veritabanı bu durumda kopyalama ve senkronizasyon yerel LAN'a zamanında erişime izin vermek üzere kullanılmaktadır.



Eğer bölgesel bir topolojinin merkezi bir yerleşkesi yoksa fakat T1, fiber optik ve benzeri teknolojiyle birbirine bağlı benzer şekilde ölçülen "mini yerleşke"lerle dağıtılıyorsa merkezi bir BLKR her bir binanın AAA ihtiyaçlarına hizmet etmek üzere kullanılmaktadır. Uzlaşan linkin imkânı düşüktür ve erişim hızları tam vaktinde kimlik kanıtlamayı yönetmek üzere yeterli olmalıdır.

WEBUI Kabulleri:

Bu kitabın tümünde, menü opsiyonlarını ve linkleri seçmek yoluyla WebUI içerisinde navigasyon yapıldığını belirtmek üzere (>) işareti kullanılmaktadır.

Örnek: Objects > Addresses > List > New (Objeler > Adresler > Liste

> Yeni) Yeni adres konfigürasyon diyalog kutucuğuna ulaşmak için :

1. Menü kolonundaki **Objects** butonunu tıklayın
2. (Küçük uygulama menüsü¹) fareyi **Addresses** üzerinde tutun. (DHTML menü) **Addresses** tıklayın **Addresses** seçeneği, bir seçenekler altkütmesi ortaya çıkaracak şekilde genişleyecektir.
3. **List**'e tıklayın. Adres defteri masası görünecektir.
4. Sağ üst köşedeki **New** linkine tıklayın. Yeni adres konfigürasyon diyalog kutusu görünecektir.

1. Menü kolonunun alt kısmında bulunan **Toggle Menu** seçeneğine tıklamak yoluyla küçük uygulama (applet) ile DHTML menü türleri arasında seçim yapabilirsiniz.

CLI Kabulleri:

Bir komut satırı arayüzü (CLI) komut işareti sunulurken aşağıdaki kabuller kullanılacaktır:

- Kare parantezler [] içersindeki her şey **opsiyoneldir**.
- Bağ parantez { } içersindeki her şey **gereklidir**.
- Birden fazla seçenek bulunması halinde, her seçenek bir çubuk işareti (|) ile ayrılacaktır. Örneğin,

```
set arayüz { ethernet1 | ethernet2 |  
ethernet3 } manage
```

bunun anlamı, “ethernet1, ethernet2 veya ethernet3 arayüzü için yönetim opsiyonlarını belirle”dir.

- Değişkenler *italik* olarak gösterilir.

Örneğin: set admin kullanıcı *name1*

password *xyz*

Bir cümle içersinde bir CLI komutu görüldüğünde, **koyu renkli** (bold) olacaktır (her zaman *italik* olan değişkenler hariç).”.

Not : Bir anahtar kelime girişi yaparken, kelimeyi benzersiz şekilde ortaya çıkarmak için yeterli sayıda harf girmeniz gerekir. Örneğin, **set admin user joe j12fmt54** komutunu girmek için **set adm u joe j12fmt54** yazmanız yeterlidir. Komut girişi yaparken bu kısaltmaları kullanabilmekle birlikte, burada belgelenen komutların tümü, herhangi bir kısaltma yapılmaksızın sunulmaktadır.

Cihazın Bağlanması:

Bu bölümde, Kablosuz cihazının şebekeye bağlanması, güç kaynağı ve anten bağlantılarının yapılması açıklanmaktadır. Kablosuz askı montaj kiti kullanıyor iseniz, bu bölümün sonunda verilmekte olan askı montaj talimatlarını kullanın.

Not: Emniyet uyarı ve ikazları için, Emniyet Kılavuzu'na başvurun. Bu kılavuzda yer alan talimatlar, bedensel yaralanmalara yol açabilecek durumlar hakkında sizleri uyarmaktadır. Herhangi bir ekipman üzerinde çalışmadan önce, elektrik devreleri ile ilgili tehlikelerden haberdar olmanız ve kazaları önlemeye yönelik standart uygulamalar hakkında bilgi edinmeniz gerekmektedir.

Cihazın Şebekenize Bağlanması:

Cisco Güvenlik duvarı cihazı, dahili şebekeleriniz ile Güvensiz şebeke arasında yerleştirildiğinde, şebekeleriniz için güvenlik duvarı ve genel güvenlik sunmaktadır. Bu kısımda fiziki bağlantılar tanımlanmaktadır.

Cihazın bir Güvensiz Şebekeye Bağlanması:

Sahip olduğunuz Kablosuz cihazının modeline bağlı olarak, aşağıdaki yollardan birini kullanmak suretiyle Güvensiz şebekeye bağlantı kurabilirsiniz:

- Güvenlik duvarı cihazı üzerindeki ADSL portundan, bir ADSL bağlantısı yoluyla
- Güvenlik duvarı cihazı üzerindeki Güvensiz porttan, bir Ethernet bağlantısı yoluyla

ADSL Port Bağlantısı:

Kablosuz ADSL cihazı üzerindeki ADSL portundan gelen ADSL kablosunu telefon çıkışınıza bağlayın. Cihazın Ek A versiyonu üzerindeki ADSL portu bir RJ-11 konektörü kullanmakta iken, Ek B versiyonu bir RJ-45 konektörü kullanmaktadır. Ek B moCiscoeri durumunda, ADSL portundan telefon çıkışına bağladığınız kablo, görüntü ve tertibat açısından bir düz 10 Baz-T Ethernet kablosu ile özdeştir.

Kablosuz ADSL cihazı üzerinde, ADSL hattı, bir dış şebekeye olan *ana* bağlantınızdır. Bir dış şebekeye yönelik bir yedek veri linki için, Kablosuz ADSL cihazı üzerindeki Güvensiz porttan gelen Ethernet kablosunu bir harici yönlendiriciye (router), bir DSL'ye ya da bir kablolu modeme bağlayabilir veya cihaz üzerindeki Modem portundan gelen bir seri kabloyu bir harici modeme bağlantılandırabilirsiniz.

Uyarı: Cihaz üzerinde bulunan hem Güvensiz portu hem de Modem portunu aynı anda bir dış şebekeye bağlayamazsınız.

Ayırıcılar (Splitter) ve Mikrofiltrelerin Bağlanması:

Bir *sinyal ayırıcı* (signal splitter), telefon sinyalini, sesli çağrılar için düşük-frekanslı ses sinyallerine, veri trafiği içinse yüksek-frekanslı veri sinyallerine bölmektedir. Servis sağlayıcımız genellikle ayırıcıyı, telefon hatlarınızı servis sağlayıcının şebekesine bağlayan bir ekipmanın parçası olarak kurmaktadır.

Servis sağlayıcı ekipmanınıza bağlı olarak, kendi kendinize kurabileceğiniz ayırıcılar da bulunmaktadır. Bu türden bir ayırıcıyı kendi başınıza tesis etmekte iseniz, Güvenlik duvarı cihazından çıkan ADSL kablosunu ve telefon hattını, ayırıcı üzerindeki uygun konektörlere (örneğin, “veri” ya da “ses”) bağlayın. Ayırıcının diğer ucunu ise telefon çıkışına bağlayın.

ADSL hattına bağlanan her bir telefon, faks cihazı, yanıtalama makinesi veya analog modem üzerine bir *mikrofiltre* kurma ihtiyacı duyabilirsiniz. Mikrofiltre, telefon hattı üzerindeki yüksek-frekanslı gürültüyü süzmektedir. Mikrofiltreyi; telefon hattı üzerinde, telefon, faks cihazı, yanıtalama makinesi veya analog modem ile ayırıcı üzerindeki ses konektörü arasına kurunuz.

Aşağıda, kendi alanınızda kuracağınız bir mikrofiltre ve ayırıcı örneği gösterilmektedir (Servis sağlayıcınızdan uygun mikrofiltre veya ayırıcıları elde etmelisiniz).



Güç Kaynağı Bağlantısı:

Kablosuz cihazına güç bağlantısı yapmak için:

1. Güç kablosunun DC konektör ucunu, cihazın arkasındaki DC güç yuvasına geçirin.
2. Güç kablosunun AC adaptör ucunu, bir AC güç kaynağına takın.

Uyarı: Güç bağlantısı için bir dalgalanma koruyucusu kullanılmasını tavsiye etmekteyiz.

Askı Montajı (Opsiyonel):

Bir Kablosuz askı-montaj kiti ile, standart bir 19 inç ekipman askısına bir veya iki Cisco Kablosuz cihazı monte edebilirsiniz. Kablosuz askı montaj kiti, tesisat talimatları ile bir askı-montaj tepsisi içermektedir. Bu tepsinin boyutları aşağıdaki gibidir:

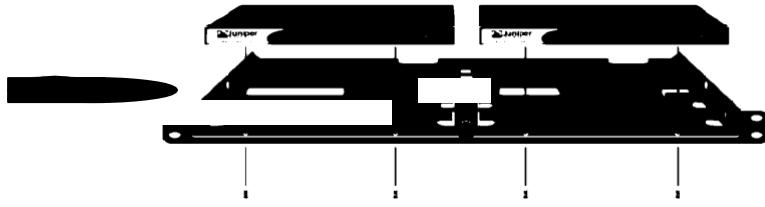
Genişlik:	48.26 cm.	19 inç.
Yükseklik:	4.013 cm.	1-5/8 inç. (1 askı)
Derinlik:	33.655 cm.	13-1/4 in.

Kablosuz cihazına(larına), askı montaj kitine ve ekipman askısına ek olarak, aşağıdakilere ihtiyaç duyacaksınız:

- PhilBLKR-başlıklı tornavida
- Ekipman askısının yiv boyutlarına denk gelen dört vida

Cihazı bir askıya monte etmek için:

1. İki vidayı, monte etmek istediğiniz her bir Cisco Kablosuz cihazının altından sökmek için bir PhilBLKR-başlıklı tornavida kullanın (Vidaları bir sonraki adımda kullanmak üzere bir kenarda tutun). Vidalar, cihazın altında ön panel yakınında bulunmaktadır.
2. Her bir cihazı, askı montaj tepsisi üzerine sokun ve 1. adımda sökmüş olduğunuz vidaları kullanarak tepsiyi sabitleyin.



3. Sağ ve sol tepsi plakalarını, geriye kalan vidalar kullanarak ekipman rafına sabitleyin.



Güç kabloları ile Ethernet kablolarını, tepsi tabanındaki açıklıklar içerisinden geçirerek ya da arka cephedeki çukurları kullanarak düzenleyebilirsiniz. Güç kaynaklarını yerleştirmek amacıyla cihazların arkasındaki boşluğu da kullanabilirsiniz.

Kablosuz Şebeke Yapılandırma

Kablosuz şebekeler, Servis Seti Belirteçleri (SSID) olarak adlandırılan isimlerden meydana gelmektedir. Bir SSID belirlenmesi, aynı lokasyonda bulunan birden fazla kablosuz şebeke elde etmenizi mümkün kılmaktadır. Her bir cihaz üzerinde maksimum sekiz SSID yapılandırabilirsiniz. SSID ismi belirlendiğinde, SSID özelliklerini yapılandırabilirsiniz.

Cisco open şeklinde bir SSID ismi belirlemek için, kablosuz şebeke bağlantısına izin verin ve kablosuz2 arayüzünü aktifleştirin:

WebUI

Wireless > SSID > New: Aşağıdakini girin
ve **OK**'e tıklayın: SSID: "Cisco open"
Kablosuz Arayüz Bağlama: kablosuz2 (seçin)
Activate Changes > **Activate Changes** butonuna tıklayın.

CLI

```
set ssid name "Cisco open"  
set ssid "Cisco open"  
authentication open encryption  
none
```

```
set ssid "Cisco open"  
arayüz wireless2 exec  
wlan reactivate
```

Wireless2 arayüzüne bir SSID tanımladığınızda, cihazı yapılandırmak için "Cihaza Erişim" kısmında verilen adımlarla, hazır wireless2 arayüz IP adresini kullanarak cihaza erişim sağlayabilirsiniz.

ADSL Konfigürasyonu

Bu kısımda, Cisco- Wireless ADSL Ek A ve Ek B cihazlarının, fabrika çıkış ayarları ve operasyonu açıklanmaktadır. Bu hazır ayarlar, çoğu durumda, yalnızca birkaç parçayı yapılandırmanıza gerek kalacak şekilde gerçekleştirilmiş durumdadır.

Bu kısımda, Güvensiz bölge arayüzüne ilişkin aşağıdaki konfigürasyonlar tanımlanmaktadır:

- ADSL Arayüzünün yapılandırılması
- Bir ADSL Arayüzüne Sanal Devreler eklenmesi
- VPI/VCI ve Çoklama Metodu
- PPPoE veya PPPoA
- Ek B Modu
- Statik IP Adres ve Netmask

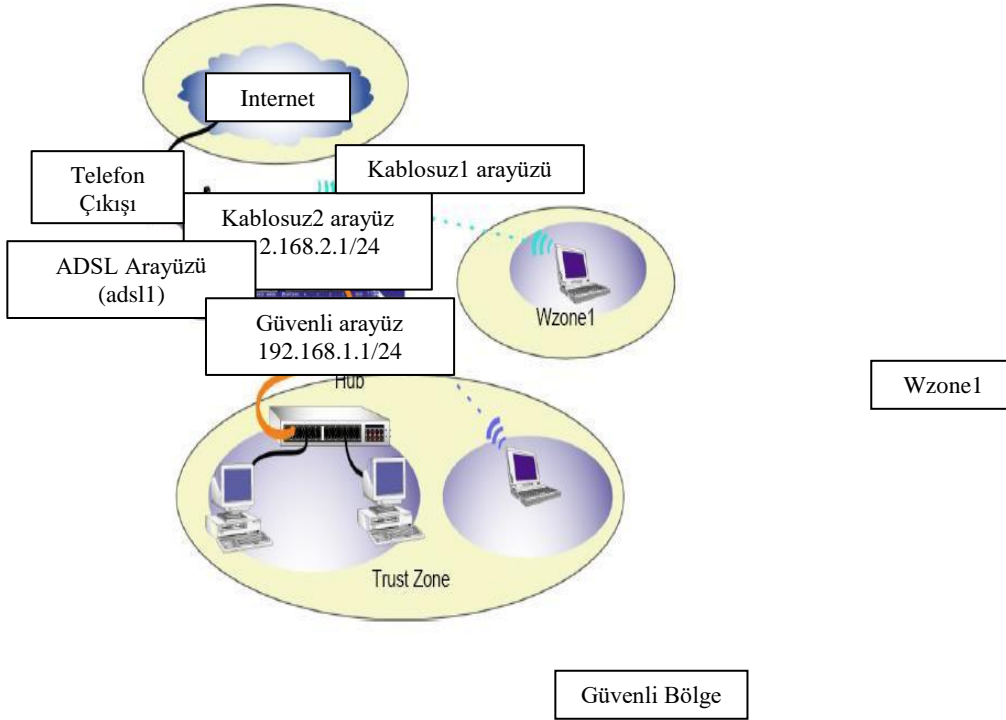
Not: Herhangibir noktada, cihazı ilk ayarlarına geri getirme ihtiyacı duyarsanız "Cihazı Fabrika Ayarlarına Getirme" kısmına bakın.

Aşağıdaki şekilde, Cisco Kablosuz ADSL cihazı için hazır konfigürasyon gösterilmektedir. ADSL arayüzü, önceden tanımlanmış "adsl1" adını taşımakta olup, şebekenizden İnternete olan ana bağlantı konumundadır. Cisco cihazının (ve şebekenizdeki cihazların) İnternete bağlanmasını mümkün kılmak için, adsl1 arayüzünü, servis sağlayıcınızdan elde edilen bilgilere göre yapılandırmanız gerekmektedir. Sayfa 20'deki "ADSL Arayüzü Yapılandırma" kısmına başvurunuz.

Cisco cihazı, Güvenli Bölgenizdeki cihazların İnternete yönelik her türlü trafiğine izin vermekle birlikte, İnternette kaynaklanan her türlü trafiğin şebekenize ulaşmasına ise izin vermemektedir. İlave kısıtlamalar da yapılandırabilirsiniz, "İlave Politikaların Yapılandırılması" kısmına başvurunuz.

ADSL Arayüzü Yapılandırma

Şebekeniz, bir Asenkronize Transfer Modu (ATM) sanal devresi aracılığıyla, servis sağlayıcınızın şebekesine bağlanmak için, Cisco cihazı üzerindeki "adsl1" ADSL arayüzünü kullanmaktadır. ADSL alt-arayüzleri oluşturmak yoluyla ilave sanal devreler yapılandırabilirsiniz (daha fazla bilgi için "bir ADSL Arayüzüne Sanal Devreler Ekleme" kısmına bakınız).



WebUI’da,Cisco cihazı üzerindeki güncel arayüzlerin bir listesini görmek için, Ağ > Arayüz seçeneklerini seçin. Bir Telnet veya Konsol oturumu kullanmakta iseniz, CLI komutu **get arayüz**’i girin. adsl1 arayüzünün Güvensiz bölgeye bağlı olduğunu görmelisiniz. Cihazı yapılandırmak için ICW kullanmış iseniz, adsl1 arayüzüne önceden tahsis edilmiş bir IP adresi ve ağ maskesi bulunabilir.

Not: ADSL arayüzünü kullanmak istemiyorsanız, bunu, **set arayüz adsl1 zone null** komutu ile Boş (Null) bölgeye bağlayabilirsiniz. Cihazı yapılandırmak için ICW kullanmakta iseniz, Güvensiz bölgeye, hazır arayüz olarak ADSL arayüzünden başka bir arayüz seçebilirsiniz.

Güvenlik duvarı cihazının servis sağlayıcısının şebekesine bağlanmasını mümkün kılmak için adsl1 arayüzünü yapılandırmanız gerekmektedir. Bunu yapmak için, servis sağlayıcınızdan aşağıdaki bilgileri elde etmelisiniz:

- Sanal Güzergah Belirteçi (Virtual Path Identifier) ve Sanal Kanal Belirteçi (Virtual Kanal Identifier) (VPI/VCI) değerleri
- Aşağıdakilerden herhangi bir olabilen ATM Adaptasyon Katmanı 5 (AAL5) çoklama metodu:
 1. içersinde her protokolün ayrı bir ATM VC üzerinden taşındığı Sanal Devre (VC)-tabanlı çoklama
 2. aynı ATM VC üzerinde birden fazla protokolün taşınmasını mümkün kılan Mantıksal Link Kontrolü (LLC) (hazır çoklama metodu)
- Ethernet üzerinden Point-to-Point Protokolü (PPPoE) veya ATM üzerinden Point-to-Point Protokolü (PPPoA) kullanarak servis sağlayıcı şebekesine bağlantı için servs sağlayıcısı tarafından tahsis edilmiş kullanıcı adı ve şifresi
- PPPoE veya PPPoA bağlantısı için sağlanan, varsa, doğrulama metodu
- Opsiyonel olarak, şebekeniz için bir statik IP adresi ve netmask değeri.

Bir ADSL Arayüzüne Sanal Devreler Ekleme:

Sanal devreler ilave etmek için, ADSL arayüzüne alt-arayüzler oluşturmanız gerekir. Maksimum 10 ADSL alt-arayüzü yaratabilirsiniz. Örneğin, kullanıcı tarafından tanımlanmış “Corp1” adlı bir bölgeye bağlı adsl1.1 isimli yeni bir alt-arayüz yaratmak için:

WebUI

Ağ > Arayüzs > New ADSL Sub-IF: Aşağıdakini girin ve ardından

Apply'a tıklayın: Arayüz Name: adsl1.1

VPI/VCI: 0/35

Zone Name: Corp1 (seçin)

CLI

```
set arayüz adsl1.1 pvc 0 35
```

```
zone corp1 save
```

“ADSL Arayüzü Konfigürasyonu”nda tanımlandığı şekilde, VPI/VCI değerlerinin ayarlanması dahil, aynen ana ADSL arayüzünde olduğu gibi, bir ADSL alt-arayüzü yapılandırmanız gerekmektedir. Bir ADSL alt- arayüzünü, ana ADSL arayüzünden bağımsız olarak yapılandırmaktasınız, yani, alt-arayüz üzerinde, ana ADSL arayüzünden farklı bir çoklama metodu, VPI/VCI ve PPP istemci yapılandırabilirsiniz. Ayrıca, ana ADSL arayüzü bir statik IP adresine sahip olmasa bile, bir alt-arayüz üzerinde bir statik IP adresi yapılandırabilirsiniz. Alt-arayüz ile ana ADSL arayüzünün; bir arayüzün PPPoA değerinin PPPoE için yapılandırılmış olması halinde aynı VPI/VCI değerlerini kullanabileceğini ve her ikisinin de LLC çoklama kullandığını not ediniz.

VPI/VCI ve Çoklama Metodu

Servis sağlayıcımız, her bir VC bağlantısı için bir VPI/VCI çifti tahsis etmektedir. Örneğin, bir tane 1 VPI değeri ve bir tane 1 VCI değeri anlamına gelen bir 1/1 VPI/VCI çifti alabilirsiniz. Bu değerler, servis sağlayıcısının, Dijital Abone Hat Erişim Çoklayıcı (DSLAM)'ın abone tarafında yapılandırmış olduğu değerlere karşılık gelmelidir.

1/1 VPI/VCI çiftini adsl1 arayüzünde yapılandırmak için:

WebUI

Ağ > Arayüzs > Edit (adsl1 arayüzü için): VPI/VCI alanına 1/1 girin ve ardından **Apply**'ı tıklayın.

CLI

```
set arayüz
```

```
adsl1 pvc 1 1
```

```
save
```

Hazır olarak, Kablosuz ADSL cihazı, her bir VC için LLC-tabanlı çoklama (çoklama) kullanmaktadır. VPI/VCI 1/1 çiftini adsl1 arayüzü üzerinde yapılandırmak ve VC üzerinde LLC kuşatmasını (encapsulation) kullanmak için:

WebUI

Ağ > Arayüzs > Edit (adsl1 arayüzü için): Aşağıdakini girin ve ardından

Apply'ı tıklayın. VPI/VCI: 1 / 2

Çoklama Yöntem: LLC (seçin)

CLI

```
set arayüz adsl1 pvc  
1 1 mux 11c save
```

PPPoE veya PPPoA

Güvenlik duvarı cihazı, ADSL linki üzerinden servis sağlayıcısının şebekesine bağlanmak üzere hem PPPoE hem de PPPoA istemcilerini içermektedir. PPPoE en yaygın ADSL kuşatma formu olup, şebekeniz üzerindeki her konak üzerinde terminasyon amaçlamaktadır. PPPoA ise, PPP oturumlarının güvenlik duvarı cihazı üzerinde sonlandırılabilmesinden ötürü, esas olarak ticaret sınıfı servis için kullanılmaktadır. Güvenlik duvarı cihazının servis sağlayıcısının şebekesine bağlanmasını mümkün kılmak için, servis sağlayıcısı tarafından tahsis edilen kullanıcı adı ve şifresini yapılandırmanız gerekmektedir. PPPoA konfigürasyonu, PPPoE konfigürasyonu ile benzerdir.

Not: Güvenlik duvarı cihazı, her bir sanal devre üzerinde yalnızca bir PPPoE oturumunu desteklemektedir.

PPPoE için “roswell” kullanıcı adını ve “area51” şifresini yapılandırmak ve PPPoE konfigürasyonunu adsl1 arayüzüne bağlamak için:

WebUI

Ağ > PPPoE > New: Aşağıdakini girin ve ardından **OK**'e tıklayın:

PPPoE Instance: poe1

Bound to Arayüz:

adsl1 (seçin)

Kullanıcıname:

roswell Password:

area51

CLI

```
set pppoe name poe1 username rowell  
password area51 set pppoe name poe1  
arayüz adsl1  
save
```

Doğrulama metodu (hazır olarak, Güvenlik duvarı cihazı Challenge Handshake Authentication Protokol veya Password Authentication Protokol'ü desteklemektedir), boşa bekleme süresi (hazır değer 30 dakika), vb. uygulamalar dahil, Güvenlik duvarı cihazı üzerinde yapılandırabileceğiniz diğer PPPoE veya PPPoA parametreleri bulunmaktadır. Servis sağlayıcısının sunucusu ile uygun iletişimi sağlamak amacıyla yapılandırmanız gereken ilave PPPoE veya PPPoA parametreleri olup olmadığını servis sağlayıcınıza sorunuz.

Ek B Modu

Bir Deutsch Telecom ADSL hattına, Kablosuz ADSL cihazının Ek B modelini bağlamakta iseniz,

bu ekipmanla çalıştırabilmek için, ADSL portu üzerindeki fiziksel arayüzü yapılandırmanız gerekmektedir. Bunu yapmak için:

WebUI

Ağ > Arayüz > Edit (adsl1 arayüzü için): Ek B modu için **DT**'yi seçin ve ardından **Apply**'a tıklayın:

Opsiyonel Konfigürasyon:

Bu kısımda, Kablosuz cihazlarının yapılandırmak isteyebileceğiniz aşağıdaki özellikleri açıklanmaktadır:

- Kısıtlayıcı Yönetim (Restricting Yönetim)
- İlave Politikaların Konfigürasyonu
- Operasyonel Mod
- Port Modunun Değiştirilmesi
- Bir Yedek Güvensiz Bölge Arayüzü Konfigürasyonu
- Güvenli veya Kablosuz2 Arayüz Adresinin Değiştirilmesi

Kısıtlayıcı Yönetim

Hazır olarak, şebekenizdeki herkes, kullanıcı adı ve şifresini bilmesi halinde güvenlik duvarı cihazını yönetebilir. Güvenlik duvarı cihazını, yalnızca şebekenizdeki bir veya birkaç spesifik konak tarafından yönetilebilecek şekilde yapılandırabilirsiniz.

Port Modunun Değiştirilmesi

Port modu, fiziksel portlar, mantıksal arayüzler ve bölgeleri bağlamaktadır.

Uyarı: Port modunun değiştirilmesi, Güvenlik duvarı cihazında mevcut konfigürasyonları ortadan kaldırmaktadır. Bundan ötürü, cihazı yapılandırmadan önce port modunu değiştirmeniz gerekmektedir.

Aşağıdaki tabloda, Kablosuz cihazlarında mevcut port modlarına ilişkin port, arayüz

Port Adı ^a	Güvenli-Güvensiz Port Modu ^b	
1	Arayüz Güvenli	Bölge Güvenli
2	Güvenli	Güvenli
3	Güvenli	Güvenli
4	Güvenli	Güvenli
Güvensiz Modem ^c	Güvensiz seri kablosuz1 kablosuz2	Güvensiz Boş Wzone1 Güvenli

Ev-İş Port Modu	
Arayüz Ethernet1- Ethernet1 Ethernet2 - Ethernet2 Ethernet3 Seri kablosuz1 kablosuz2 kablosuz3	Bölge İş- İş Ev -Ev Güvensiz Boş Wzone1 İş Ev

Güvenli/Güvensiz/DMZ (Genişletilmiş) Mod		Dual Güvensiz Port Modu		Birleşik Port Modu	
Arayüz ethernet1 ethernet1 ethernet2 ethernet2 ethernet3 seri kablosuz1 kablosuz2 kablosuz3	Bölge Güvenli Güvenli DMZ DMZ Güvensiz Boş Wzone1 Güvenli DMZ	Arayüz ethernet1 ethernet1 Ethernet1 ethernet2 ethernet3 seri kablosuz1 kablosuz2	Bölge Güvenli Güvenli Güvenli Güvensiz Güvensiz Boş Wzone1 Güvenli	Arayüz ethernet1 ethernet2 ethernet2 ethernet3 güvensiz seri kablosuz1 kablosuz2 kablosuz3	Bölge İş Ev Ev Güvensiz Güvensiz Boş Wzone1 İş Ev
kablosuz4	Wzone2				

- a. Güvenlik duvarı cihazı dış cephesinde etiketlidir.
b. Hazır port modu.
c. Modem portu kullanarak Güvensiz bölgeye bir yedek arayüzü yapılandırabilirsiniz. “Bir Yedek Güvensiz Bölge Arayüzü Konfigürasyonu” kısmına bakınız.

Aşağıdaki tabloda, Kablosuz ADSL cihazlarında mevcut port modlarına ilişkin port, arayüz ve bölge bağları özetlenmektedir:

Port Adı ^a	Güvenli-Güvensiz Port Modu ^b		Ev-İş Port Modu		Güvenli/Güvensiz/DMZ (Genişletilmiş) Mod	
	Arayüz	Bölge	Arayüz	Bölge	Arayüz	Bölge
1	güvenli	Güvenli	ethernet1	İş İş	ethernet1	Güvenli
2	güvenli	Güvenli	ethernet1	Ev Ev	ethernet1	Güvenli
3	güvenli	Güvenli	ethernet2		ethernet2	DMZ
4	güvenli	Güvenli	ethernet2	Boş ^c Boş ^c	ethernet2	DMZ
Güvensiz	güvensiz	Boş ^c Boş ^c	ethernet3	Güvensiz	ethernet3	Boş ^c Boş ^c
Modem	seri adsl1	Güvensiz	seri adsl1	Wzone1 İş	seri adsl1	Güvensiz
ADSL	kablosuz1	Wzone1	kablosuz1	Ev	kablosuz1	Wzone1
	kablosuz2	Güvenli	kablosuz2		kablosuz2	Güvenli
	kablosuz3		kablosuz3		kablosuz3	DMZ
					kablosuz4	Wzone2

- a. Güvenlik duvarı cihazı dış cephesinde etiketlidir.
b. Hazır port modu.
c. Modem portunu veya Güvensiz Ethernet portunu kullanarak Güvensiz bölgeye bir yedek arayüzü yapılandırabilirsiniz. Sayfa 28’deki “Bir Yedek Güvensiz Bölge Arayüzü Konfigürasyonu” kısmına bakınız.