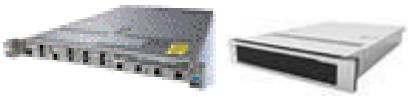
İNTERNET GÜVENLİK CİHAZI

Türkçe Tanıtım ve Kullanma Kılavuzu

MARKA: CİSCO

MODEL

SMA-M390/390X/380-K9



TEKNİK ÖZELLİKLERİ

	Cisco SMA M390	**Cisco SMA M390X**	**Cisco SMA M380**
Donanım platformu			
Form faktörü	1 raf ünitesi (1RU)	1 raf ünitesi (1RU)	2 raf ünitesi (2RU)
Boyutlar (Y x G x D)	1,7 inç x 19 inç x 31 inç (4.3 cm x 48.3 cm x 78.7 cm)	1,7 inç x 19 inç x 31 inç (4.3 cm x 48.3 cm x 78.7 cm)	3,5 inç x 19 inç x 29 inç (8.9 cm x 48.3 cm x 73.7 cm)
Yedek güç kaynağı	Evet	Evet	Evet
Uzaktan güç döngüsü	Evet	Evet	Evet
DC güç seçeneği	Yok hayır	Yok hayır	Evet (930W)
Çalışırken değiştirilebilir sabit sürücü	Evet	Evet	Evet
Güç tüketimi	2626 BTU / saat	2626 BTU / saat	2216,5 BTU / saat
Güç kaynağı	770W	770W	650W
Ethernet arabirimleri	6 bağlantı noktası 1G Base-T bakırağ arabirimi (NIC'ler), RJ-45	6 bağlantı noktası 1G Base-T bakırağ arabirimi (NIC'ler), RJ-45	6 bağlantı noktası 1G Base-T bakırağ arabirimi (NIC'ler), RJ-45
Hız (Mbps)	10/100/1000, otomatik anlaşma	10/100/1000, otomatik anlaşma	10/100/1000, otomatik anlaşma
Fiber seçeneği	Yok hayır	Yok hayır	Yok hayır
HD Boyutu	Altı 600 GB Sabit Disk Sürücüsü Var	Sekiz 600 GB Sabit Disk sürücüsü var	Cisco M380 İçerik Güvenliği Yönetimi cihazı, dört (4) 600 G HDD
İşlemci	İki adet E5-2620 v3 işlemci	İki adet E5-2620 v3 işlemci	İki Intel Xeon ES-2620 Serisi işlemci (2.0 G, 6C).
Veri deposu	İki adet 8GB DDR4-2133 DIMM1	İki adet 8GB DDR4-2133 DIMM1	Sekiz (8) 4 GB DDR3-1600-MHz RDIMM DRAM

*** Periyodik bakım gerektirmemektedir. Ürüne, tüketici kendi başına herhangi bir müdahalede bulunmamalıdır.

Kullanım Sırasında İnsan ve Çevre Sağlığı Açısından Tehlikeli veya Dikkat Edilmesi Gereken Noktalar ile İlgili Uyarılar:

Ana bilgisayar kasası genişleme yuvasına takılan kenar bağlayıcısı dışında, aşağıdaki 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 diğer parçaları arasında korunmalıdır.

Ana Bilgisayarın Diğer 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 çindeki daha büyük olan mesafeler, cihaz, nem ve yoğunlaşma nedeniyle toz ve diğer türde kirlenmelerin elektrik iletebileceği 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 bağlıyken 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 kurulumuna 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 öğesi 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 dâhil) çıkarın. Metal nesneler, güç ve toprağa bağlandıklarında ısınır ve ciddi yanıklara neden olabilir ya da metal nesneleri uçbirimlere 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 kaçının.
- 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 (çıkarılamayan, yalnızca bir kez takılan fişler dışında) yalnızca PTO ekibi ya da uygun şekilde eğitim görmüş mühendisler tarafından yapılmalıdır.

-Yönelticinin 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, yönelticiden uzak olan uçtaki bağlantıyı önce kesin.

-Elektrik şokundan kaçınmak için yönelticideki güç Açıkken ya da ağ kabloları takılıyken, bir WAN arabirim kartını 2 yuvalı bir modüle yerleştirmeyin.

-Aşağıdaki prosedürlerden herhangi birini gerçekleştirmeden 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.

-Yönelticinin 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, yönelticiden 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 kurulumuna 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 kablosunu döşeyin. Düzgün kablolama dizisi, toprak toprağa, pozitif pozitife ve negatif negatifedir. Toprak kablosunun 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, güvenliğiniz 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.

Ürün Özellikleri

Cisco SMA'lar, farklı boyuttaki kuruluşların gereksinimlerini karşılamak ve tüm Cisco ESA'larını ve Cisco WSA'larını tamamlamak üzere üretilmiştir. Tablo 2, performans spesifikasyonlarını, Tablo 3'te donanım spesifikasyonları, Tablo 4'te Cisco SMA'ya ait sipariş bilgileri verilmektedir.

Tablo 2. Cisco SMA Performans Özellikleri

	Kullanıcı Sayısı *	**Model**	**Disk alanı**	**RAID Yansıtma**	**Bellek**	**CPU'lar**
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M390	3.6 TB (6 x 600 GB SAS)	Evet, (RAID 10)	16 GB DDR4	2 x 2.4GHz, 6C
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M390X	4,8 TB (8 x 600 GB SAS)	Evet, (RAID 10)	16 GB DDR4	2 x 2.4GHz, 6C
Orta ölçekli ofis	2000 ila 10.000	Cisco SMA M380	2,4 TB (4 x 600 GB SAS)	Evet, (RAID 10)	32 GB, DDR3	2 x 2.0GHz, 6C

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 yapılıp 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°/+80° arasında bulunmalıdır.

TÜKETİCİNİN YAPABİLECEĞİ BAKIM-ONARIM VEYA ÜRÜNÜN TEMİZLİĞİNE İLİŞKİN BİLGİLER:

Güç ve Soğutma Sistemlerinin Sorunlarının Giderilmesi

Sorunu belirmek için aşağıdakileri öğeleri kontrol edin:
*Güç anahtarı AÇIK (ON) konumundayken (|) 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 belirmek için aşağıdakileri öğeleri kontrol edin:
*Router bir bağlantı noktasını algılamazsa, kablo bağlantısını kontrol edin.
*Güç anahtarı AÇIK (ON) konumundayken (|) 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, aygıtla birlikte gelen basılı belgede bulunabilir.

1. TÜKETICININ SEÇIMLILIK HAKLARI

Malın ayıplı olduğunun anlaşılması durumunda tüketici, 6502 sayılı Tüketicinin Korunması Hakkında Kanunun 11 inci maddesinde yer alan;
a- Sözleşmeden dönme,
b- Satış bedelinden indirim isteme,
c- Ücretsiz onarılmasını isteme,
ç- Satılanın ayıpsız bir misli ile değiştirilmesini isteme,
haklarından birini kullanabilir.
Tüketicinin bu haklardan ücretsiz onarım hakkını seçmesi durumunda satıcı; işçilik masrafı, değiştirilen parça bedeli ya da başka herhangi bir ad altında hiçbir ücret talep etmeksizin malın onarımını yapmak veya yaptırmakla yükümlüdür. Tüketici ücretsiz onarım hakkını üretici veya ithalatçıya karşı da kullanabilir. Satıcı, üretici ve ithalatçı tüketicinin bu hakkını kullanmasından müteselsilen sorumludur.
Tüketicinin, ücretsiz onarım hakkını kullanması halinde malın;
- Garanti süresi içinde tekrar arızalanması,
- Tamiri için gereken azami sürenin aşılması,
- Tamirinin mümkün olmadığının, yetkili servis istasyonu, satıcı, üretici veya ithalatçı tarafından bir raporla belirlenmesi durumlarında; tüketici malın bedel iadesini, ayıp oranında bedel indirimini veya imkân varsa malın ayıpsız misli ile değiştirilmesini satıcıdan talep edebilir. Satıcı, tüketicinin talebini reddedemez. Bu talebin yerine getirilmemesi durumunda satıcı, üretici ve ithalatçı müteselsilen sorumludur.

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

[redacted] AEEE YÖNETMELİĞİNE UYGUNDUR.

İTHALATÇI 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

İMALATÇI ADRESI:
CISCO SYSTEMS, INC.
170 WEST TASMAN DRIVE,
SAN JOSE, CA 95134-1706 USA
http://ww.cisco.com
TEL: 408526-4000
800553-NETS (6387)
FAKS: 408526-4100

KURULUM

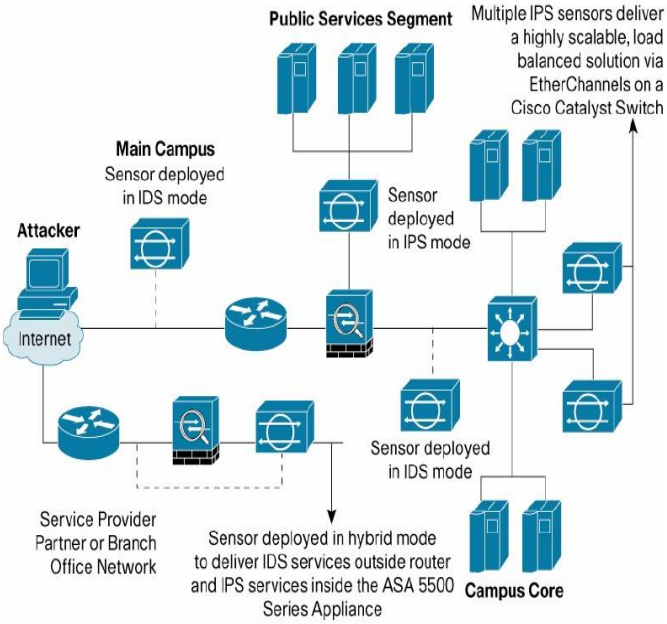
Kurulumun Nasıl Yapılacağını Gösterir Bağlantı Şeması ile Bağlantı ve Kurulum ile İlk Çalıştırılmasının Kimler Tarafından Yapılması (Kullanıcı, Teknik Servis) Gerektiğine İlişkin Bilgiler:

Esnek Konuşlandırma
Mevcut birçok çeşitli grupta BLKR teknolojilerinin parçası olarak Cisco SMA-M680-K9= Güvenlik Duvarları IPv4 ve IPv6 çeşitli ağ ortamlarında konuşlandırılabilmektedir.
SMA-M390/390X/380-K9 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 SMA-M390/390X/380-K9 Güvenlik Duvarları içine katılmış bir BLKR konfigürasyonunda sık değişen bir IDS konfigürasyonu veya hem içindeki hem de değişken eş zamanlı olarak konuşlandırılabilmektedir.
● IPv4 ve IPv6 ağları üzerinde kritik varlıklarınız maksimum konuşlandırma esnekliği ve daha düşük mülkiyet maliyeti içi tek bir adet Cisco SMA-M390/390X/380-K9 Güvenlik Duvarları ile korunmaktadır.
Cisco SMA-M390/390X/380-K9 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 SMA-M390/390X/380-K9 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 tasarlamanıza 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 SMA-M390/390X/380-K9 = Güvenlik duvarları için Konuşlandırma Senaryoları



Dağıtım Performansı

Cisco SMA-M390/390X/380-K9 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 websitelerin çoğunda görünene 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

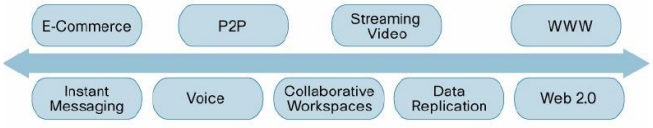
Ticari ortamlar bağlantılarla tanımlanmaktadır.

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 ticari lar arasındaki spektrumu göstermektedir.

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



Transactional	Media-Rich
Higher Connection Rates	More Transactions per Connection
More Concurrent Connections	Higher Transaction Size
Higher Transaction Rate	

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 (dahildir).

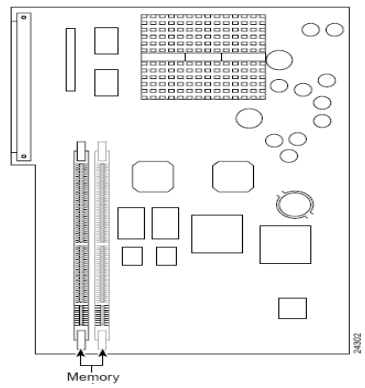
*Bir Fast Ethernet bağlantı noktasına bağlantı için Ethernet 10/100BaseT kablosu (dahildir).

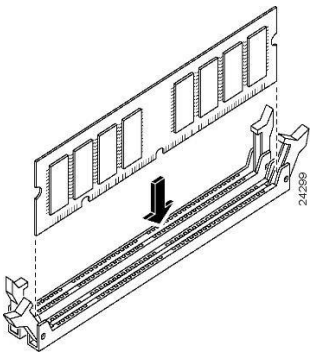
*Token Ring bağlantı noktası için bir Token Ring lob kablosu

*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 sahBLKReniz, 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 **Accept**i tıklayınız. Hoşgeldiniz penceresi açılır.

5. **Next**i tıklayınız. Başlamadan Önce pencere açılır.

6. Karşılayan her bir koşulu doğrulayınız, sonra her bir parça için kontrol kutusunu tıklayınız. **Next**i tıklayınız. (Listelenen parçalar hakkında daha fazla bilgi için Explain'e tıklayınız. Eğer herhangi bir koşul karşılanmıyorsa Kurulumdan çıkmak için **Cancel**i 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 konfigürsyon 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; Eger ikinci seçeneği seçerseniz CiscoGüvenli BLKR her iki veritabanını da kontrol edecektir.

11. (Seçmeli) Windows NT Kullanıcı Yöneticisinde açıkca 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 Ismi—NASın ismi CiscoSecure BLKR servisleri için kullanıyor olacaktır.

Erişim Sunucu IP Adresi—NASın IP adresi CiscoSecure BLKR servisleri kullanıyor 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 komünikasyonu 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:

Düzeltici 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—İsmini 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 conşekil 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 Başlatmak

CiscoSecure BLKR başlatmak için BLKR Admin için URL ile bir tarayıcı başlatmak için BLKR Admin ikonuna çift tıklayınız veya şunu giriniz:

http://IP address:2002

Örneğin:

http://172.16.0.1:2002

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

Ağdaki BLKRyi yerleştirmek için

Yönergeler Tanıtımı

Bu döküman bir şirket ağındaki Windows NT/2000 için CiscoSecure Erişim Kontrol Sunucusunu (BLKR) konuşlandırma için planlama, tasarı ve uygulama pratiklerini ele almaktadır. Ağ topolojisi, kullanıcı tabanlı seçenekler, erişim gereksinimlerini, harici veritabanları entegrasyonu ve BLKRnin olanakları hakkında açık oturumları ihtiva etmektedir. Bu döküman içerisindeki bilgi BLKR versiyonları 2.6 ve 3.0 tabanlıdır.

BLKR Konuşlandırmasını Etkileyen Faktörler

BLKR'nin İşletim ağı içine nasıl konuşlandıracağı hususunu etkileyen BLKRA faktörlerinin sayısı:

- Ağ topoloji
- Uzaktan-erişim politikası
- Güvenlik politikası
- Idari erişim politikası
- Veritabanı
- Kullanıcıların Sayısı
- Veritabanı tipi
- Ağ hızı ve güvenilirliği

Kimlik kanıtlama, Yetkilendirme, ve Sayışım

Cisco Güvenli BLKR, Windows NT/2000 için bir kimlik kanıtlama, yetkilendirme, ve sayışım (AAA) erişim kontrolü sunucusudur. BLKR bağımsız üç set güvenlik fonksiyonlarını uyumlu şekilde konfigürasyonu için bir yapısal çerçeve olan AAA vasıtasıyla ağ erişim sunucusuna erişim kontrolü sağlamaktadır.

AAA aşağıdaki servislerin gerçekleştirilmesi için modüler bir yol sağlamaktadır:

- Kimlik kanıtlama—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, Ağlararası 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 kullanmaktadır: Uzaktan erişim Kimlik kanıtlama

Dahili-Çevirme Kullanıcı Servisi (RADIUS) ve Uçbirim Erişim Denetleyici Erişim Kontrolü Sistemi (TACBLKR+).

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

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

BLKR aynı zamanda RFC2868 (Tünel Protokol Desteği için RADIUS Öznitelikleri) desteklemektedir. IETF önerilen standartlarının metini aşağıdaki URLlerde 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 kanıtlama and yetkilendirme sağlamaktadır. Kullanıcı ağa bağlandığı zaman NAS bir kullanıcı ismi ve bir şifre için bilgi isteminde bulunur. NAS bu durumda isteği BLKRye gönderecektir. NAS erişim kısıtlamaları ve kullanıcı başına konfigürasyon bilgisini içerebilmektedir. RADIUS sunucu kimlik kanıtlama 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 kanıtlama, yetkilendirme ve sayışım adımlarını ayırmaktadır. Bu mimari yetkilendirme ve sayışım için hala TACBLKR+ kullanabilen ayrı kimlik kanıtlama çözümlerini olanaklı kılmaktadır.

Bir oturum esnasında eğer ilave yetkilendirme kontrolüne ihtiyaç olursa erişim sunucusu kulanıcı 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 kanıtlama mekanizmasından yetkilendirme sürecini ayrıştırır.

Örneğin, TACBLKR+ ile Kerberos Protokol kimlik kanıtlama ve TACBLKR+ yetkilendirme ve sayışımını kullanmak mümkündür. Bir NAS kimlik kanıtlamayı Kerberos sunucuya geçtiğinde TACBLKR+ kimlik kanıtlama mekanizmasını kullanarak NASi 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 RADIUSun 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+ kout filtreleme gibi daha kapsamlı destek kabiliyetinden dolayı NAS erişimi için tavsiye edilmektedir.

Ağ Topolojisi

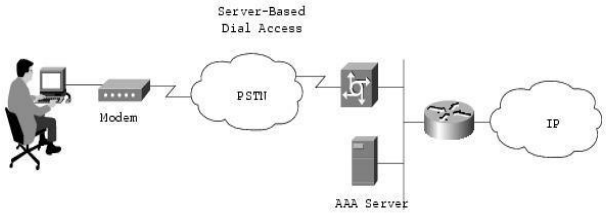
Şirket ağının nasıl konfigüre edildiği muhtemelen BLKRnin nasıl konuşlandırılacağı konusunda en önemli tek faktördür. AAA ilk önce hesaba katıldığında ağ erişimi ya doğrudan LANa bağlantılı aygıtlarıyla veya modem vasıtasıyla erişime ulaşan uzaktan erişim aygıtlarıyla kısıtlanmaktadır.

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

Çevirim Erişimi

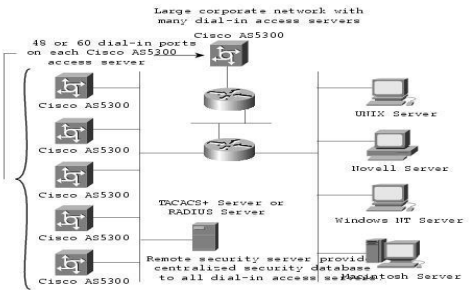
Çevirim erişimin geleneksel modelinde (bir PPP bağlantısı) bir modem veya Bütünleşik Servisler Dijital Ağ(ISDN) bağlantı kullanan bir kullanıcı bir NAS vasıtasıyla intanete erişimi onaylamaktadır. Kullanıcılar küçük bir işletmede tek bir NAS ile bağlantı kurabilmektedir veya birçok coğrafi olarak dağıtılmış 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.

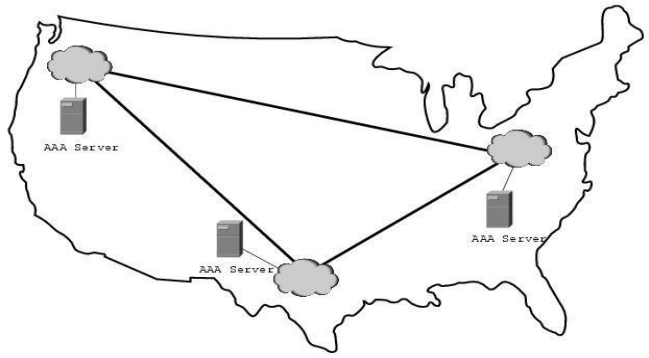
Şekil 2. Geniş Çevirim Ağı:



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 veritabanı kopyalama veya senkronizasyonu lüzumlu olabilmektedir. Bu ayrıca harici veritabanların kullanımıyla (NT veya kimlik kanıtlama için kullanılan Hafif Ağırlıktaki Dizin Erişim Protokolü [LDAP] gibi) ile güçleştirilebilmektedir.

Ilave 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:



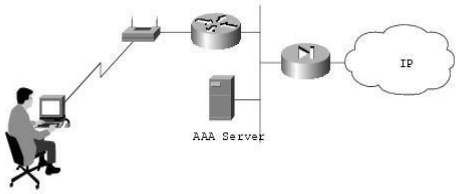
Kablosuz Ağ

Kablosuz ağ AAAya göre yenidir. Cisco Aironet® serisi gibi kablosuz erişim noktası (AP) gezgin istemciler için LANa köprülü bir bağlantı sağlamaktadır. Kimlik kanıtlama APye 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" LANdakine benzer şekilde kablosuz LANın (WLAN) mobilite faktörü çevirim ağı olarak benzer öneme sahiptir. "Kablolu" LANden farklı olarak bununla birlikte WLAN daha kolayca genişletilebilmektedir. WLAN teknolojisi bir AP vasıtasıyla bağlanan kullanıcıların sayısında fiziksel limitlere sahip olmamasına rağmen APlerin sayısı çabucak büyüyebilmektedir. 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.

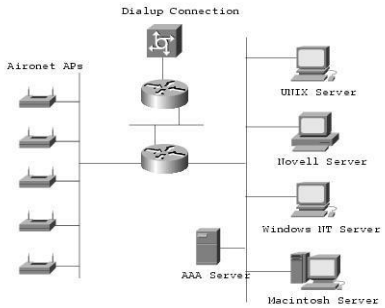
Bu WLANlarla birlikte eşsiz bir sonuç yetiştirmektedir: APler arasında “roam(dolaşım)” için bir kullanıcı kapasitesi.

Şekil 4. Basit WLAN:



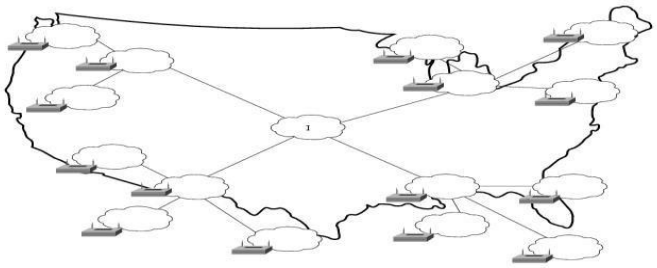
Basit bir WLANda tek bir AP kurulabilmektedir (Şekil 4). Sadece tek bir AP olduğu için birincil sorun güvenliktir. Bu ortamda genellikle küçük bir kullanıcı tabanı ve endişelenecek az ağ aygıtı vardır. Ağ üzerindeki diğer aygıtlara AAA servisleri sağlamak BLKR üzerindeki herhangi bir önemli ilave yüke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

Şekil 5. Yerleşke WLAN:



Bir WLAN içinde geniş bir bina veya yerleşke ortamında APlerin birkaçı konuşlandırıldığında (Şekil 5) BLKRnin nasıl konuşlandırılacağı hakkında kararlar daha karmaşık olmaktadır. Şekil 5 aynı LAN üzerindeki bütün APleri göstermesine rağmen yönlendiriciler ve anahtarlar vasıtasıyla bağlanan LAN boyunca dağıtılabilmektedir. WLANların daha geniş coğrafi dağıtımında BLKR konuşlandırma çevirim LANların geniş bölgesel dağıtımına benzerdir (Şekil 3). Bu özellikle bölgesel topoloji yerleşke WLAN olduğu zaman doğrudur. Bu model WLANlar daha çok basit WLANa benzeyen küçük sitelerin birçoğunda WLANlar konuşlandırıldığı zaman değişmeye başlar(Şekil 4). Bu model şehir veya eyelet boyunca ulusal veya evrensel olarak küçük mağaza zincirlerine uygulanabilirdir(Şekil 6).

Şekil 6. Küçük Sitelerin Geniş Konuşlandırması:



In the Şekil 6 model, the decision for kimlik kanıtlama from the BLKR depends on whether kullanıcıs from the bütün ağ need erişim on any AP or whether they only require regional or yerel ağ erişim. This factor, along ile veritabanı tipi, kontrols whether yerel or region BLKR kurulums are required and how

veritabanı continuity is maintained. In this very large deployment model, güvenlik becomes more complicated, too.

VPN Kullanarak Uzaktan Erişim

VPNler Internet veya dış Internetler (extranetler) gibi üçüncü parti ağlar üzerinden uçtan uça 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 kiralanmış 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.

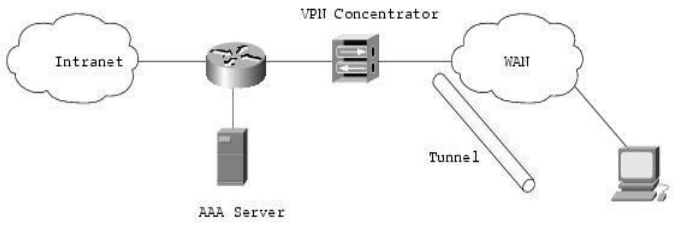
- **Güvenlik—**VPNler yetkisiz erişimden veriyi koruyan gelişmiş şifreleme ve kimlik kanıtlama protokollerini kullanarak en yüksek seviyede güvenlik düzeyi sağlamaktadır.

- **Ölçeklenebilirlik—**VPNler şirketlere ISPlerin 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 sağlarak ortak ağlarına erişimi elde ettiklerinde DSL ve kablo gibi yüksek hız, geniş bantlı bağlanırlılık avantajlarını mobil çalışanlarına, telecommuterlara (bilgisayar bağlantısı aracılığıyla iletişim kurarak evde çalışan insanlara) ve mesai çalışanlarına sağlamaktadır.

Şekil 7. Basit VPN Konfigürasyonu:



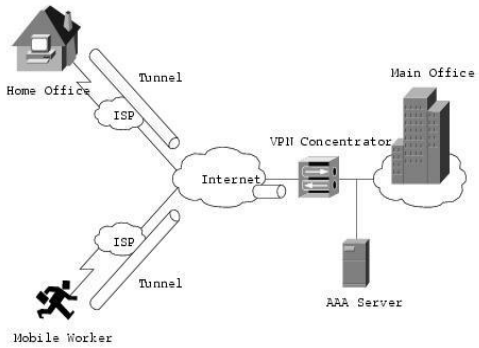
İki tip ağa erişim VPNleri vardır:

Siteden Siteye VPNler—Internet gibi genel bir ağ üzerinden uzaktan erişim ofisleri ve merkezi ofisler gibi çoklu sabit siteler arasında geniş-ölçekli şifreleme sağlayara 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 VPNler tipik bir WAN bağlantısı olarak değerlendirilebilmektedir ve güvenli başlangıç bağlantısına AAA genellikle kullanmak üzere konfigüre edilmemektedir. Bununla birlikte uzaktan-erişim VPNler 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 LANa veya LANdan dışardaki özkaynaklara (diğer deyişle, Internet) nasıl bağlanacağını tanımlamaktadır. Bu bağlantı birkaç yolda meydan 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 spesifisik ağ yönlendirme(erişim listeleri), günün her saatinde erişim, NAS erişim üzerindeki kişisel kısıtlamalar(erişim kontrol listeleri) gibi diğer kararları içermektedir ve böylece aynı zamanda BLKRnin 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 veritabanı bütün kullanıcı IDlerini, 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 (ACLler) 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 organizasyou 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 döküman aşağıdaki URLlerde 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/scdoverv.htm

Idari Erişim Politikası

Bir ağı yönetmek bir ölçek işidir. Ağr 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 veritabanı ve tek bir lokasyonda eklenebilen veya silinebilen yöneticiler için imkan sunmaktadır.

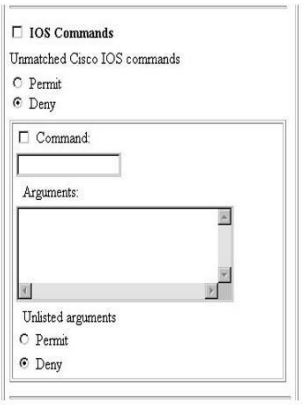
TACBLKR+ NAS idari erişimini kontrol etmek için tavsiye edilen bir NAS yöneticisinin aygıta erişiminin komut kontrolü başına (komut filtreleme) kapasitesinden dolayı AAA protokol seçeneğidir. Kimlik kanıtlama kabülü esnasında yetkilendirme bilgisinin tek-zamanlı transferinden dolayı RADIUS bu amaç için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

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

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 değişen spesifik komutların ayrıcalık düzeylerini gerektirmektedir ve spesifik ayrıcalık düzeyleri kullanıcı girişi için tanımlanmaktadır. Komut ayrıcalık düzeyi düzenleyerek aynı zamanda daha çok problemlere yol açmak oldukça kolaydır. BLKR üzerindeki komut filtrelemeyi kullanmak değişen kontrollü komutların ayrıcalık düzeyini gerektirmez. NAS ayrıştırılacak BLKRye 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 verdiğinden NAS filtreleme her NAS temeli üzerinde bu aygılara erişimi sınırlandırmak için kullanılabilmektedir.

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 BLKRnin kullanımı sanal bir gereksinim olmaktadır. Aygıtlarının birçoğunun yönetimi erişim düzeylerini çeşitlendirmekle daha çok sayıda yöneticilere gereksinim duymaktadır

Yerel kontrolün kullanımı yöneticileri ve aygıtlar değişirken gereken konfigürasyon değişiklerini 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 edebilldiği için BLKRnin desteklediği yöneticilerin sayısı bir mesele değildir.

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 almalıdır. Bu genel kullanıcı popülasyonunu idari takımdan izole edecektir ve yanlışlıkla ya da kazaren ağ aygıtlarına erişimi olasılığını azaltacaktır. Eğer uygun bir çözüm değilse uzaktan erişim ağına erişmek için RADIUS ve idari girişler içim (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 kazaran erişim ağ erişimine tesadüfi bozulmasına neden olabilir. Genel kullanıcıları idari kullanıcılardan ayırmak AAA ve BLKRnin 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. BLKRde 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 aygıta bağlanmak üzere yetkilendirilecektir. Bu BLKR üzerinde NASın 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 vee 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 aygıta 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 veritabanı tipi olmak üzere kullanılan tümü BLKRnin 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 kanıtlama sunucusunun kaybından dolayı yerel bir ağı erişilmez hale getirecektir.

Bu önemli noktaya ek olarak tek bir BLKRyi idare eden kullanıcıların sayısını azaltmak verilen herhangi bir zamanda meydana gelen girişlerin sayısını azaltarak veya kendi veritabanı üzerindeki yükü düşürerek performansı geliştirmektedir.

Kimlik kanıtlamanın Tipi

BLKR kimlik kanıtlama seçenekleri sayısını desteklemektedir. BLKRnin mevcut versiyonları altında seçenekler yerel BLKR veritabanı kullanımı, harici veritabanı yoluyla uzaktan erişimkimlik kanıtlama veya BLKR yerel veritabanıyla ilgili veritabanı yönetim sistemi (RDBMS) uzaktan erişim bir senkronizasyon içermektedir. Tablo 1 çeşitli seçenekleri ve mevcut teknik özellikleri göstermektedir.

Tablo 1. BLKR Veritabanı Seçmeli

Kimlik kanıtlama 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
AndaçlıSunucu (OTP)	X	X			
MCIS	X	X	X	X	X
Uzaktan erişimAAA Sunucusu	X	X	*	*	

* Eğer uzaktan erişim AAA sunucusu tarafından destekleniyorsa.

Her bir veritabanı seçeneği ölçeklenebilirlik and performans ile ilgili olarak kendi avantajları kadar sınırlamalara sahiptir.

Yerel Veritabanı

Tam teknik özellik desteği sağlamaktadır. Yerel veritabanını kullanarak kimlik kanıtlamanın maksimum hızını sağlamaktadır. Kullanılan veritabanı kopyalamasını en aza indirgeyen bölgesel ölçeklenebilirlik problemlere sahip olabilir. Bununla birlikte, kopyalama BLKR sistemleri arasında birincil/ikincil ilişki gerektirmektedir.

İkinci BLKR kurulum konfigürasyonu üzerinde birinci BLKR kurulumundan seçili konfigürasyon parçalarını kopyalarak tamamıyla ikinci üzerindeki konfigürasyon parçalarıyla yer değiştirerek AAA sunucularını senkronize tutmaktadır.

Bu ilk BLKR kurulumuna kullanıcı hesaplarının bakımını sınırlamaktadır. Diğer sakınca eğer bir organizasyonun kullanıcılar için mevcut veritabanı varsa, her iki veritabanı ayrı olarak bakımı yapılmalıdır.

Windows NT/2000 AD

İçinde dayanıklı Windows NT/2000 kullanıcı veritabanı zaten mevcut olan organizasyonlarda BLKR herhangi bir ilave giriş olmaksızın veritabanı oluştururken yatırım yapılan işi manivela edebilmektedir. Bu ayrı veritabanları için gereksinimi bertaraf etmektedir. NAS kullanıcı ismini BLKRye gösterdiğinde BLKR bir eşleştirme kurmak için veritabanını araştırmaktadır.

Eğer BLKR bir eşleştirme bulamazsa ve BLKR Windows NT/2000 kullanıcı veritabanını kontrol etmek için konfigüre edilebilirse kullanıcı ismi ve şifre Windows NT/2000 kullanıcı veritabanındakilere karşı kimlik kanıtlama için Windows NT/2000ye gönderilmektedir.

Eğer bir eşleştirme teyit edilirse kullanıcı ismi (fakat şifre değil) ilerdeki kimlik kanıtlama talepleri CiscoSecure kullanıcı veritabanında saklanmaktadır.

Daha sonraki kimlik kanıtlama talepleri daha hızlı doğrulayacaktır çünkü BLKR kimlik kanıtlama için doğrudan Windows NT/2000 kullanıcı veritabanına gitmaktedir. Grup gönderimi kullanıcı ayrıcalıklarında daha geniş esneklik vermektedir. Kullanıcı'Nin grubuna tahsis edilen yetkilendirme ayrıcalıkları henüz doğrulanmış kullanıcıya atanmaktadır. Birincil Domain (Tanım Kümesi) Denetçi (PDC) kullanarak güvenli bağıntıyla BLKR tarafından doğrulanabilen kullanıcıların sayısını büyütmektedir. Zaman aşımları, NT dağıtım ağındaki arasıra-halihazır atalet süresinden dolayı PDC güvenli bağıntıları kullanımında bir problem olabilir. Windows NT/2000 kullanıcı veritabanın karşı doğrulamadaki diğer problem üçüncü parti şifrelerin depolamasına izin vermemesidir. (Örneğin, Challenge Handshake Authentication Protocol [CHAP]).

Novell NDS veSoysal LDAP

BLKR LDAP ve Novell NetWare Dizini Servislerini (NDS) kullanan bir dizin sunucuda saklanan kayıtlara karşı kullanıcıların kimlik kanıtlamasını desteklemektedir. BLKR Novell ve Netscape içeren en çok popular dizin sunucularla etkileşmektedir.

Password Authentication Protocol (Şifre Kimlik Kanıtlama Protokolü) (PAP) ve şifresi belge şifreleri dizin sunucusuna karşı belgelenirken kullanılmaktadır. Bu servisler CHAP veya Microsoft CHAP (MS-CHAP) desteklemez. Ağ aygıtarını kullanmaya çalışırken bu protokollerden (diğer deyişle Cisco Aironet kablosuz)birini kullanmaya sınırlıysa bu bir mesele olabilir. Grup gönderimleri Windows NT veya 2000 ile mevcuttur.

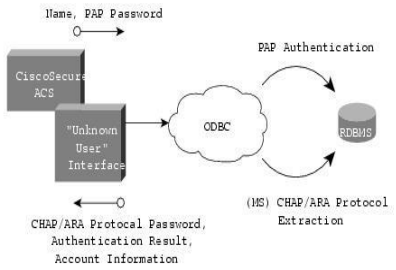
LDAP kimlik kanıtlama ile ilgili resmi broşür aşağıdaki web sayfasında mevcuttur:
http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/ldcsa_wp.htm

Açık Veritabanı Bağlanırlılığı

BLKR Açık Veritabanı Bağlanırlılığıyla (ODBC) uyumlu ilgili veritabanına karşı kimlik kanıtlamayı desteklemektedir. Bu mevcut kullanıcı kayıtlarının kullanımına olanak sağlamaktadır. ODBC ilk kez Microsoft tarafından geliştirilmiş standartlaşmış uygulama programlama arayüzüdür ve şu anda bir çok büyük veritabanı sağlayıcıları tarafından kullanılmaktadır. ODBC şimdi Structured Query Language (SQL) Erişim Grubunun özelliklerini takip etmektedir. Windows ODBC teknik özelliği veritabanı ile iletişim kurmak için diğer lüzumlu önemli parametreler ve veritabanını belirten bir Veri Source Name (DSN) oluşturmanıza olanak sağlar.

BLKR ODBC bağlantısıyla ilgili veritabanına kullanıcı bilgisini geçmektedir. İlgili veritabanı uygun tabloları sorgulayan ve CiscoSecure BLKRye geri dönen bellenmiş bir prosedüre sahip olmalıdır. Eğer sağlanan kullanıcı ismi ve şifreyi gösteren geri döndürülmüş değerler geçerli ise BLKR kullanıcı erişimini onaylamaktadır. Aksi takdirde BLKR kullanıcı erişimini tanımaz (Şekil 10). Şifre çıkartmaya izin veren ODBC özelliğinden dolayı ODBC şifresiz belge, PAP, CHAP, MS-CHAP, ve ARA Protokol şifrelerini doğrulayabilmektedir.

Şekil 10. ODBC Haricil Veritabanı Kimlik Kanıtlaması:



LDAP kimlik kanıtlama ile ilgili resmi broşür aşağıdaki web sayfasında mevcuttur:
http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/exatu_wp.htm.

RDBMS Senkronizasyonu

RDBMS senkronizasyonu NDS veya NT ile birlikte harici bir veritabanıyla uzakten erişim kimlik kanıtlama sağlamaz. Onun yerine, RDBMS senkronizasyonu (veya "dbsybc") bir ODBCnin-uyumlu ilişkisel veritabanından- yerel veritabanının uzak erişim konfigürasyonunu sağlamaktadır. Ayrı bir RDBMS veritabanı avantajları ve yerel veritabanıyla sağlanan tüm düzeydeki servislere olanak sağlamaktadır. “dbsync” SQL-tabanlı faturalama ve yönetim sistemine halihazırda sahip ve programlı şekilde veriyi BLKR konfigürasyonuna sevketmek isteyen gelişmiş istemci için tasarlandığı kaydetmeye değerdir.

Andaçlı(Token)Kart Sunucusu:

Ağların birçoğu tek-zamanlı şifre kimlik kanıtlama (OTP) için andaçlı (token) bir karta gereksinim duymaktadır. Bu yöntem çok güvenlidir fakat bazı ihtarları yapmak gerekir. İk önce, şifreli şifre protokolleriyle birleştirilemez (CHAP ve MS-CHAP). OTP yapısından dolayı ihtiyaç yoktur. Bununla birlikte LDAP ve NDS ile birlikte bu protokollerden birini kullanmaya sınırlı (diğer deyişle, Aironet kablosuz) Ag aygıtlarını kullanmaya çalışma mevzusundan dolayı bir probleme sebep olur. Diğer problem ise grup gönderimleri mevcut değildir. Andaçlı (token) kart sunucu olası ağ atalet süresi mevzularından dolayı BLKR kurulumuna uygun yakınlıkta konumlandırılmalıdır.

Uzaktan erişim AAA Sunucusu (Proxy):

Proxy(Vekil) otomatik olarak kimlik kanıtlama 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 profil 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, grub bilgisi yerel BLKR üzerinde sağlanmak zorunda değildir. Diğer avantajı ise organizasyon BLKR ile sınırlı değildir. Diğer sağlayıcıların AAA ürünleri kullanılabilmektedir. 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 tanmlı bir karakter dizinidir.) Diğer dezavantajı ise NAS filtreleme icra edilirken problem yaratmasıdır. İletilen BLKRnin NAS IP adresi talebi oluşturan NASın IP adresinden daha çok kullanılmaktadır.

Ağ Hızı ve Güvenilirliği:

Aynı zamanda ağ atalet süresini ilgilendiren ağ hızı ve ağ güvenilirliği BLKRnin nasıl konuşlandırılacağı konusunda önemli bir rol oynamaktadır. Kimlik kanıtlamadaki gecikmeler istemci tarafında veya NASta zaman aşımlarıyla 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 kanıtlama 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 BLKRyi 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 bi mesaj almaktan çok zaman aşımı problemlemiyle karşı karşıya kalmasıdır. NAS BLKR ile kontakt kurabilebilecektir fakatBLKR cevap için bir sure bekleyecektir ya da hiçbir şekilde cevap almayacaktır. Eğer BLKR uzaktaysa NAS zaman aşımına uğrayacak ve kullanıcıyı doğrulmak için alternatif bir yöntem deneyecektir fakat sonraki durumda muhtemelen kullanıcının istemci programı ilk önce zaman aşımına uğrar.

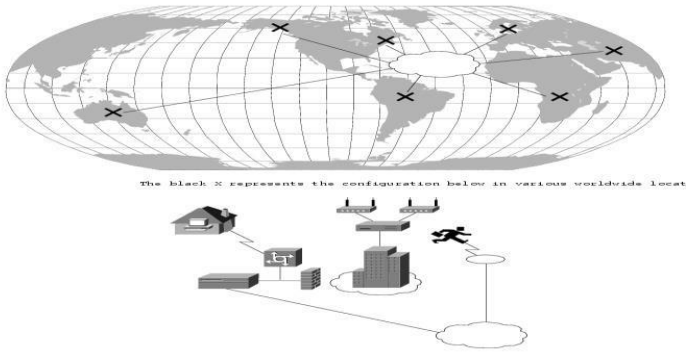
Gözden Geçirilmesi

BLKRnin 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 tabaı olarak gelişti ve erişim sunucularının lokasyonlarını AAA sunucusunun gerektirdiği daha çok kapasiteyle geniş çapta dağıtabilmekteydi. Bölgesel daha sonra global olarak gereksinimler yayygınlaştık. 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 kanıtlama 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 kullanımda 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 Amerikadaki BLKR ilk önce LDAP veritabanını kontrol etmelidir. Bu aynı zamanda Asyadaki NDS veritabanını kontrol etmek üzere konfigüre edilebilmektedir fakat bu veritabanına daha az talep olacağından harici veritabanı konfigürasyonundaki liste daha uzun olabilmektedir. Tersi de Asyadaki BLKR için geçerlidir. Eğer bölgeler ortak bir veritabanı paylaşıyorsa senkronize kurulumlar her bir bölgede konumlanmalıdır ve kendi BLKRleri 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 LANa zamanında erişime izin vermek üzere kullanılmaktadır.



Eğer bölgesel bir topolojinin merkezi bir "yerleşke"si 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 imkanı düşüktür ve erişim hızları tam vaktinde kimlik kanıtlamayı yönetmek üzere yeterli olmalıdır.

WEBUI Kabulleri:

Bu kitabın tümünde, menü opsiyonlarını ve linkleri seçmek yoluyla WebUI içersinde 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 menüsü[1]) fareyi **Addresses** üzerinde tutun.
   (DHTML menü) **Addresses** tıklayın
   Addresses seçeneği, bir seçenekler altkümesi 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 **opsiyonel**dir.
- Bağ parantez { } içersindeki her şey **gerekli**dir.
- 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 göründüğünde, **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, herhangibir 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.

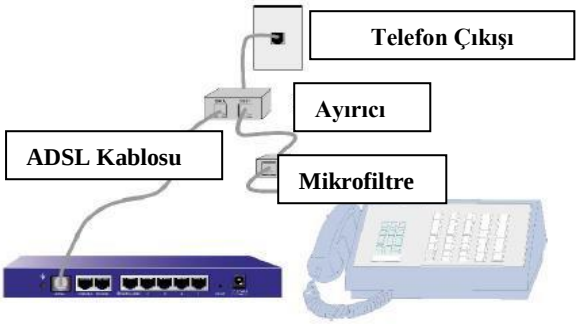
Ayırıcılar (Splitter) ve Mikrofiltrelerin Bağlanması:

Bir *sinyal ayırıcı* (signal splitter), telefon sinyalini, sesli çağrılar için düşük-frekanslı ses sinyallerine, veri trafiği içinse yüksek-frekanslı veri sinyallerine bölmektedir. Servis sağlayıcınız genellikle ayırıcıyı, telefon hatlarınızı 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, yanıtlama 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, yanıtlama 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 :

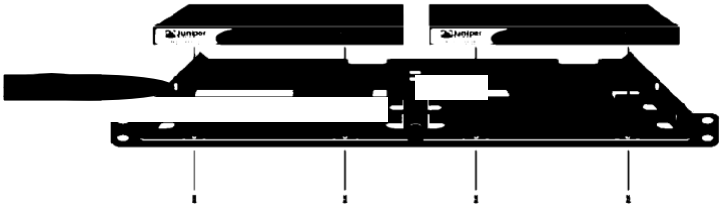
Genişlik:	48.26 cm.	19 inç.
Yükseklik:	4.013 cm.	1-5/8 inç. (1 askı ünitesi)
Derinlik:	33.655 cm.	13-1/4 in.

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 tepsiye sabitleyin.



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

Güç kabloları ile Ethernet kablolarını, tepsi tabanındaki açıklıklar içersinden 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.***

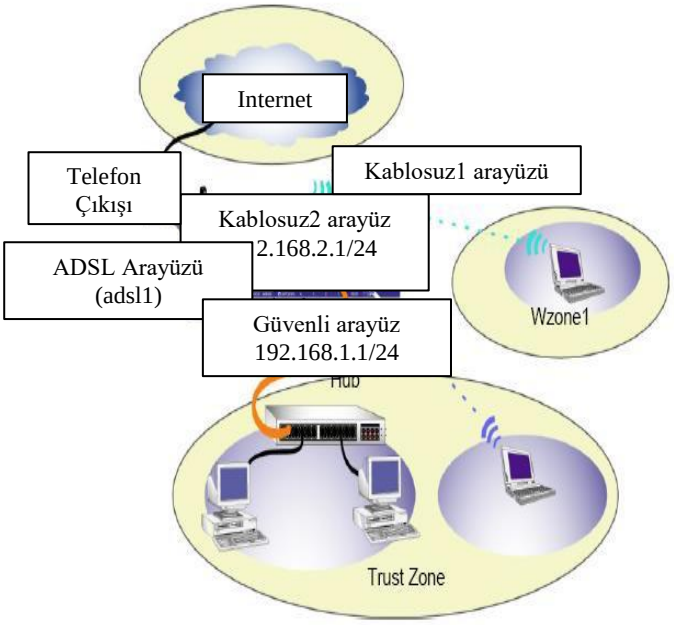
Aşağıdaki şekilde, Cisco Kablosuz ADSL cihazı için hazır konfigürasyon gösterilmektedir.

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).



Wzone1

WebUI’da,Cisco cihazı üzerindeki güncel aray Güvenli Bölge ni görmek için, Ağ > Arayüzs 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 netmask bulunabilir.

Not: *ADSL arayüzünü kullanmak istemiyorsanız, bunu,* ***set arayüz adsl1 zone null*** *komutu ile Boş (Null) bölgeye bağlayabilirsinz. 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 herhangibir 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 diğerinin 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 sağlayıcınız, 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 istemcilarını 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)
Kullanıciname: 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), boşta 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 > Arayüzs > 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]	
	Arayüz	**Bölge**
1	güvenli	Güvenli
2	güvenli	Güvenli
3	güvenli	Güvenli
4	güvenli	Güvenli
Güvensiz	güvensiz	Güvensiz
Modem[c]	seri	Boş
	kablosuz1	Wzone1
	kablosuz2	Güvenli

Ev-İş Port Modu	
Arayüz	**Bölge**
ethernet1	İş
ethernet1	İş
ethernet2	Ev
ethernet2	Ev
ethernet3	Güvensiz
seri	Boş
kablosuz1	Wzone1
kablosuz2	İş
kablosuz3	Ev

Güvenli/Güvensiz/DMZ (Genişletilmiş) Mod		**Dual Güvensiz Port Modu**		**Birleşik Port Modu**	
Arayüz	**Bölge**	**Arayüz**	**Bölge**	**Arayüz**	**Bölge**
ethernet1	Güvenli	ethernet1	Güvenli	ethernet1	İş
ethernet1	Güvenli	ethernet1	Güvenli	ethernet2	Ev
ethernet2	DMZ	Ethernet1	Güvenli	ethernet2	Ev
ethernet2	DMZ	ethernet2	Güvensiz	ethernet3	Güvensiz
ethernet3	Güvensiz	ethernet3	Güvensiz	güvensiz	Güvensiz
seri	Boş	seri	Boş	seri	Boş
kablosuz1	Wzone1	kablosuz1	Wzone1	kablosuz1	Wzone1
kablosuz2	Güvenli	kablosuz2	Güvenli	kablosuz2	İş
kablosuz3	DMZ			kablosuz3	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.
ve bölge bağları özetlenmektedir:

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	ethernet1	Güvenli
2	güvenli	Güvenli	ethernet1	İş	ethernet1	Güvenli
3	güvenli	Güvenli	ethernet2	Ev	ethernet2	DMZ
4	güvenli	Güvenli	ethernet2	Ev	ethernet2	DMZ
Güvensiz	güvensiz	Boş[c]	ethernet3	Boş[c]	ethernet3	Boş[c]
Modem	seri	Boş[c]	seri	Boş[c]	seri	Boş[c]
ADSL	adsl1	Güvensiz	adsl1	Güvensiz	adsl1	Güvensiz
	kablosuz1	Wzone1	kablosuz1	Wzone1	kablosuz1	Wzone1
	kablosuz2	Güvenli	kablosuz2	İş	kablosuz2	Güvenli
			kablosuz3	Ev	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.

Güvenlik duvarı cihazını İş-Ev port moduna değiştirmek için:

WebUI

Konfigürasyon > Port Mode: Aşağıya doğru uzayan listeden Ev-İş (Home-Work) tercihi yapın ve ardından **Apply**'a tıklayın.

Aşağıdaki ekran komutunda, **OK**'e tıklayın:

"Operational mode change will erase current konfigürasyon and reset the device, continue?"
(Operasyonel mod değişimi, güncel konfigürasyonu silecek ve cihazı sıfırlayacaktır. devam etsin mi?)

CLI

exec port-mode home-work

Aşağıdaki ekran komutunda, **y** (yes) ye basın:

Change port mode from <trust-untrust> to <home-work> will erase sistem konfigürasyon and reboot box
Are you sure y/[n] ? **y**