İleri Düzey Kurumsal Ağ Projesi #13

Güvenli Bir Şirket Ağı Sisteminin Tasarımı ve Uygulaması

Cytonn Innovation Ltd, müşterilerine dünya çapında yenilikçi bulut çözümleri sağlayan dinamik ve ileri görüşlü bir şirkettir. Şirket, işletmelerin değişen ihtiyaçlarına uygun bulut tabanlı çözümleri geliştirmek ve uygulamak için son teknolojiye ve yüksek nitelikli profesyonellerden oluşan bir ekibe sahiptir. Cytonn Innovation, operasyonel verimliliği, ölçeklenebilirliği ve rekabet gücünü artırmak için organizasyonlara güç vermeyi amaçlayarak yaratıcılık, çeviklik ve müşteri merkezliliğine güçlü bir vurgu yapmaktadır.

600 kişilik bir iş gücüne sahip olan Cytonn Innovation Ltd, yakın zamanda genişleyerek yeni bir binaya taşınma hazırlığı yapmaktadır. Üç katlı bu yeni bina, Satış ve Pazarlama, İnsan Kaynakları ve Lojistik, Finans ve Muhasebe, İdare ve Halkla İlişkiler, BİT (Bilişim Teknolojileri) ve bir Sunucu Odası gibi çeşitli departmanlara ev sahipliği yapacaktır. BİT departmanı ayrıca Yazılım Geliştiriciler, Bulut Mühendisleri, Siber Güvenlik Mühendisleri, Ağ Mühendisleri, Sistem Yöneticileri, BT Destek Uzmanları, İş Analistleri ve Proje Yöneticileri gibi profesyonelleri de barındırmaktadır.

Taşınma öncesinde, yeni binada bir ağ hizmetinin tasarlanması ve uygulanması gerekmektedir. Güçlü bir güvenlik sağlamak için Cytonn Innovation, dahili ve harici tehditlere karşı ağı korumak için birkaç güvenlik önlemi uygulayacaktır. Güvenlik duvarı dış, iç ve DMZ güvenlik bölgelerine sahip olacak ve temel sunucular bu tahkim edilmiş alan içerisinde stratejik olarak yerleştirilecektir. Ek olarak, kullanıcıları, bilgisayarları ve ağ içerisindeki kaynakları yöneten ve kimlik doğrulamasını sağlayan Active Directory (AD) sunucuları güvenlik duvarının iç kısmında yer alacaktır. DHCP, DNS ve Radius gibi hizmetleri sağlayan önemli sunucular güvenlik duvarının iç kısmında yer alırken, FTP, WEB, E-posta, Uygulama ve NAS depolama gibi diğer sunucular DMZ'de yer alacak olup, şimdilik herhangi bir güvenlik duvarına bağlanabilir. Bu titiz planlama ve güvenlik önlemlerinin uygulanması, Cytonn Innovation Ltd'nin yeni binadaki operasyonlarını güvence altına alacak ve sorunsuz bir geçiş sağlayacaktır.

BİT altyapısının ayrılmaz bir parçası olarak aşağıdaki bileşenler dahil edilmiştir:

a) **İnternet Servis Sağlayıcısı (ISS):** Üniversite, iki ISS (SEACOM & Safaricom) ile abonelik kurmuş olup yedekli internet bağlantısını sağlamaktadır.

b) **Ağ Güvenliği:** 5500-X serisi iki adet Cisco ASA güvenlik duvarı, ağ güvenliği ve yedekliliği artırmak için satın alınmıştır.

c) **Ağ Yönlendirmesi:** Hem güvenlik duvarları hem de çekirdek anahtarlar için yönlendirici yerine anahtarlar kullanılacaktır.

d) **Anahtarlama Altyapısı:** Şirket, birincil iletişim için Catalyst 3850 48-Port Anahtarlar ve Catalyst 2960 48-Port Anahtarlar kullanarak ağ kurulumunu tamamlamıştır.

e) Sunucu Donanımı ve Sanallaştırma:** Sanallaştırma yoluyla çeşitli hizmetler için birden fazla sanal makine elde etmek amacıyla iki fiziksel sunucu kullanılacaktır.

f) Kablosuz Altyapı:** Bir Cisco Kablosuz LAN Denetleyicisi (WLC) ve çeşitli Hafif Erişim Noktaları (LAP'ler) kablosuz ağın yönetimini merkezileştirecektir.

g) VoIP veya IP Telefonları:** Ağda telefon hizmetini sağlamak için bir Cisco Ses Geçidi kullanılacaktır.

Bulut bilişim, dünya genelindeki müşterileri şirketin hizmetlerine ve kaynaklarına bağlamak için önemli bir teknoloji olarak kullanılmaktadır. Bu nedenle, önerilen ağın ekibin bu kaynaklara erişimini sağlaması gerekir.

Bu nedenle, Ağlar Ekibinin kilit bir üyesi olarak, size yeni bina için bir ağ tasarlama görevi verilmiştir. Bu aşamada, ağın mevcut iş gereksinimlerini karşıladığından ve geleceğe yönelik koruma sağladığından emin olmak için gerekli önlemleri gösteren mantıksal bir tasarım gereklidir.

Gereksinimler:

Şirket, ağ altyapısında en üst düzeyde performans, yedeklilik, ölçeklenebilirlik ve erişilebilirliği sağlama konusunda büyük bir vurgu yapmaktadır. Bu nedenle, göreviniz kapsamlı bir ağ tasarımı oluşturmak ve uygulamasını gerçekleştirmektir. Bu çabayı kolaylaştırmak için Üniversite, belirli IP adresi aralıklarını tahsis etmiştir:

- **Yönetim Ağı:** Yönetim için 192.168.10.0/24 IP adresi aralığı tahsis edilmiştir.
- **WLAN:** WLAN ağı, 10.20.0.0/16 IP adresi aralığında çalışacaktır.
- **LAN:** Yerel ağ (LAN) için 172.16.0.0/16 IP adresi aralığı ayrılmıştır.
- **VoIP:** Yerel alan ağı (LAN) için 172.30.0.0/16 IP adresi aralığı tahsis edilmiştir.
- **DMZ:** Korunmuş Bölge (DMZ) için 10.11.11.0/27 aralığında IP adresleri atanacaktır.
- **Genel Adresler:** SEACOM ve Safaricom'dan 105.100.50.0/30 ile 197.200.100.0/30 aralığındaki genel IP adresleri atanacaktır

Teknik Gereksinimler:

1. **Tasarım Aracı:** Ağ çözümünü tasarlamak ve uygulamak için Cisco Packet Tracer kullanılacaktır.
2. **Hiyerarşik Tasarım:** Ağ dayanıklılığını artırmak için yedeklemeyi içeren hiyerarşik bir model uygulayın.
3. **ISS'ler:** Ağ altyapısında iki ISS'ye bağlantı sağlanacaktır.
4. **WLC:** Her departmanın, çalışanlar, kurumsal kullanıcılar, dış denetçiler ve misafirler için merkezi olarak Kablosuz LAN Denetleyicileri (WLC) tarafından yönetilen bir Kablosuz Erişim Noktası (WAP) ile donatıldığından emin olunacaktır.
5. **VLAN:** Aşağıdaki kimliklerle VLAN'lar korunacaktır: Yönetim için 10, LAN için 20, WLAN için 50, VoIP için 70 ve kullanılmayan tüm portların yerleştirildiği Blackhole için 199.
6. **EtherChannel:** Link Aggregation Control Protocol (LACP) kullanarak EtherChannel yapılandırmasını uygulayın ve bağlantı toplama verimliliğini artırın.
7. **Telefon Hizmeti:** Ses geçidi yönlendirici üzerinde VoIP yapılandırın ve arama numaralarını 4.. biçiminde tahsis edin.
8. **STP PortFast ve BPDUGuard:** Spanning Tree Protocol (STP) PortFast ve BPDUGuard'ı yapılandırarak portların bloklama durumundan iletim durumuna geçişini hızlandırın.
9. **Alt Ağ Oluşturma:** Her ağ grubuna uygun sayıda IP adresi tahsis etmek için alt ağ oluşturma tekniklerini kullanın.
10. **Temel Ayarlar:** Cihazların temel ayarlarını yapılandırın, buna ana bilgisayar adları, konsol parolaları, etkin parolalar, mesajlar, parola şifreleme ve IP domain lookup'ı devre dışı bırakma dahil.
11. **VLAN'lar Arası Yönlendirme:** Tüm departmanlardaki cihazların VLAN'lar arası yönlendirme için çok katmanlı anahtarı yapılandırarak birbirleriyle iletişim kurmalarına olanak sağlayın.
12. **Çekirdek Anahtarı:** Yönlendirme ve anahtarlama işlevlerini sağlamak için çok katmanlı anahtarlara IP adresleri atayın.
13. **DHCP Sunucusu:** Ağdaki tüm cihazların, sunucu çiftliği sitesinde bulunan DHCP sunucularından dinamik olarak IP adresi almasını sağlayın.
14. **HSRP:** Yük dengeleme, yedekleme ve geçiş yeteneklerini sağlamak için HSRP gibi yüksek kullanılabilirlik yönlendirici protokollerini uygulayın.
15. **Statik Adresleme:** Sunucu odasında bulunan cihazlara statik IP adresleri atayın.
16. **Yönlendirme Protokolü:** Güvenlik duvarı, yönlendiriciler ve çok katmanlı anahtarlarda rotaları tanıtmak için OSPF'yi kullanın.
17. **SSH için Standart ACL:** Üst düzey Ağ Güvenliği Mühendisliği PC'sinde yalnızca SSH yoluyla uzaktan yönetim görevlerine izin vermek için basit bir standart Erişim Kontrol Listesi (ACL) kurun.
18. **Cisco ASA Güvenlik Duvarı:** Ağda erişim kontrolünü ve kaynak kullanımını tanımlamak için güvenlik duvarında varsayılan statik rotaları, temel ayarları, güvenlik seviyelerini, bölgeleri ve politikaları yapılandırın.
19. **Son Test:** Tüm öğelerin amaçlandığı gibi çalıştığından emin olmak ve düzgün iletişimi doğrulamak için kapsamlı bir test uygulayın.