EXAMENSARBETE

Uppbyggnad av virtuellt nätverk hos Atea Sverige AB

Robin Andersson Rahkonen
Patrik Bromark
2016

Högskoleexamen
Datornätverk

Luleå tekniska universitet
Institutionen för system- och rymdteknik

LULEÅ TEKNISKA UNIVERSITET

Robin A Rahkonen
Patrik Bromark

Examensarbete, D0032D
LTU Skellefteå
Instritutionen för System- och rymdteknik
VT 2016

Uppbyggnad av virtuellt nätverk hos Atea Sverige AB

Sammanfattning

En virtuell miljö, bestående av sex kontor och ett datacenter, skulle planeras och presenteras. En lista med krav från ett fiktivt företag skulle följas, till bästa förmåga, och förslag på lösningar skulle tas fram. Test på olika lösningar utfördes till stor del i virtuell miljö, och de funktioner som ej gick att testas virtuellt utfördes på fysiska enheter.

Två lösningar, en till de större kontoren där redundans och driftsäkerhet var prioritet, och en lösning till de mindre kontoren, där kostnaden för redundans blev för hög i jämförelse med fördelarna med en sådan lösning, togs fram.

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Atea är ett IT-företag specialiserat inom it-infrastruktur och har kunder i hela Sverige. Examensarbetet som dokumenterats i denna rapport utfördes på Atea Skellefteå.

1.2 Syfte

Syftet med detta examensarbete var att simulera en verklighetstrogen företagsmiljö bestående utav 6 st. kontor av varierande storlek. Utöver kontoren fanns även ett datacenter med ett antal servrar som kontoren behövde åtkomst till.

En lista innehållandes det fiktiva företagets krav och specifikationer gavs ut, för att få en förståelse av vad företaget krävde av sina kontorsnätverk.

- Företaget jobbar 07:00-16:00, dvs ingen shiftgång etc.
- Ni är även ISP, dvs har tillgång till kopplingarna mellan orterna.
- Lämplig redundans ska finnas på alla nivåer.
- Respektive trafik ska segmenteras på Layer 2 nivå.
- Kunden använder Office365 och dess tjänster.
- Tillgång till trådlöst gästnät med centralt automatiskt genererat månadslösenord ska finnas på alla orter.
- Mobiltelefoner används på alla orter och ska ha möjlighet till internetaccess.
- Skrivarna är upplagda på servrar i datacentret.
- Produktionsmaskiner ska segmenteras och ha fast IP-address.
- Minimalt antal externa IP-addresser ska användas.
- Övervakning och managering av nätverk ska ske från datacentret.
- Uppkopplingsmöjligheter från utsidan, t. ex. hemifrån, flygplats etc.
- Säkerhet har hög prioritet hos kunden.
- Krav på driftsäkerhet och hög prestanda.

I slutändan skulle fyra saker presenteras:

- Ett dokument som förklarar hur vi uppnått kraven på kravlistan.
- En nätskiss med tillhörande IP-planering. (Bilaga 1 för IP-planering, bild 2 samt 3 för nätskiss över kontor)
- Konfigurationsfiler för de olika nätverksenheter som konfigurerats. (Bilaga 2)
- En utrustningslista innehållande alla nätverksenheter för alla kontor, samt en prislista på utrustningen. (Bilaga 3)

2. Teori och ordlista

I detta kapitel beskrivs begrepp som kommer att användas i rapporten.

2.1 VPN

VPN står för Virtual Private Network och används för att koppla ihop två nätverk över exempelvis Internet. Med hjälp av detta så kan man bland annat utnyttja interna resurser på ett avlägset nätverk. Trafiken skickas då genom krypterade “tunnlar” mellan nätverken, vilket förhindrar avlyssning av trafiken som skickas.

2.2 RADIUS-server

RADIUS står för Remote Authentication Dial-In User Service och är ett nätverksprotokoll som hanterar:

- Authentication (verifiering) används för att identifiera vem som loggar in, oftast med hjälp av att användaren loggar in med ett användarnamn och lösenord.
- Authorization (behörighet) bestämmer vad användaren har tillgång till på nätverket.
- Accounting (redogörelse) övervakar hur länge användaren varit ansluten, vilka resurser som använts etc. Denna information kan sedan användas för t. ex. analysera trender i nätverket, fakturering m.m.

Detta kallas med en kortare term AAA. RADIUS-servern använder sig utav detta protkoll för att säkert tillåta användare att verifiera och ansluta sig mot diverse nätverkstjänster. [1]

2.3 WAN

WAN står för Wide Area Network och är ett nätverk, oftast bestående av två eller fler LAN, som är så stort att det omfattar ett större område, exempelvis ett land. Företag, skolor och regeringar kan till exempel använda sig utav detta för att skicka trafik mellan anställda, studenter, kunder, köpare och säljare. Internet kan anses vara ett stort WAN. [2]

2.4 VLAN

VLAN står för Virtual Local Area Network och används för att dela upp nätverket virtuellt, även om de olika nätverken delar samma fysiska nät. Detta kan användas för att bland annat minska broadcastdomäner, segmentera trafik, och öka säkerheten i nätverket. [3][10]

2.5 GNS3

GNS3 står för Graphical Network Simulator-3, och är ett program som används för att simulera nätverksenheter.
Detta program användes för att testa de olika lösningarna för kontoren.
Har ej stöd för avancerad konfiguration utav switchar, vilket begränsar tester av vissa delar i nätverket.

2.6 STP

STP står för Spanning-tree protocol och används utav switchar för att förhindra att trafik fastnar i en “loop”. Detta görs genom att stänga ned en länk så att det ej finns möjlighet att detta sker. De avstängda länkarna kan återaktiveras vid behov, vilket skapar redundans på nätverket.
[4][5][6][7][10]

2.7 PVST

PVST står för Per-VLAN Spanning Tree och har samma funktionalitet som STP, men har ett eget spanning-tree för varje VLAN. [3][10]

2.8 ASA

ASA står för Adaptive Security Appliance och är en brandvägg framtagen av Cisco som är väldigt populär hos företag då den är enkel att sätta upp och har de viktigaste funktionerna som krävs av en brandvägg.

2.9 L3-switch

L3-switch är en lager 3-switch, vilket är en switch som har tillgång till router-funktioner. Fördelen med dessa är att de har ett stort antal portar i jämförelse med en router, som ofta enbart har ett fåtal portar. Detta möjliggör mer avancerade nätverkslösningar samt minskar antalet nätverksenheter i nätverket då den kan agera både router och switch.

2.10 VRRP

VRRP står för Virtual Router Redundancy Protocol, där två eller fler routrar arbetar som en grupp, som en enda virtuell router, och skapar därmed redundans. Detta görs genom att gruppen endast har en master router, där resterande routrar i gruppen är backup routers. Om master routern skulle gå ned, så tar en backup router över och delar ut en ny väg genom nätverket utan att det resterande nätverket märker någon skillnad. [8][10]

2.11 GLBP

GLBP står för Gateway Load-Balancing Protocol, där en grupp bestående utav två eller fler routrar arbetar tillsammans, och gör så att det resterande nätverket endast ser dessa som en enda virtuell router. En AVG (Active Virtual Gateway) utses för varje grupp, som sedan delar ut samma virtuella MAC adress till alla medlemmar inom gruppen. Alla routrar inom gruppen med en virtuell MAC adress kallas AVF (Active Virtual Forwarders) och ansvarar för att skicka vidare paket som tas emot via den virtuella adressen. Detta skapar både redundans och lastbalansering inom gruppen. [10]

3. Metod

För att testa de olika lösningarna användes GNS3, ett program där simulering av nätverksenheter är möjligt. Med hjälp av detta program, togs större delen av konfigurationen fram. Utöver simulering användes även fysisk utrustning för att testa funktioner som ej gick att simulera i GNS3.

Modellen som användes för att ta fram en struktur för kontoren var Cisco:s “Core-Distribution-Access” modell, även kallad den hierarkiska nätverksmodellen. [9] Modellen var till grund för hur kontorens nätverksstruktur byggdes upp, och små justeringar till modellen gjordes efter behov.

En gång i veckan diskuterades lösningen med handledare, och ibland även Ateas nätverkstekniker, som såg till att arbetet gick åt rätt håll. Detta gjordes genom att gå igenom tankar och idéer, eventuellt få förslag på förbättringar, samt få hjälp med diverse oklarheter kring kravlistan.

4. Resultat

4.1 Nätverksstruktur

Efter att ha gjort planering för varje kontor, kunde två olika strukturer användas för varje kontor, beroende på storlek.

De stora kontoren, Skellefteå, Luleå och Östersund, strukturerades så att redundans fanns mellan alla lager i hierarkin. (*Se bild 2*). “L3-1” och “L3-2” agerade som default-gateways för de interna nätverken och använde sig utav VRRP, så att om en skulle gå ned så kan den andra ta över tills problemet blivit fixat.

På de mindre kontoren, Kiruna, Visby och Piteå, behövdes ej samma redundans som på de större kontoren. Eftersom kravlistan specificerat att *lämplig* redundans skulle finnas, så fick det varken finnas för mycket eller för lite redundans. (*Se bild 3*).

4.2 Lastbalansering

Eftersom PVST används så kunde justeringar göras så att “L3-1” och “L3-2” blev root-bridges och secondary root-bridges för de olika vlanen.
L3-1 är den primära root-bridgen för vlan 10, 30 och 50.
L3-2 är den primära root-bridgen för vlan 20, 40 och 60.
Detta gör så att spanning-tree stänger ned korrekt länkar utan att någon ytterligare konfiguration behöver göras.

4.3 Redundans

Mellan Core (ASA) och Distribution (L3) så används “floating static routes” för att uppehålla redundansen om en länk eller enhet skulle gå ned. Detta innebär att ASA:n vet om en annan väg ner till det interna nätverket, men använder bara denna väg om den primära vägen inte finns tillgänglig.

Detta, i samarbete med PVST och VRRP, gjorde att nätverket kunde fortsätta fungera även om en nätverksenhet skulle gå ned.

4.4 Nätverken

Produktion är en avdelning av nätverket där datorer och annan nätverksutrustning finns som ej ska ha internetåtkomst, utan behöver enbart ha tillgång till det interna nätet. Det enda undantaget för åtkomst utifrån är datacentret, som har tillgång till produktionsnätverket för att kunna övervaka enheter. Detta gjordes via access-listor i brandväggen, som blockerar all trafik utifrån att ta sig till produktionsnätverket, med datacentret som undantag.

Arbetsplats är arbetsplatserna på kontoret. Det skulle även finnas IP-telefoner vid vissa arbetsplatser och datorerna har även mjukvara för IP-telefoni.

En telefoniserver i datacentret tillhandahåller all IP-telefoni för alla kontor, där alla telefoner tilldelas både IP-adresser samt telefonnummer.

Utöver det som visas på bilderna finns det även accesspunkter på varje kontor. Två trådlösa nätverk skulle finnas, ett trådlöst nätverk för de som arbetar på kontoret och ett trådlöst nätverk för gäster. Inbyggt i Lager 3-switcharna finns det en “wireless controller”, som används för att kontrollera accesspunkterna.

Gästnätverket har ej tillgång till det interna nätet, utan kan bara användas för att ta sig ut på internet. Detta kontrollerades via access-listor i distributions-lagret. Utöver det så skulle ett nytt lösenord till gästnätverket automatiskt genereras en gång i månaden. Detta löstes via en RADIUS server i datacentret, där ett skript körs en gång i månaden. Detta skript genererar ett nytt lösenord för gästnätverket på alla kontor och mailar sedan det nya lösenordet till lämplig personal på varje kontor.

4.5 Utrustning

Den utrustning som används på kontoren är följande:

- “Cisco ASA 5505 Firewall” agerar gateway mot internet.
- “Cisco 2960 Lager 2 Switch” finns på de större kontoren i access-lagret.
- “Cisco 3650 Lager 3 Switch” finns på alla kontor och kan hittas i distributions-lagret. På de mindre kontoren agerar denna även som access.
- “Ubiquiti Unifi AP-AC Lite” är den typ av accesspunkt som finns lokerad på varje kontor. Dessa fungerar som access-lagret för de trådlösa nätverken.

Med dessa tre typer av nätverkenheter kunde kontorens nätverksstruktur byggas upp. Totalt för alla kontor behövdes det:

- 9 st. ASA-brandväggar
- 9 st. Cisco 3650 L3 switchar
- 8 st. Cisco 2960.L2 switchar
- 12 st. accesspunkter

Antalet accesspunkter varierar beroende på den fysiska storleken på kontoret. Eftersom att detta är en generell lösning, där den fysiska storleken på kontoren ej behandlas, så beräknas två accesspunkter per kontor, en för varje trådlöst nätverk.

4.6 VPN

Ett av kraven i kravlistan var att ett minimalt antal externa IP-adresser skulle användas. Då datacentret har ett flertal servrar som kontoren behöver ha åtkomst till, så sattes en site-to-site VPN upp för att enkelt komma åt de interna resurserna som datacentret tillhandahåller.

Alla kontor har en site-to-site VPN till datacentret. Varje kontor har en unik intern adressrymd, detta för att datacentret skall kunna urskilja kontoren från varandra.

Utöver site-to-site VPN så sattes även en Clientless VPN upp på samtliga brandväggar på alla kontor, vilket möjliggör åtkomst till det interna nätverket från till exempel hemmet. Användare som ansluter sig via denna VPN autentiseras mot en RADIUS server som finns i datacentret.

4.7 Övervakning

Övervakning och administration av nätverken på samtliga kontor sker från datacentret. Denna lösning utnyttjar site-to-site anslutningen för att få åtkomst till kontorens interna resurser. Administration av nätverksenheter från datacentret sker via SSH med inloggning, där varje nätverksenhet har en användare sparad lokalt.[10]

5. Diskussion

Eftersom en del nätverksenheter, som t.ex. ASA, accesspunkter och switchar, ej simuleras korrekt eller helt enkelt ej går att simulera i GNS3, är det ingen garanti på att alla de lösningar vi tagit fram fungerar. De flesta lösningarna har testats i mindre miljöer eller vid tidigare tillfällen, och mycket information om hur enheter fungerar har fått hämtats från internet.

Konfigurationen är inte helt färdigställd, så pass att den är optimerad och redo att bara implementeras på ett kontor, men den stora helheten finns där. Mindre, men ändå viktiga, saker såsom till exempel traps till övervakningen kunde ha skrivits in. En annan sak vi kunde implementerat var portfast i access-lagret, mot alla arbetsplatser.

På de stora kontoren följer strukturen i stort sett Cisco:s hierarki. En av skillnaderna vi gjorde var att vi ej har länkar mellan L3-switcharna i Dist och brandväggarna i Core. (Se bild 1)

Anledningen till att vi tog bort denna länk var att det var minimalt med trafik som skulle gå regelbundet över den länken. Det är självklart möjligt att ha en länk mellan dom med rätt spanning-tree konfiguration, men vi valde att göra det lite enklare att ha en bild över vilken väg trafik kommer gå genom nätverket.

Det sistnämnda är även en av anledningarna till att VRRP valdes över GLBP (Gateway Load Balancing Protocol). GLBP skulle ha möjliggjort dynamisk lastbalansering mellan de två L3-switcharna, men vi ville som sagt ha lite mer kontroll över trafiken och vilket VLANs trafik som gick var. Utöver detta hade vi ej möjlighet att testa GLBP tillräckligt mycket för att vara säkra på att det skulle fungera korrekt.

En av de tidigare lösningarna vi hade var att skapa ett WAN mellan alla kontoren och datacentret. I denna lösning gick alla kontorens trafik ut mot internet via huvudkontoret i Skellefteå, som hade extra utrustning för att hantera den stora datamängden. (Se *bild 3*) Fördelen med denna lösning var att alla kontoren enkelt kunde komma åt de andra kontorens och datacentrets interna resurser.

Nackdelen, och anledningen till att idén skrotades, var att i kravlistan stod det specificerat: “Kunden använder Office365 och dess tjänster”.
Detta betyder att kunden använder sig utav molntjänster som finns ute på internet. För att dessa ska fungera bra, så vill man ha minimal fördröjning till de servrar som tillhandahåller molntjänsterna. I WAN lösningen behövde kontor som till exempel Visby skicka sin trafik ända upp till Skellefteå, för att sedan skickas vidare till exempelvis Tyskland, varpå trafiken måste tillbaka upp till Skellefteå innan den slutligen hamnar i Visby. Detta var därför ej en optimal lösning för denna kund.

Referenser

1. John Vollbrecht, The Beginnings and History of RADIUS, 2006.
2. Groth, David, Skandier, Toby. (2005).Network+ Study Guide, Fourth Edition. Sybex.
3. Virtual Bridged Local Area Networks, IEEE standard 802.1Q, 2005.
4. Decker, Langille, Rijsinghani, McCloghrie. (1993). Definititions of Managed Objects for Bridges, RFC 1493, IETF.
5. Decker, Langille, Rijsinghani, McCloghrie. (1993). Definititions of Managed Objects for Source Routing Bridges, RFC 1525, IETF.
6. Bell, Smith, Langille, Rijhsinghani, McCloghrie. (1999). Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, RFC 2674, IETF.
7. MAC Bridges Standard, IEEE standard 802.1D, 2004.
8. Nadas. (2010). Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6, RFC 5798, IETF.
9. *High Availability Campus Network Design* (PDF) http://www.cisco.com/application/pdf/en/us/guest/netsol/ns431/c649/ccmigration_09186a00808f6c34.pdf
10. Froom, Richard, Sivasubramanian, Balaji och Frahim, Erum. (2010). *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning Guide.* Cisco Press.

Bilagor

Bilaga 1

Se separat dokument Atea IP-Planering.

Bilaga 2

Se separat dokument Atea Konfiguration.

Bilaga 3

Se separat dokument Atea Utrustningslista+Prislista.

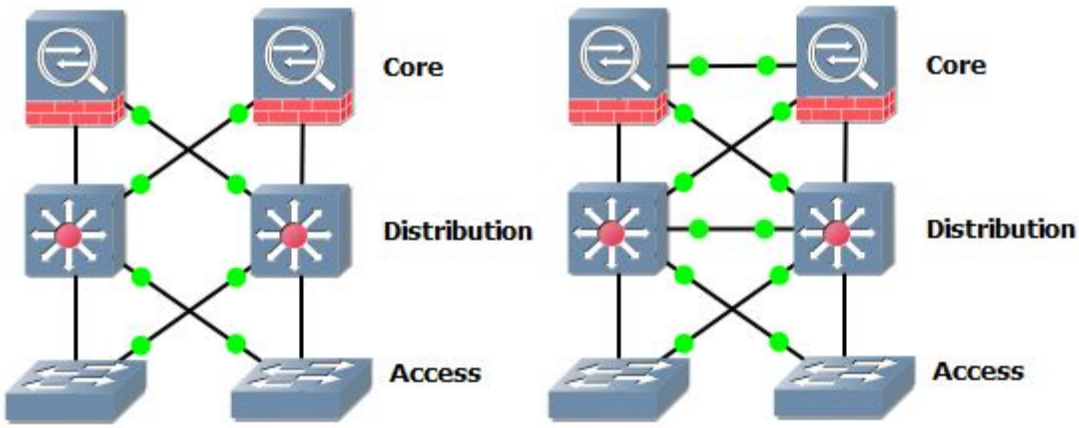

Bild 1. Lösning för Atea (till vänster) och Ciscos hierarki (till höger).

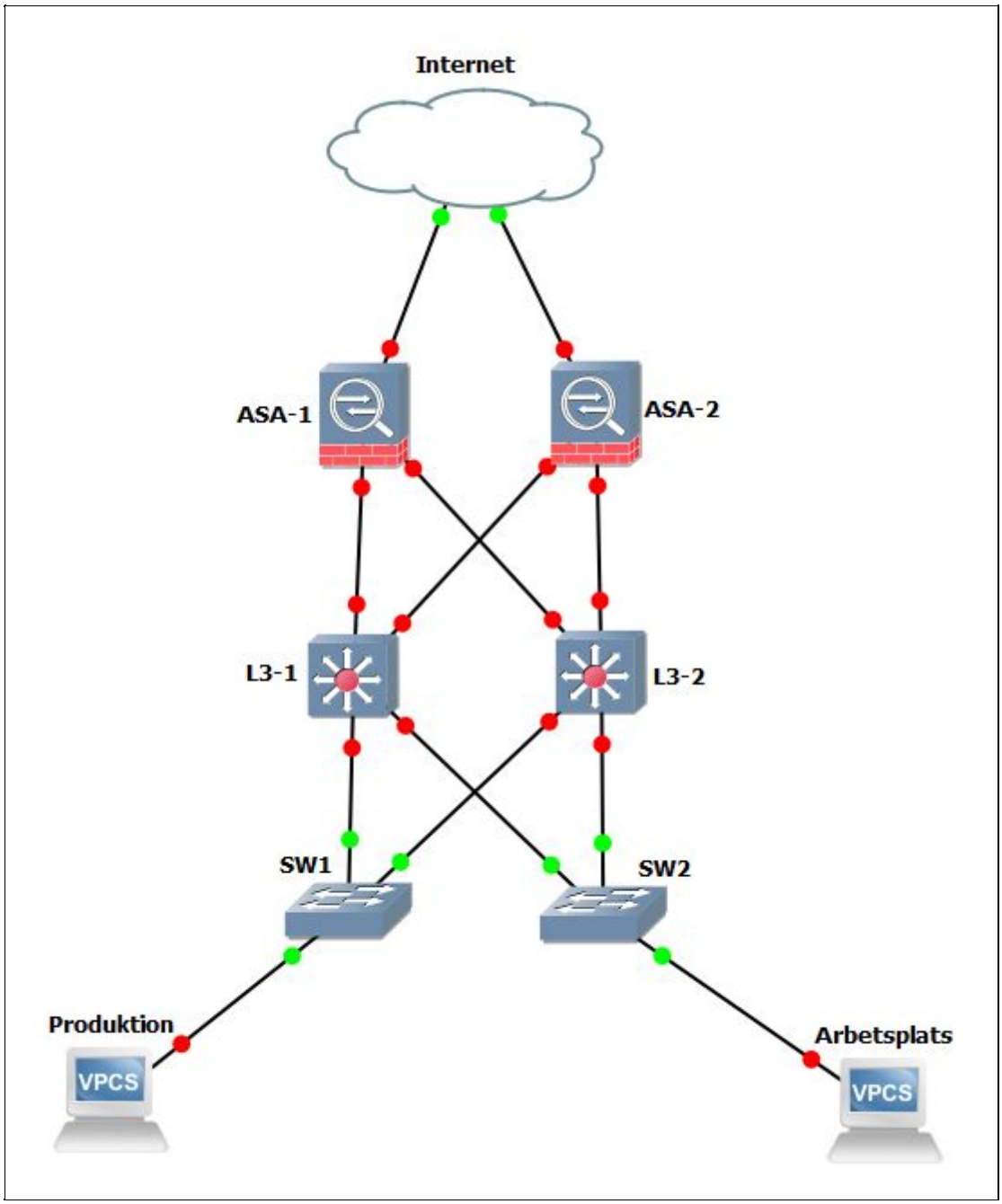

Bild 2, stort kontor.

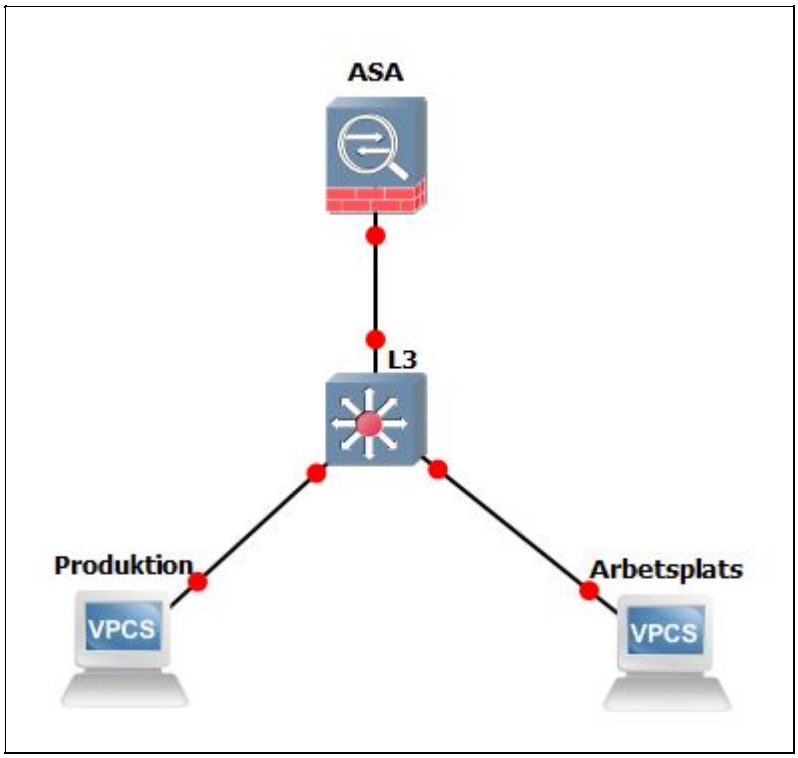

Bild 3, litet kontor.

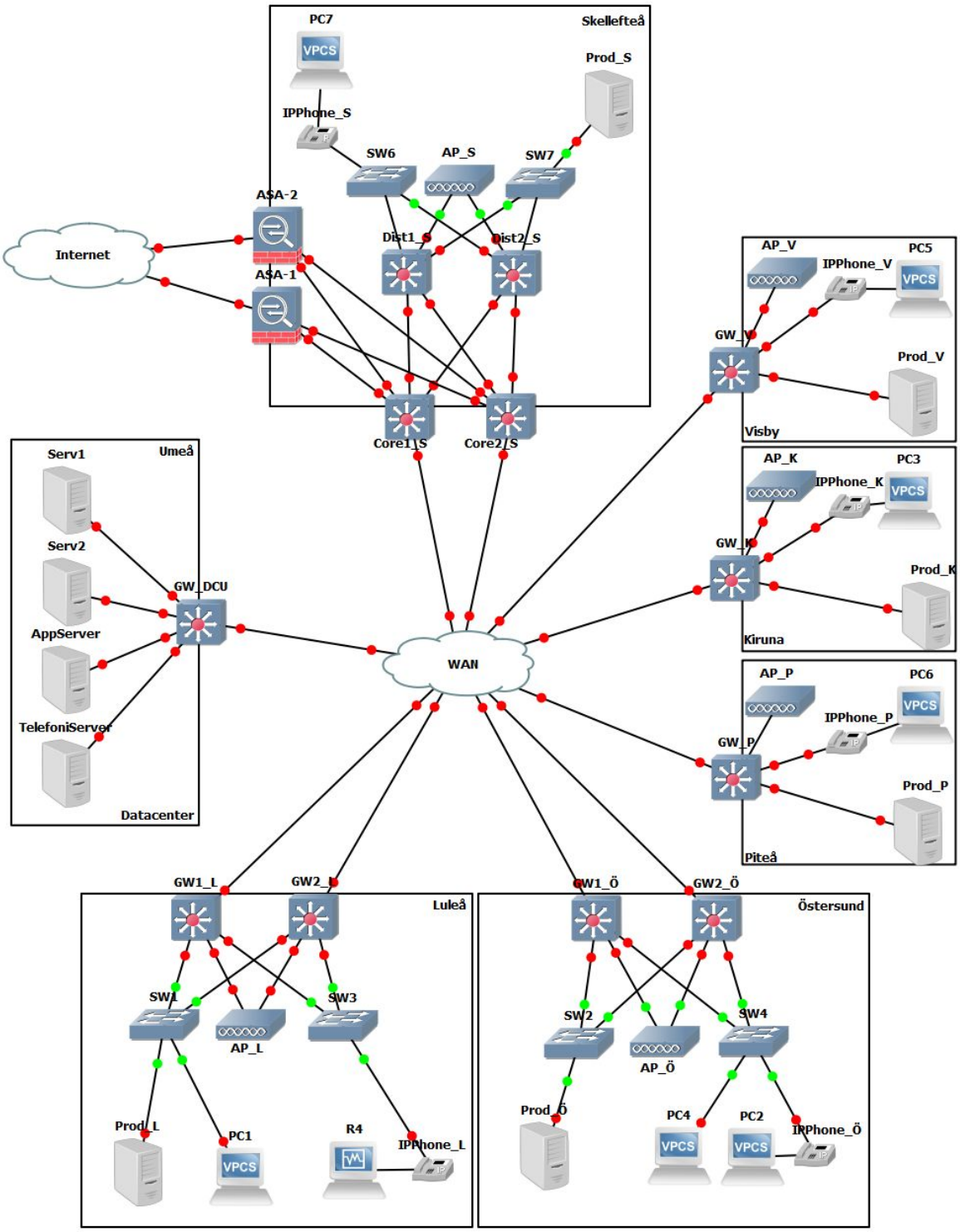

Bild 4, WAN-lösningen som ej används.