



Göteborg (VLAN 1)		
Ettet / Interface	IP Address	Gateway
Router Subinterface		
RT-GBG-Gb1/10 (Kontor)	172.16.2.0/26	172.16.2.1
RT-GBG-Gb1/20 (Guest)	172.16.2.4/24	172.16.2.182
RT-GBG-Gb1/99 (Admin)	172.16.2.128/26	172.16.2.129
RT-GBG Serial 0/0/1 (ISP)	60.60.60.2/30	
RT-GBG Tunnel 1	192.168.255.0/30	
Utgång Switch SW		
SW-GBG-AGG SW1	172.16.2.131	172.16.2.128
Access Switch SW		
SW-GBG-P1 SW1 (kontor)	172.16.2.131	172.16.2.128
SW-GBG-P2 SW1 (kontor)	172.16.2.132	172.16.2.128
PC		
PC-GBG-NIC (Kontor)	172.16.2.6	172.16.2.9
PC-GBG-NIC (Guest)	172.16.2.26	172.16.2.72
PC-GBG-NIC (Admin)	172.16.2.114	172.16.2.133

Stockholm (VLAN 1)		
Ettet / Interface	IP Address	Gateway
Router Subinterface		
RT-STH-Qb1/10 (Kontor)	10.0.1.5/26	10.0.1.6
RT-STH-Qb1/20 (Guest)	10.0.1.9/26	10.0.1.10
RT-STH-Qb1/99 (Admin)	10.0.1.134/26	10.0.1.135
RT-STH-Tunnel 1	192.168.255.1	-
Utgång Switch SW		
SW-STH-Agg SW	10.0.1.5/26	10.0.1.132
Access Switch SW		
SW-STH-P1 (kontor)	10.0.1.5/26	10.0.1.132
SW-STH-P2 (kontor)	10.0.1.9/26	10.0.1.132
PC		
PC-STH-MC (Kontor)	10.0.1.5/26	10.0.1.6
PC-STH-MC (Guest)	10.0.1.9/26	10.0.1.10
PC-STH-MC (Admin)	10.0.1.134/26	10.0.1.135

Säkerhetsåtgärder

1. VLAN-indelning:

- Vi har delat nätverket i olika vlan, t.ex. "Guest, kontor och admin" för att skapa en tydlig gräns mellan olika delar av verksamheten vilket gör att nätverken blir mer kontrollerbart och säkrare.

OSI Lager 2 (Data länk)

2. Portar:

- 2a. Vi har stängt alla oanvända portar och aktiverat port security på de portar som används för att förhindra obehöriga enheter från att ansluta sig till nätverket.
- 2b. Vi har tillåtit bara 1 enhets Mac adress vid varje port (port security maximum 1).
- 2c. Mac adress sticky: Vi har använt mac adress sticky, så att switchen automatiskt lär sig den anslutna enhetens Mac adress och sparar den i sin konfiguration.
- 2d. Violation shutdown: Vi har aktiverat violation shutdown, om en regel bryts, stängs porten automatiskt.

OSI Lager 2 (Data länk)

3. ACL - Access Control List

- Vi har implementerat en accesslista (ACL) som begränsar administrativ åtkomst till nätverksutrustningen. Endast SSHv2 tillåts, äldre SSH-versioner och Telnet blockeras. ACL:en tillåter endast anslutningar från admin-subnätet och är applicerad på alla VTY-linjer, vilket säkerställer att endast behöriga administratörer kan logga in på enheterna.

OSI Lager 3 (Nätverk)

5. SSH och RSA nycklar

Vi har aktiverat SSH (Secure shell) och genererat RSA-nycklar för att fjärrhantering av vårt nätverk ska vara säker och krypterad så att ingen obehörig ska lyssna eller manipulera trafiken.

OSI Lager 7 (Applikation)

7. DHCP-snooping

- Vi har aktiverat DHCP snooping för att förhindra att obehöriga enheter agerar falska DHCP-servrar. Endast betrodda portar får skicka DHCP-svar, vilket skyddar nätverket mot attacker som DHCP spoofing och felaktig IP-tilldelning.

OSI Lager 2 (Data länk) / lager 3 (nätverk).

8. Dynamic ARPing Inspection (DAI)

- Vi har aktiverat Dynamic ARP Inspection för att stoppa ARP-spoofing i nätverket. DAI verifierar att ARP-meddelanden stämmer överens med DHCP snooping-tabellen och blockerar falska ARP-svar, vilket skyddar klienter från att bli omdirigerade till angripare.

OSI Lager 2 (Data länk)

4. Blockerad HTTP.

Vi har säkrat servern genom att blockera HTTP (port 80) och endast tillåta HTTPS (port 443) för att allt kommunikation mellan användarna ska krypteras och inte i klartext. HTTPS använder SSL/TLS kryptering vilket gör att det går inte att läsa av data som skickas.

OSI Lager 7 (Applikation)

6. CDP

Vi har stängt av CDP (Cisco Discovery Protocol) för att hindra att Cisco enheterna utbyter information om sig själva. Detta gör att vi minskar mängden av synlig information, försvarar kartläggning av våra enheter och gör nätverket säkrare mot avlyssning och intrång.

OSI Lager 2 (Data länk)

9. Extended access list (Guest isolation):

Vi har skapat en extended access list, där vi har isolerat guest datorerna för att kontrollera vilken trafik som får passera eller blockeras. Guest datorerna hindras från att nå andra interna vlan och är blockerade till andra interna subnät och tunneln. Det här förhindrar spridning av eventuella virus och attacker.

OSI Lager 2 (Data länk)

10. Router ACL (Server)

Vi har använt oss av en ACL-list för att förhindra att obehöriga kan nå servern och försöker stjäla data eller genomföra någon attack. Det här förebygger också spridning av skadligt trafik då den inte skulle nå servern.

OSI Lager 3 (nätverk) /4 (transport)