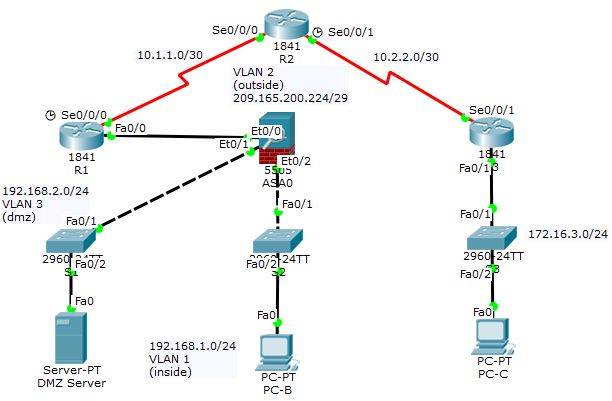
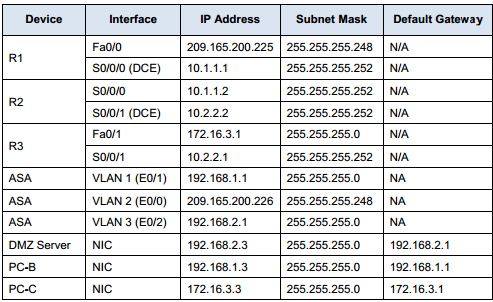
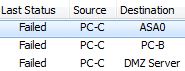
**LAPORAN PRAKTIKUM KEAMANAN JARINGAN 2**

**UNIT 8**

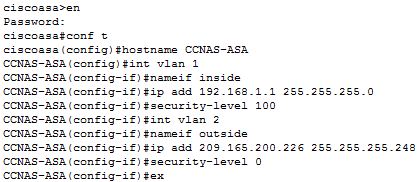




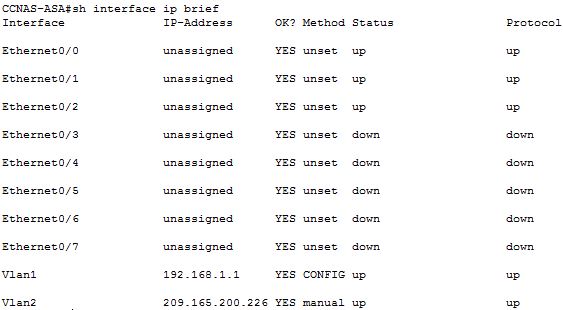
Pada praktikum kali ini , dibuat topologi seperti gambar di atas. Topologi tersebut menggunakan tiga router, tiga switch, dua PC, satu server, dan satu perangkat ASA. Praktikum kali ini bertujuan untuk mengonfigurasikan ASA. ASA merupakan perangkat yang memiliki fungsi seperti firewall. Setelah membuat topologi tersebut, berikan IP sesuai dengan IP table di atas. Selanjutnya, tes konektivitas topologi yang telah dibuat. Dari PC-C belum berhasil melakukan ping ke ASA, PC-B, maupun DMZ server, namun PC-C berhasil melakukan ping ke router interface nya yaitu R3.



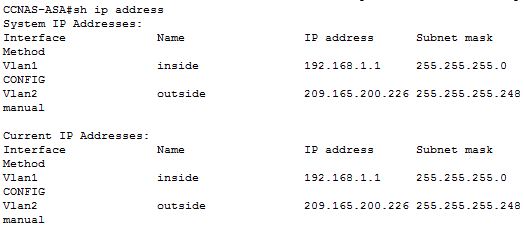
Kemudian, pada ASA lakukan konfigurasi. Pertama, berikan hostname CCNAS-ASA terlebih dahulu. Lalu, konfigurasikan interface inside dan outside dari ASA. Vlan 1 dijadikan interface inside, kemudian diberikan alamat IP dan level keamanannya adalah 100. Sedangkan vlan 2 dijadikan interface outside dengan level keamanan 0.



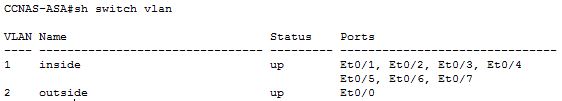
Setelah itu, untuk dapat melihat hasil konfigurasi yang telah dilakukan, dapat dengan show interface ip brief, yaitu untuk dapat melihat status interface ASA.



Kemudian, untuk dapat melihat informasi dari interface layer 3 vlan dapat dnegan show ip address.

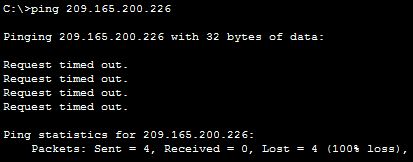


Untuk dapat melihat hasil konfigurasi vlan inside maupun outside dari ASA, dapat dengan show switch vlan.

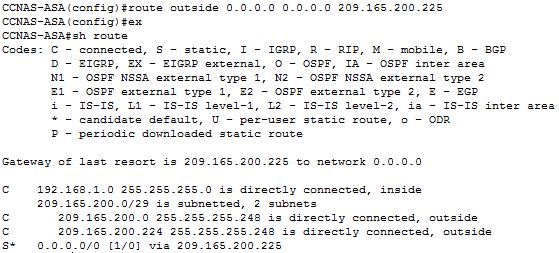


Setelah melakukan konfigurasi di atas, lakukan tes konektivitas dengan melakukan ping dari PC-B ke ASA yang akan berhasil, dan dari PC-B juga melakukan ping ke interface outside 209.165.200.226 yang akan gagal, karena ping menggunakan protocol icmp.

6.JPG



Selanjutnya, konfigurasi route static pada ASA. Buat route "quad zero" yang digabungkan dengan interface outside ASA, dan fa0/0 R1 sebagai gateway nya. Kemudian, untuk melihat hasil konfigurasi tersebut dapat dengan show route.



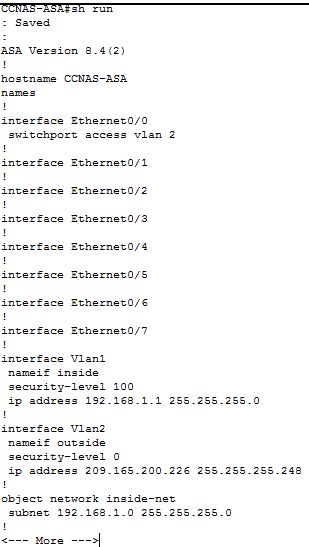
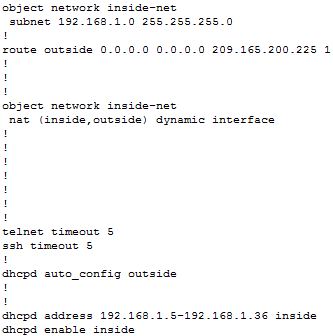
Setelah melakukan konfigurasi di atas, ASA dapat melakukan ping ke R1.

9.JPG

Lalu, lakukan konfigurasi dengan PAT dan network object, dengan membuat network object inside-net. Hal ini dilakukan untuk pen-spesifikasi-an IP yang ingin diterjemahkan melalui proses mapping. Pada proses ini, dilakukan konfigurasi nat inside dan outside dynamic.

10.JPG

Untuk dapat melihat hasil konfigurasi NAT object yang telah dibuat, dapat dengan show run.

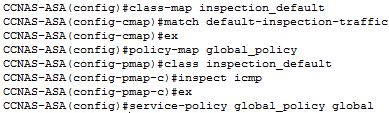
Selanjutnya, PC-B akan tidak berhasil melakukan ping ke R1.

13.JPG

Dan untuk dapat melihat hasil konfigurasi yang telah dilakukan pada NAT yaitu dengan show nat.

14.JPG

Kemudian, lakukan modifikasi pada MPF (Modular Policy Framework) pada ASA. Pertama, konfigurasi untuk menyamakan default traffic inscpection, kemudian pada policy map masuk ke global security dan class pada inspection default, dan menonaktifkan inspeksi pada komunikasi yang melibatkan protokol icmp. Kemudian, modifikasi pada service policy dan global policy pada global.



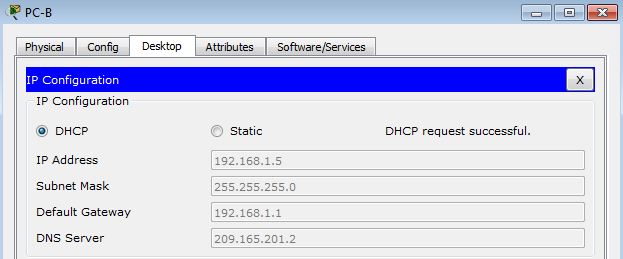
Setelah melakukan modifikasi tersebut, PC-B akan berhasill melakukan ping ke R1, karena traffic sudah diijinkan.

16.JPG

Selanjutnya, adalah konfigurasikan dengan AAA dan SSH. Konfigurasikan DHCP address pool dan enable-kan ke interface inside. Lalu, berikan DNS dan enable-kan DHCP daemon untuk dapat enable dengan interface inside. Buat range IP untuk membuat IP dhcpd pada jaringan yang akan masuk.

17.JPG

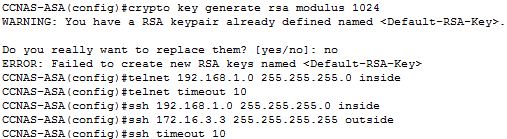
Dan pada PC-B ubah IP dari static menjadi DHCP.



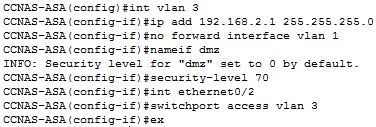
Kemudian, lakukan konfigurasi AAA untuk dapat menggunakan database lokal untuk autentikasi. Buat username dan password dan buat autentikasi user telnet dan ssh. Hal ini adalah untuk keamanan tambahan pada komunikasi keluar masuk jaringan. SSH dan telnet hanya dilakukan jika jaringan yang meremote bersifat lokal. Kemudian, terapkan keamanan berupa kriptografi rsa modulus 1024 untuk mengenkripsi komunikasi data selama proses remote dengan ssh dan telnet berjalan.

19.JPG

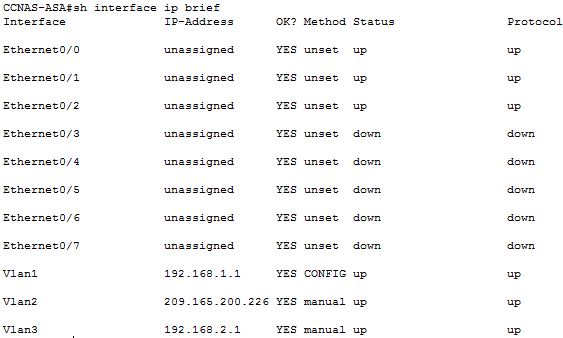
Setelah itu, konfigurasi remote access. Yaitu dengan melakukan generate RSA key, kemudian konfigurasi ASA untuk mengijinkan koneksi telnet dari host pada jaringan dalam 192.168.1.0/24 dan atur session timeout telnet nya adalah 10 menit. Lalu, konfigurasi ASA untuk mengijinkan koneksi ssh dari host ke jaringan dalam 192.168.1.0/24 dan dari host remote management pada jaringan luar. Diberikan timeout agar ketika tidak adanya komunikasi selama 10 menit maka akan otomatis keluar dari terminal.

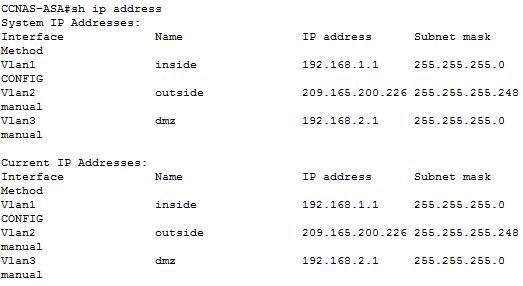


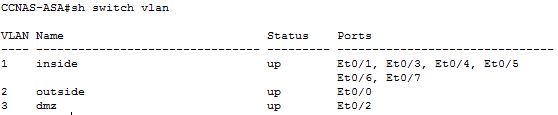
Setelah itu, konfigurasi DMZ, static NAT, dan ACL. Konfigurasikan DMZ vlan 3 dan berikan level keamanan 70, kemudian disable-kan forward interface vlan 1 karena server tidak membutuhkan komunikasi dengan user di jaringan dalam.



Kemudian, lihat hasil konfigurasi dengan show interface ip brief, show ip address, dan show switch vlan.







Setelah itu, konfigurasikan static NAT pada DMZ server dengan network object.

25.JPG

Konfigurasikan ACL juga untuk dapat mengijinkan akses ke DMZ server dari internet. ACL ini mengijinkan protokol ocmp dari 192.168.2.3 dan protokol tcp kecuali yang berasal dari port 80 (HTTP) dari 192.168.2.3. Dan untuk komunikasi keluar dapat diatur dnegan access-group.

26.JPG

**Kesimpulan**

Dalam melakukan konfigurasi pada ASA, terdapat perbedaan pengaturan dalam komunikasi data yang masuk dan keluar. Selain itu pada ASA juga jika tidak ditentukan batasannya maka pada proses mapping akan otomatis melakukan blok pada seluruh komunikasi paket data.