Key:

activation-key 0x1321CF73 0xFCB68F7E 0x801111DC 0xB554E4A4 0x0F3E008D

reload

Cấu hình ASA và bảo mật

En

Conf t

Interface vlan 1

Nameif inside

Ip address 192.168.1.1 255.255.255.0

security-level 100

no shut

ex

int vlan 2

nameif outside

ip address 209.165.200.226 255.255.255.0

security-level 0

no shut

ex

int vlan 3

nameif dmz

no forward int vlan 1

ip address 192.168.3.1 255.255.255.0

security-level 50

no shut

ex

int vlan 4

nameif KinhDoanh

no forward int vlan 1

ip address 192.168.4.1 255.255.255.0

security-level 70

no shut

ex

int vlan 5

nameif PhanTich

no forward int vlan 1

ip address 192.168.5.1 255.255.255.0

security-level 70

no shut

ex

int vlan 6

nameif ThietKe

no forward int vlan 1

ip address 192.168.6.1 255.255.255.0

security-level 70

no shut

ex

int vlan 7

nameif LapTrinh

no forward int vlan 1

ip address 192.168.7.1 255.255.255.0

security-level 70

no shut

ex

int vlan 8

nameif NhanSu

no forward int vlan 1

ip address 192.168.8.1 255.255.255.0

security-level 70

no shut

ex

int vlan 9

nameif KyThuat

no forward int vlan 1

ip address 192.168.9.1 255.255.255.0

security-level 100

no shut

ex

int vlan 10

nameif BackupServer

no forward int vlan 1

ip address 192.168.10.1 255.255.255.0

security-level 100

no shut

ex

route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

class-map testMap

match any

policy-map testPolicy

class testMap

inspect icmp

!

service-policy testPolicy global

!

telnet timeout 5

ssh timeout 5

!

dhcpd auto\_config outside

!

!

dhcpd address 192.168.1.5-192.168.1.34 inside

dhcpd enable inside

object network inside-net

subnet 192.168.1.0 255.255.255.0

nat (inside,outside) dynamic interface

object network dmz-net

subnet 192.168.3.0 255.255.255.0

nat (dmz,outside) dynamic interface

end

conf t

class-map inspection\_default

match default-inspection-traffic

ex

policy-map global\_policy

class inspection\_default

inspect icmp

ex

service-policy global\_policy global

dhcpd address 192.168.1.5-192.168.1.36 inside

dhcpd dns 209.165.201.2 interface inside

dhcpd enable inside

username admin password adminpa55

aaa authentication ssh console LOCAL

crypto key generate rsa modulus 1024

no

ssh 192.168.1.0 255.255.255.0 inside

ssh 172.16.3.3 255.255.255.255 outside

ssh timeout 10

int vlan 3

ip address 192.168.2.1 255.255.255.0

no forward int vlan 1

nameif dmz

security-level 70

int E 0/2

sw acc vlan 3

ex

conf t

object network KinhDoanh-obj

subnet 192.168.4.0 255.255.255.0

nat (KinhDoanh,outside) dynamic interface

ex

conf t

object network PhanTich-obj

subnet 192.168.5.0 255.255.255.0

nat (KinhDoanh,outside) dynamic interface

ex

conf t

object network ThietKe-obj

subnet 192.168.6.0 255.255.255.0

nat (ThietKe,outside) dynamic interface

ex

conf t

object network LapTrinh-obj

subnet 192.168.7.0 255.255.255.0

nat (LapTrinh,outside) dynamic interface

ex

conf t

object network NhanSu-obj

subnet 192.168.8.0 255.255.255.0

nat (NhanSu,outside) dynamic interface

ex

conf t

object network KyThuat-obj

subnet 192.168.9.0 255.255.255.0

nat (KyThuat,outside) dynamic interface

ex

conf t

object network BackUp-obj

subnet 192.168.10.0 255.255.255.0

nat (BackupServer,dmz) dynamic interface

ex

conf t

object network dmz-obj

subnet 192.168.3.0 255.255.255.0

nat (dmz,outside) dynamic interface

ex

conf t

Sw III:

en

conf t

int f 0/24

no switchport

ip address 192.168.1.1 255.255.255.0

no shutdown

exit

vlan 2

name outside

ex

vlan 3

name dmz

ex

vlan 4

name KinhDoanh

ex

vlan 5

name BaoVe

ex

object network dmzServer

host 192.168.3.3

nat (dmz,outside) static 209.165.200.227

ex

conf t

object network emailServer

host 192.168.3.4

nat (dmz,outside) static 209.165.200.228

ex

conf t

object network dnsServer

host 192.168.3.10

nat (dmz,outside) static 209.165.200.229

ex

Xu ly ouside => inside, dmz

access-list outside extended permit tcp any host 192.168.3.3

access-list outside extended permit tcp any host 192.168.3.3 eq 80

access-list outside extended permit icmp any host 192.168.3.3

access-list outside extended permit icmp any object KinhDoanh-obj echo-reply

access-list outside extended permit icmp any object PhanTich-obj echo-reply

access-list outside extended permit icmp any object ThietKe-obj echo-reply

access-list outside extended permit icmp any object LapTrinh-obj echo-reply

access-list outside extended permit icmp any object NhanSu-obj echo-reply

access-list outside extended permit icmp any object KyThuat-obj echo-reply

access-list outside extended permit icmp any object inside-subnet echo-reply

access-list outside extended permit tcp any host 192.168.3.10

access-list outside extended permit tcp any host 192.168.3.10 eq domain

access-group outside in interface outside

no access-list dmz extended permit tcp any host 192.168.3.3 eq domain

no access-list dmz extended permit tcp any host 192.168.3.4 eq smtp

no access-list dmz extended permit tcp any host 192.168.3.4

Xu ly dmz

access-list dmz extended permit icmp any object KinhDoanh-obj echo-reply

access-list dmz extended permit icmp any object PhanTich-obj echo-reply

access-list dmz extended permit icmp any object ThietKe-obj echo-reply

access-list dmz extended permit icmp any object LapTrinh-obj echo-reply

access-list dmz extended permit icmp any object NhanSu-obj echo-reply

access-list dmz extended permit icmp any object KyThuat-obj echo-reply

access-list outside extended permit icmp any object inside-subnet echo-reply

access-list dmz extended permit udp any eq domain any

no access-list dmz extended permit udp any any eq domain

no access-list dmz extended permit tcp any any eq domain

no access-list dmz extended permit tcp any eq domain any

Access-group dmz in interface dmz

no access-group kd in interface KinhDoanh

no access-list kd extended permit udp 192.168.4.0 255.255.255.0 host 192.168.3.10 eq domain

no access-list kd extended permit tcp object KinhDoanh-obj object dnsServer eq domain

no access-list kd extended permit udp any any eq domain

Cam cac vlan

access-list kd extended permit tcp object dmzServer object KinhDoanh-obj

access-list kd extended permit tcp object dmzServer object KinhDoanh-obj eq www

access-list kd extended permit icmp object KinhDoanh-obj object dmzServer

access-list kd extended deny icmp object KinhDoanh-obj object LapTrinh-obj

access-list kd extended deny icmp object KinhDoanh-obj object PhanTich-obj

access-list kd extended deny icmp object KinhDoanh-obj object ThietKe-obj

access-list kd extended deny icmp object KinhDoanh-obj object NhanSu-obj

access-list kd extended deny icmp object KinhDoanh-obj object KyThuat-obj

access-list kd extended permit icmp object KinhDoanh-obj any

access-list outside extended permit icmp any object inside-subnet echo-reply

access-list kd extended permit udp 192.168.4.0 255.255.255.0 object dnsServer eq domain

access-list kd permit tcp any any eq smtp

access-group kd in interface KinhDoanh

access-list pt extended permit tcp object dmzServer object PhanTich-obj

access-list pt extended permit tcp object dmzServer object PhanTich-obj eq www

access-list pt extended permit icmp object PhanTich-obj object dmzServer

access-list pt extended deny icmp object PhanTich-obj object LapTrinh-obj

access-list pt extended deny icmp object PhanTich-obj object KinhDoanh-obj

access-list pt extended deny icmp object PhanTich-obj object ThietKe-obj

access-list pt extended deny icmp object PhanTich-obj object NhanSu-obj

access-list pt extended deny icmp object PhanTich-obj object KyThuat-obj

access-list pt extended permit icmp object PhanTich-obj any

access-list pt extended permit udp 192.168.5.0 255.255.255.0 object dnsServer eq domain

access-list pt permit tcp any any eq smtp

access-group pt in interface PhanTich

access-list thietke extended permit tcp object dmzServer object ThietKe-obj

access-list thietke extended permit tcp object dmzServer object ThietKe-obj eq www

access-list thietke extended permit icmp object ThietKe-obj object dmzServer

access-list thietke extended deny icmp object ThietKe-obj object LapTrinh-obj

access-list thietke extended deny icmp object ThietKe-obj object PhanTich-obj

access-list thietke extended deny icmp object ThietKe-obj object KinhDoanh-obj

access-list thietke extended deny icmp object ThietKe-obj object NhanSu-obj

access-list thietke extended deny icmp object ThietKe-obj object KyThuat-obj

access-list thietke extended permit icmp object ThietKe-obj any

access-list thietke extended permit udp 192.168.6.0 255.255.255.0 object dnsServer eq domain

access-list thietke permit tcp any any eq smtp

access-group thietke in interface ThietKe

access-list laptrinh extended permit tcp object dmzServer object LapTrinh-obj

access-list laptrinh extended permit tcp object dmzServer object LapTrinh-obj eq www

access-list laptrinh extended permit icmp object LapTrinh-obj object dmzServer

access-list laptrinh extended deny icmp object LapTrinh-obj object KinhDoanh-obj

access-list laptrinh extended deny icmp object LapTrinh-obj object PhanTich-obj

access-list laptrinh extended deny icmp object LapTrinh-obj object ThietKe-obj

access-list laptrinh extended deny icmp object LapTrinh-obj object NhanSu-obj

access-list laptrinh extended deny icmp object LapTrinh-obj object KyThuat-obj

access-list laptrinh extended permit icmp object LapTrinh-obj any

access-list laptrinh extended permit udp 192.168.7.0 255.255.255.0 object dnsServer eq domain

access-list laptrinh permit tcp any any eq smtp

access-group laptrinh in interface LapTrinh

access-list nhansu extended permit tcp object dmzServer object NhanSu-obj

access-list nhansu extended permit tcp object dmzServer object NhanSu-obj eq www

access-list nhansu extended permit icmp object NhanSu-obj object dmzServer

access-list nhansu extended deny icmp object NhanSu-obj object LapTrinh-obj

access-list nhansu extended deny icmp object NhanSu-obj object PhanTich-obj

access-list nhansu extended deny icmp object NhanSu-obj object ThietKe-obj

access-list nhansu extended deny icmp object NhanSu-obj object KinhDoanh-obj

access-list nhansu extended deny icmp object NhanSu-obj object KyThuat-obj

access-list nhansu extended permit icmp object NhanSu-obj any

access-list nhansu extended permit udp 192.168.8.0 255.255.255.0 object dnsServer eq domain

access-list nhansu permit tcp any any eq smtp

access-group nhansu in interface NhanSu

access-list kythuat extended permit tcp object dmzServer object KyThuat-obj

access-list kythuat extended permit tcp object dmzServer object KyThuat-obj eq www

access-list kythuat extended permit icmp object KyThuat-obj object dmzServer

access-list kythuat extended deny icmp object KyThuat-obj object LapTrinh-obj

access-list kythuat extended deny icmp object KyThuat-obj object PhanTich-obj

access-list kythuat extended deny icmp object KyThuat-obj object ThietKe-obj

access-list kythuat extended deny icmp object KyThuat-obj object NhanSu-obj

access-list kythuat extended deny icmp object KyThuat-obj object KinhDoanh-obj

access-list kythuat extended permit icmp object KyThuat-obj any

access-list kythuat extended permit udp 192.168.9.0 255.255.255.0 object dnsServer eq domain

access-list kythuat permit tcp any any eq smtp

access-group kythuat in interface KyThuat

no access-list kd extended permit icmp any object LapTrinh-obj echo-reply

no access-list kd extended permit icmp any object KinhDoanh-obj echo-reply

no access-list kd extended permit icmp any object ThietKe-obj echo-reply

no access-list kd extended permit icmp any object PhanTich-obj echo-reply

no access-list kd extended permit icmp any object NhanSu-obj echo-reply

no access-list kd extended permit icmp any object KyThuat-obj echo-reply

int vlan 4

ip address 192.168.4.1 255.255.255.0

no shut

ex

int vlan 5

ip address 192.168.5.1 255.255.255.0

no shut

ex

int f 0/4

sw mode acc

sw acc vlan 4

ex

int f 0/5

sw mode acc

sw acc vlan 5

ex

ip routing

ex

show vlan brief

show ip route

SSH va Telnet

En

conf t

username admin password admin

telnet 192.168.1.10 255.255.255.255 inside

telnet timeout 50

aaa authentication telnet console LOCAL

enable password 123