```
ASA Version 8.4(1)9
!
hostname firewall
domain-name mycompany.com
!
interface GigabitEthernet0/1
 speed 100
 duplex full
 nameif inside
 security-level 100
 ip address 30.0.0.1 255.255.255.0
!
interface GigabitEthernet0/2
 speed 1000
 duplex full
 nameif outside
 security-level 0
 ip address 50.0.0.1 255.255.255.0
!
boot system disk0:/asa841-9-k8.bin
ftp mode passive
clock timezone GMT 2
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 20.0.0.12
 domain-name mycompany.com
same-security-traffic permit intra-interface
object network obj-30.0.0.0
 subnet 30.0.0.0 255.255.255.0
object network obj-20.0.0.0
 subnet 20.0.0.0 255.255.255.0
object network obj-40.0.0.0
 subnet 40.0.0.0 255.255.255.0
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network obj-0.0.0.0
 host 0.0.0.0
!
pager lines 20
logging enable
logging timestamp
logging standby
logging buffer-size 100000
logging monitor debugging
logging buffered debugging
logging trap debugging
logging asdm informational
logging facility 23
logging host inside 20.0.0.201
```

```
mtu inside 1500
mtu outside 1300
ip local pool vpn-pool 40.0.0.10-40.0.0.254 mask 255.255.255.0
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip audit name IDSInfo info action alarm
ip audit name IDSAttack attack action alarm
ip audit interface outside IDSInfo
ip audit interface outside IDSAttack
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
asdm image disk0:/asdm-641.bin
asdm history enable
arp timeout 14400
nat (inside,any) source static obj-30.0.0.0 obj-30.0.0.0 destination static obj-40.0.0.0 obj-40.0.0.0
nat (inside,any) source static obj-20.0.0.0 obj-20.0.0.0 destination static obj-40.0.0.0 obj-40.0.0.0
!
object network obj_any
 nat (inside,outside) dynamic obj-0.0.0.0
route outside 0.0.0.0 0.0.0.0 50.0.0.2 1
route inside 20.0.0.0 255.255.255.0 30.0.0.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
ldap attribute-map AD-LDAP
dynamic-access-policy-record DfltAccessPolicy
aaa-server myldap-grp protocol ldap
aaa-server myldap-grp (inside) host 20.0.0.200
 timeout 20
 server-port 1389
 ldap-base-dn dc=mycompany,dc=com
 ldap-scope subtree
 ldap-naming-attribute mail
 ldap-login-password xxxx
 ldap-login-dn cn=admin,o=admin,dc=mycompany,dc=com
aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authentication http console LOCAL
http server enable 4443
http server idle-timeout 5
http server session-timeout 5
http 20.0.0.21 255.255.255.255 inside
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart
service resetoutside
crypto ipsec ikev2 ipsec-proposal MyTransformSet
 protocol esp encryption aes-256 aes-192 aes 3des
 protocol esp integrity sha-1
crypto dynamic-map outside_dyn_map 20 set ikev2 ipsec-proposal MyTransformSet
crypto map outside_cry_map 10 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_cry_map interface outside
crypto map inside_cry_map 10 ipsec-isakmp dynamic outside_dyn_map
crypto map inside_cry_map interface inside
crypto ca trustpoint myinternalca
 revocation-check crl
 enrollment terminal
 subject-name CN=firewall.mycompany.com
 ip-address 50.0.0.1
 keypair mykey
 client-types ipsec
 id-usage ssl-ipsec code-signer
 crl configure
crypto ca certificate map MyCM2 1
 issuer-name attr cn co myinternalca
crypto ca certificate chain myinternalca
 certificate xxx
    ...
  quit
crypto isakmp nat-traversal 30
crypto isakmp disconnect-notify
crypto ikev2 policy 1
 encryption aes-256 aes-192 aes 3des
 integrity sha md5
 group 5 2 1
 prf sha
 lifetime seconds 86400
crypto ikev2 enable inside client-services port 443
crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint myinternalca
telnet timeout 5
ssh scopy enable
ssh 20.0.0.21 255.255.255.255 inside
ssh timeout 50
console timeout 15
management-access inside
no vpn-addr-assign aaa
threat-detection basic-threat
threat-detection scanning-threat
threat-detection statistics host number-of-rate 3
threat-detection statistics port number-of-rate 3
threat-detection statistics protocol number-of-rate 3
threat-detection statistics access-list
```

```
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
ntp server 20.0.0.145
ssl encryption aes128-sha1 aes256-sha1
ssl trust-point myinternalca outside
ssl trust-point myinternalca inside
ssl certificate-authentication interface inside port 443
ssl certificate-authentication interface outside port 443
webvpn
 enable inside
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.0.0629-k9.pkg 1
 anyconnect image disk0:/anyconnect-linux-3.0.0629-k9.pkg 2
 anyconnect profiles myvpn disk0:/myvpn.xml
 anyconnect profiles sslprofile disk0:/sslprofile.xml
 anyconnect enable
 tunnel-group-list enable
 default-language en
 certificate-group-map MyCM2 1 MyTunnelGroup
group-policy MyGroupPolicy internal
group-policy MyGroupPolicy attributes
 wins-server value 20.0.0.10
 dns-server value 20.0.0.11
 dhcp-network-scope 40.0.0.0
 vpn-simultaneous-logins 20
 vpn-tunnel-protocol ikev2 ssl-client ssl-clientless
 default-domain value mycompany.com
 webvpn
  anyconnect profiles value myvpn type user
tunnel-group MyTunnelGroup type remote-access
tunnel-group MyTunnelGroup general-attributes
 address-pool vpn-pool
 authorization-server-group myldap-grp
 default-group-policy MyGroupPolicy
 authorization-required
 username-from-certificate UPN
tunnel-group MyTunnelGroup webvpn-attributes
 authentication certificate
tunnel-group MyTunnelGroup ipsec-attributes
 chain
 isakmp keepalive threshold 3600 retry 5
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect h323 h225
```

```
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect ftp
  inspect dns
  inspect http
!
service-policy global_policy global
prompt hostname state priority
coredump enable filesystem disk0: size 100
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
hpm topN enable
```