Basic PIX Firewall Configuration

There is basic PIX Firewall configuration on-hand from time to time. The client that does the following:

1. NAT overload from an inside network to an outside network
2. Accept incoming PPTP VPN connections from ouside clients
3. Turns on the web-based GUI on the PIX

: Saved
:
PIX Version 6.3(4)
interface ethernet0 auto
interface ethernet1 100full
:These two lines activate the outside (Ethernet0) and inside (Ethernet1) interfaces
nameif ethernet0 outside security0
nameif ethernet1 inside security100
:These two lines assign names to the interfaces
enable password ------ encrypted
:Sets the password for privileged mode
passwd -------- encrypted
:Sets the telnet password
hostname pixfirewall
domain-name ciscopix.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
no fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
:Fixup protocols allow advanced applications to work through NAT. All the above fixup protocol configuration is in the PIX by default.
names
access-list 101 permit ip 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list 102 permit icmp any any
access-list 102 permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list 103 permit ip any any
:Same access-list syntax as a router. These are used below.
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside x.x.x.x 255.255.255.248
:Sets the outside interface IP address

ip address inside 192.168.1.1 255.255.255.0
:Sets the inside interface IP address
ip audit info action alarm
ip audit attack action alarm
ip local pool pptp-pool 192.168.2.10-192.168.2.50
:Defines a local DHCP pool of addresses for the PIX to give to incoming PPTP VPN clients
pdm logging informational 100
pdm history enable
:This tracks access to the PDM (the web-based GUI) built-in to the PIX
arp timeout 14400
global (outside) 1 interface
:This is a HUGE command. It turns on NAT translation for all addresses matching NAT rule 1 (shown below) to be translated through the outside interface (to the Internet, in this case)
nat (inside) 0 access-list 101
:This creates NAT rule 0 which tells NAT not to translate addresses that are defined in access list 101 (shown above). This keeps NAT from translating any communication between internal clients (192.168.1.0/24) and VPN clients (192.168.2.0/24).
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
:This creates NAT rule 1 which matches ALL addresses coming from the inside interface
conduit permit icmp any any
:Conduits are the old form of access-lists. This one permits all ICMP messages to the PIX
route outside 0.0.0.0 0.0.0.0 x.x.x.x
:Sets a default route to the ISP router (represented with x.x.x.x)
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
http server enable
http 192.168.1.0 255.255.255.0 inside
:Turns on the HTTP interface to the PIX, but only allows internal users (192.168.1.0/24) to access it. This enables the PDM (the web-based GUI) on the PIX
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-pptp
:Also a very huge command. This allows PPTP connections to the PIX firewall without the need for an access-list permitting PPTP. You can also use commands like sysopt connection permit-ipsec to permit IPSEC VPN connections
telnet 192.168.1.0 255.255.255.0 inside
:Allows telnet access to the PIX only from the internal subnet
telnet timeout 5
ssh timeout 5
console timeout 0

vpdn group 1 accept dialin pptp
:Allows PIX to accept PPTP connections
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
:Allows PPTP users to authenticate using any of the above methods (listed from weakest to strongest)
vpdn group 1 ppp encryption mppe auto
vpdn group 1 client configuration address local pptp-pool
:Points the PIX to hand out IP addresses to incoming VPN clients from the DHCP pool called "pptp-pool" (shown above in the config)
vpdn group 1 client configuration dns 192.168.1.252
vpdn group 1 client configuration wins 192.168.1.251
:Points the VPN clients to the right DNS and WINS server addresses
vpdn group 1 pptp echo 60
:Sends an "echo" (kinda like a keepalive) once every 60 seconds. If a response is not heard, VPN is torn down
vpdn group 1 client authentication local
:Authenticates VPN users using a local user database (shown below)
vpdn username jonesr password *********
vpdn username cepa password *********
vpdn username bob password *********
:Three VPN users allowed to connect
vpdn enable outside
:Turns on VPN connectivity on the outside interface
dhcpd lease 3600
dhcpd ping_timeout 750
username cisco password -------- encrypted privilege 15
:If I telnet with this username/password, I go straight to privileged mode
terminal width 80
: end
from JC