VPNs on PIX/ASA Version 7

Per-VPN ACLs on PIX/ASA version 7

Version 7 of the PIX/ASA software introduces the ability to define an ACL which is applied per-VPN or per-VPN user without needing to "pollute" the ACL applied to the outside-facing interface. This benefits are…

- The ACL on the outside interface only need contain rules allowing unencrypted traffic in from the outside. This keeps the ACL very clean
- You don't need a separate IP address pool for each VPN group in order to do per-group filtering (although you can still do so)

The configuration highlights are as follows:-

```
access-list VPNGROUP1 permit tcp ADDRESSPOOL 255.255.255.0 object-group GROUP1SERVERS

access-list VPNGROUP2 permit tcp ADDRESSPOOL 255.255.255.0 object-group GROUP2SERVERS
(…etc – separate ACL for each distinct VPN group)

access-list EMCG permit ip any any  ! He's a good egg with an honest face – we trust him !!

username eamonn password xxxxxxxx encrypted
username eamonn attributes
 vpn-filter value EMCG        ! This VPN user gets his own ACL (overrides group policy)
 group-lock value GROUP2      ! Be safe: only allow this username to be used with a fixed VPN group

sysopt connection permit-vpn  ! VPN traffic isn't subject to the regular ACL (but see "DfltGrpPolicy" below)

access-list DENY-ALL deny ip any any

group-policy DfltGrpPolicy attributes
vpn-filter value DENY-ALL     ! Be safe: deny all traffic for VPN groups without an ACL defined

group-policy GROUP1 attributes
 vpn-filter value VPNGROUP1   ! Apply the "VPNGROUP1" ACL to traffic with this tunnel-group
 group-lock value GROUP1

group-policy GROUP2 attributes
 vpn-filter value VPNGROUP2   ! Apply the "VPNGROUP2" ACL to traffic with this tunnel-group
 group-lock value GROUP2

tunnel-group GROUP1 type ipsec-ra
tunnel-group GROUP1 general-attributes
 address-pool ADDRESSPOOL     ! You can use one address pool for all user groups now
 default-group-policy GROUP1  ! Apply a particular group-policy to this VPN group
tunnel-group GROUP1 ipsec-attributes
 pre-shared-key *

tunnel-group GROUP1 type ipsec-ra
tunnel-group GROUP1 general-attributes
 address-pool ADDRESSPOOL
 default-group-policy GROUP1
```

```
tunnel-group GROUP1 ipsec-attributes
 pre-shared-key *
```

TODO:

- Try this with site-to-site VPNs

VPN Authentication off SecurID Server

This is a working configuration demonstrating how to set up an ASA to authenticate off a SecurID server using the native SDI protocol. It also includes the per-VPN ACLs discussed in the previous section.

```
PIX Version 7.2(4)
!
hostname VPNTEST
domain-name dqnetworks.ie
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 192.168.78.50 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.10.10.97 255.255.255.240
!
ftp mode passive
dns server-group DefaultDNS
 domain-name dqnetworks.ie
access-list DENY-ALL extended deny ip any any
access-list REMOTE extended permit ip any any
pager lines 24
logging enable
logging buffered informational
no logging message 710005
mtu outside 1500
mtu inside 1500
ip local pool REMOTE 10.10.10.80-10.10.10.88 mask 255.255.255.240
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-524.bin
no asdm history enable
arp timeout 14400
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
aaa-server SECURID protocol sdi ! Define the address of the SecurID servers
aaa-server SECURID (inside) host 10.10.10.100
aaa-server SECURID (inside) host 10.10.10.101
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map OUTSIDE-DYN 20 set pfs
crypto dynamic-map OUTSIDE-DYN 20 set transform-set ESP-DES-MD5
crypto map OUTSIDE 65535 ipsec-isakmp dynamic OUTSIDE-DYN
crypto map OUTSIDE interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash md5
 group 2
 lifetime 86400
crypto isakmp policy 20
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
telnet timeout 5
ssh timeout 5
console timeout 0
group-policy REMOTE internal ! Apply the "REMOTE" ACL to VPN connections made using this policy
group-policy REMOTE attributes
 vpn-filter value REMOTE
group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter value DENY-ALL    ! Default VPN ACL is to deny everything
 vpn-tunnel-protocol IPSec l2tp-ipsec
 password-storage disable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain none
 split-dns none
 intercept-dhcp 255.255.255.255 disable
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
 nem disable
 backup-servers keep-client-config
```

```
 msie-proxy server none
 msie-proxy method no-modify
 msie-proxy except-list none
 msie-proxy local-bypass disable
 nac disable
 nac-sq-period 300
 nac-reval-period 36000
 nac-default-acl none
 address-pools none
 smartcard-removal-disconnect enable
 client-firewall none
 client-access-rule none
tunnel-group REMOTE type ipsec-ra
tunnel-group REMOTE general-attributes
 address-pool REMOTE
 authentication-server-group SECURID
 default-group-policy REMOTE
tunnel-group REMOTE ipsec-attributes
 pre-shared-key *
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:4c67ce1c5f41ae250c62dad97bd55031
: end
```