APPENDIX C

Configuration of the EttF Demilitarized Zone

Security Configuration

ASA Configuration

```
ASA Version 7.2(2)
!
hostname DMZ-ASA-1
domain-name cisco.com
enable password 7w22FjI5eWal1BPD encrypted
names
!
interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.18.1.1 255.255.255.0 standby 10.18.1.3
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 10.13.2.1 255.255.255.248 standby 10.13.2.3
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 10.19.2.9 255.255.255.248 standby 10.19.2.10
!
interface GigabitEthernet0/3
description LAN/STATE Failover Interface
!
interface Management0/0
nameif management
security-level 100
ip address 172.28.212.31 255.255.255.0
management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa722-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
access-list outside extended permit tcp any any eq telnet
access-list outside extended permit tcp any any eq www
access-list outside extended permit icmp any any
access-list INSAUTH extended permit tcp any host 10.19.2.5 eq telnet
```

```
access-list INSAUTH extended permit tcp any host 10.19.2.5 eq www
access-list INSAUTH extended permit tcp any host 10.19.2.5 eq 8080
access-list dmz extended permit tcp any any eq telnet
access-list dmz extended permit tcp any any eq www
access-list dmz extended permit icmp any any
access-list DMZ_authentication extended permit tcp any any eq telnet
access-list inside extended permit tcp any any eq www
access-list inside extended permit tcp any any eq https
access-list inside extended permit icmp any any
access-list inside extended permit tcp any host 10.19.2.1 eq telnet
access-list OUTAUTH extended permit tcp any host 10.18.1.2 eq telnet
access-list OUTAUTH extended permit tcp any host 10.18.1.2 eq www
access-list ips-acl extended permit ip any any
access-list ips-acl extended permit icmp any any
pager lines 24
logging enable
logging buffered debugging
logging trap debugging
logging host management 172.28.212.22
mtu inside 1500
mtu outside 1500
mtu DMZ 1500
mtu management 1500
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface DMZ
ip verify reverse-path interface management
failover
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover replication http
failover link failover GigabitEthernet0/3
failover interface ip failover 10.18.2.33 255.255.255.248 standby 10.18.2.34
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-521.bin
asdm history enable
arp timeout 14400
access-group inside in interface inside
access-group outside in interface outside
access-group dmz in interface DMZ
route inside 10.17.0.0 255.255.0.0 10.18.1.5 1
route inside 10.18.0.0 255.255.0.0 10.18.1.5 1
route DMZ 10.19.0.0 255.255.0.0 10.19.2.1 1
route management 171.70.0.0 255.255.0.0 172.28.212.1 1
route management 172.0.0.0 255.0.0.0 172.28.212.1 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 uauth 0:05:00 absolute
aaa-server ETTF2 protocol tacacs+
aaa-server ETTF2 (DMZ) host 10.19.2.11
key cisco
username root password /bieFEvWpEclHwvP encrypted privilege 15
aaa authentication match OUTAUTH outside ETTF2
aaa authentication ssh console LOCAL
aaa authentication serial console LOCAL
aaa authentication http console LOCAL
aaa authentication match INSAUTH inside ETTF2
aaa authentication match DMZ_authentication DMZ ETTF2
http server enable
http 0.0.0.0 0.0.0.0 management
snmp-server host management 172.28.212.22 community marstring
no snmp-server location
```

```
no snmp-server contact
snmp-server community marstring
snmp-server enable traps snmp authentication linkup linkdown coldstart
virtual telnet 10.18.1.254
telnet 0.0.0.0 0.0.0.0 DMZ
telnet timeout 1440
ssh scopy enable
ssh 10.18.0.0 255.255.0.0 inside
ssh 10.17.0.0 255.255.0.0 inside
ssh 10.19.0.0 255.255.0.0 DMZ
ssh 0.0.0.0 0.0.0.0 management
ssh timeout 10
console timeout 0
!
class-map ips-class
match access-list ips-acl
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map ips-policy
class ips-class
ips inline fail-close
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
service-policy ips-policy interface inside
service-policy ips-policy interface outside
service-policy ips-policy interface DMZ
webvpn
csd image disk0:/securedesktop-asa-3.1.1.29-k9.pkg
csd enable
prompt hostname context
Cryptochecksum:dd189225023b09b212fb39b73974edad
: end
```

IPS Configuration

```
! ------------------------------
! Current configuration last modified Thu Mar 29 23:03:06 2007
! ------------------------------
! Version 6.0(1)
! Host:
```

```
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S263.0   2006-12-18
!     Virus Update        V1.2     2005-11-24
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 172.28.212.32/24,172.28.212.1
host-name dmz-ssm-1
telnet-option disabled
access-list 0.0.0.0/0
login-banner-text You are logging on to AIP-SSM of DMZ-ASA-1
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
trap-destinations 172.28.212.22
trap-community-name marstring
trap-port 162
exit
enable-notifications true
enable-set-get true
read-only-community marstring
read-write-community marstring
trap-community-name marstring
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
status
enabled false
exit
exit
signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|produce-verbose-alert
exit
alert-frequency
summary-mode fire-all
summary-key AxBx
exit
exit
status
enabled true
```

```
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service analysis-engine
exit
```