

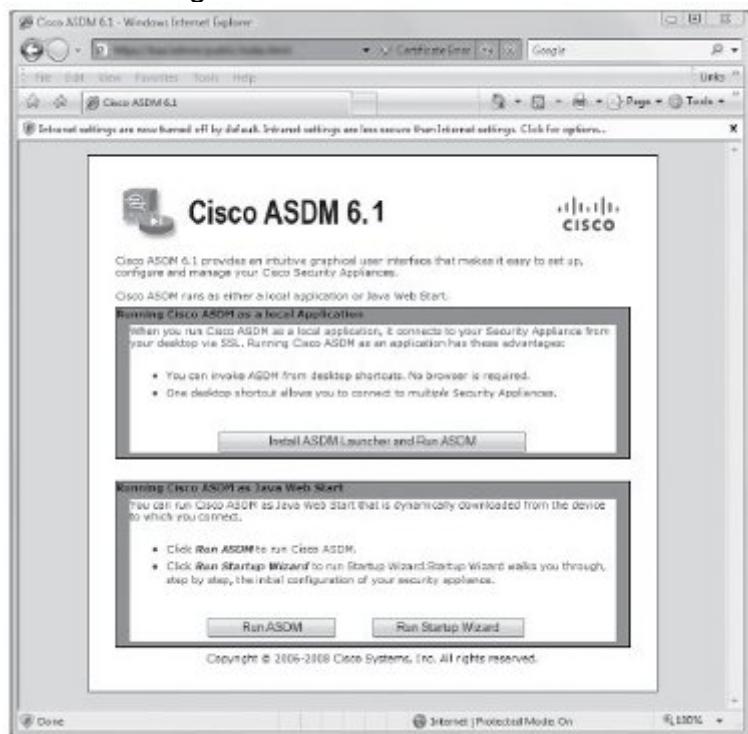
SSL VPN Configuration of a Cisco ASA 8.0

SSL VPN Configuration of a Cisco ASA 8.0

The Cisco® ASA family of devices are based on the Cisco® PIX platform (Figure 19); however they have been re-engineered and improved with feature rich functions. Included in the ASA Platform is IPSec VPN, SSL VPN, Web Portal and Secure Desktop facilities. The IPSec VPN functions are included for no extra charge; the remainder are chargeable options after version 7.0 of the ASA.

Configuration of the Cisco ASA can be either through the CLI (command line interface) using SSH or through the ASDM GUI interface. The ASDM client software for Windows and Mac OS

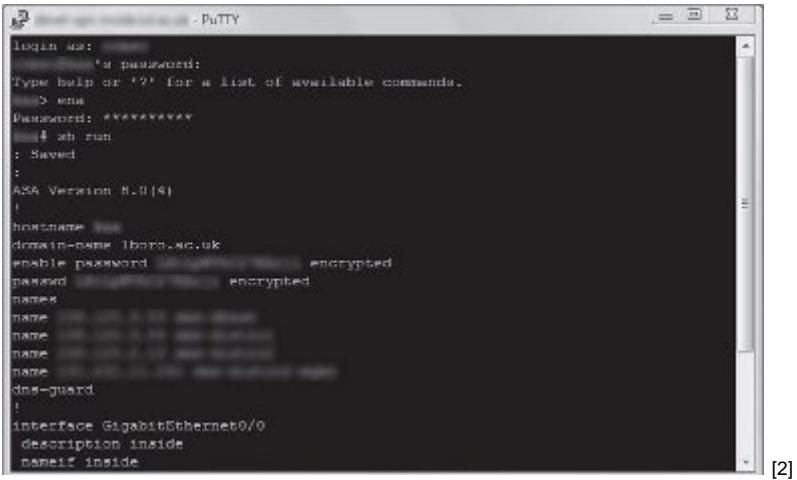
may be downloaded and installed by all features of the ASA are supported



[1]

Figure 20. Cisco ASDM download and installation.

The CLI interface can be reached through the SSH protocol, typically using PuTTY under Windows (Figure 21) or SSH/Slogin on Unix/Linux Operating Systems.



```

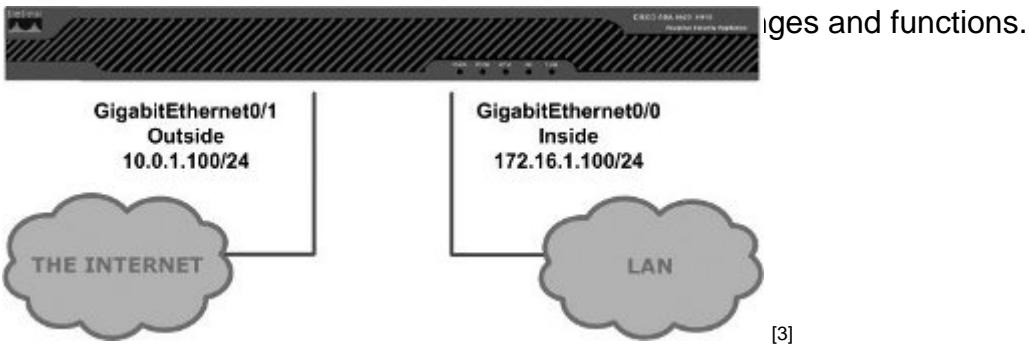
login as: [REDACTED]
password: [REDACTED]
Type help or '?' for a list of available commands.
> enable
Password: [REDACTED]
# config
# Saved
ASA Version 8.0(4)
!
hostname [REDACTED]
domain-name [REDACTED].uk
enable password [REDACTED] encrypted
password [REDACTED] encrypted
names
name
name
name
name
name
dns-guard
!
interface GigabitEthernet0/0
description inside
nameif inside

```

[2]

Figure 21. Cisco ASA access through the CLI using PuTTY.

Configuration Example



The following configuration example configures the Cisco ASA for IPSec and SSL VPN connectivity, and provides pointers to areas mentioned in the SSL VPN chapter.

1. Configure the interfaces on the ASA for connectivity on the organisational LAN. Security levels should be configured so the inside interface is a higher value than the outside. Add default routes:

```

interface GigabitEthernet0/0
description inside
nameif inside
security-level 100
ip address 172.16.1.100 255.255.255.0
!
route inside 172.16.0.0 255.255.0.0 172.16.1.1

```

```
route inside 192.168.1.0 255.255.255.0 172.16.1.1.1
```

2. Clear the ASA flash and upload new firmware images:

```
show flash:
```

```
erase flash:
```

```
copy tftp://<tftp Server>/asa803-6-k8.bin flash:
```

```
copy tftp://<tftp Server>/asdm-611.bin flash:
```

3. Configure the new images as the default boot images:

```
boot system disk0:/asa803-6-k8.bin
```

```
asdm image disk0:/asdm-611.bin
```

```
wr mem
```

```
reload
```

4. Configure the ASA with appropriate passwords:

```
enable password -password-
```

```
passwd -password-
```

5. Enable SSH on the inside interface:

```
crypto key generate rsa modulus 1024
```

```
ssh 172.16.0.0 255.255.0.0 inside
```

```
ssh 172.16.1.0 255.255.255.0 management
```

```
ssh timeout 5
```

```
ssh version 2
```

```
Check with ssh <IP Address> -l pix
```

6. Configure other Interfaces and Routing:

```
interface GigabitEthernet0/1
```

```
description outside
```

```
no shutdown
```

```
nameif outside security-level 0
```

```
ip address 10.0.1.100 255.255.255.0
```

```
!
```

```
interface GigabitEthernet0/2
```

```
shutdown
```

```
no nameif
```

```
no security-level
```

```
no ip address
```

```
!
```

```
interface GigabitEthernet0/3
```

```
shutdown
```

```
no nameif
```

```
no security-level
```

```
no ip address
```

```
!
```

```
interface Management0/0
```

```
description management
```

```
no shutdown
```

```
nameif management
```

```
security-level 100
```

```
ip address 172.16.1.0 255.255.255.0
```

```
management-only
```

```
!
```

```
route outside 0.0.0.0 0.0.0.0 10.0.1.1.1
```

7. Configure DNS:

```
dns domain-lookup inside
```

```
dns server-group DefaultDNS
```

```
name-server <Primary DNS IP Address>
name-server <Secondary DNS IP Address>
name-server <Tertiary DNS IP Address>
domain-name camford.ac.uk
names
name <IP Address> <Static FQDN>
etc...
dns-guard
```

8. The ASA can categorise entities into object groups. Adding hostnames for entries within the configuration can make administration easier; in this example entries for Microsoft SMS Server are added:

```
object-group service MSRDP tcp
port-object eq 3389
object-group network SMS_Servers
network-object host sms-server1
network-object host sms-server2
network-object host sms-database
```

9. Create the Access Lists to support the security of the VPN/Firewall within the ACL:

```
access-list CAMFORD-NETBLOCKS-v1 standard permit 172.16.0.0 255.255.0.0
access-list CAMFORD-NETBLOCKS-v1 standard permit 192.168.1.0 255.255.255.0
access-list CAMFORD-NETBLOCKS-v1 standard deny any
access-list ANY-TO-ANY extended permit ip any any log critical
access-list CAMFORD-CENTRAL-SERVICES-v1 extended permit ip any 172.16.1.0
255.255.255.0
access-list CAMFORD-CENTRAL-SERVICES-v1 extended permit ip any 172.16.16.0
255.255.255.0
access-list CAMFORD-CENTRAL-SERVICES-v1 extended permit tcp any any eq ssh log
alerts
access-list CAMFORD-CENTRAL-SERVICES-v1 extended permit tcp any any object-
```

```
group MSRDP log alerts  
access-list inside_nat0_outbound extended permit ip any 172.16.154.0 255.255.254.0 log  
critical  
access-list Split_Tunnel_List remark allow only our traffic  
access-list Split_Tunnel_List standard permit 172.16.0.0 255.255.0.0  
access-list Split_Tunnel_List standard permit 192.168.1.0 255.255.255.0  
access-list CAMFORD_splitTunnelAcl standard permit 172.16.0.0 255.255.0.0  
access-list CAMFORD_splitTunnelAcl standard permit 192.168.1.0 255.255.255.0  
access-list CAMFORD-NOSMS extended deny tcp any object-group SMS_Servers eq  
www log alerts  
access-list CAMFORD-NOSMS extended deny tcp any object-group SMS_Servers eq  
https log alerts
```

10. Configure the logging options:

```
logging enable  
logging timestamp  
logging console critical  
logging buffered warnings  
logging trap informational  
logging asdm informational  
logging facility 16  
logging device-id hostname  
logging host inside <IP Address of SYSLOG Server>
```

11. Configure MTU size and ICMP:

```
mtu inside 1500  
mtu outside 1500  
mtu management 1500  
icmp unreachable rate-limit 1 burst-size 1  
icmp permit 172.16.0.0 255.255.0.0 inside
```

```
icmp permit 192.168.1.0 255.255.255.0 inside
```

```
icmp permit 10.0.1.0 255.255.255.0 outside
```

12. Configure IP Address Local Pool and NAT:

```
ip local pool CAMFORD-LOCAL-POOL-v1 172.16.150.20-172.16.151.253 mask  
255.255.254.0
```

```
nat (inside) 0 access-list inside_nat0_outbound
```

```
nat (inside) 0 0.0.0.0 0.0.0.0
```

```
static (inside,outside) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
```

13. Configure the ASA Timeout values:

```
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
```

14. Configure LDAP Attribute Map, to map LDAP attributes to meaningful names:

```
ldap attribute-map AD-Group-Mapping
```

```
map-name memberOf IETF-Radius-Class
```

```
map-value memberOf CN=maths,OU=groups,OU=SCIENCE,DC=camford,DC=ac,DC=uk  
mathsstaff
```

15. Configure Dynamic Access Policies to be applied depending on LDAP attributes:

```
dynamic-access-policy-record DfltAccessPolicy
```

```
network-acl CAMFORD-CENTRAL-SERVICES-v1
```

```
network-acl CAMFORD-NOSMS
```

```
dynamic-access-policy-record CAMFORD-DAP-MATHSSTAFF-v1
```

```
network-acl CAMFORD-MATHSSTAFF-v1
```

```
network-acl CAMFORD-CENTRAL-SERVICES-v1
```

```
network-acl CAMFORD-NOSMS
```

16. Enable WebServer:

```
http server enable  
http 0.0.0.0 0.0.0.0 outside  
http 172.16.0.0 255.255.0.0 inside  
http 172.16.1.0 255.255.255.0 management  
http redirect outside 80  
http redirect inside 80
```

17. Configure SNMP:

```
snmp-server host inside <SNMP Monitoring IP> community public version 2c  
snmp-server host inside <SNMP Monitoring IP> community public version 2csnmp-server  
location <LOCATION>  
snmp-server contact <EMAIL>  
snmp-server community <COMMUNITY>  
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

18. Crypto Map configuration is entirely dependent on the cryptography features required. The cryptomap command in the Cisco ASA allows the configuration of the cryptography features outlined in section 5.5.4 with specific reference to FIPS 140-2 Compliance.

19. IDS: Configure the basic, built-in IDS code:

```
threat-detection basic-threat  
threat-detection statistics
```

20. NTP:

```
ntp server <IP of Server1> source inside prefer  
ntp server <IP of Server2> source inside
```

21. WebVPN Configuration can be implemented in as little as eight stages. Section 8.2 explores web-based portals in more detail:

```
webvpn  
enable outside  
http-proxy <Web Proxy IP> 3128
```

```
https-proxy <Web Proxy IP> 3128  
svc enable  
smart-tunnel list "RDP_SSH" "PuTTY" "putty.exe"  
smart-tunnel list "RDP_SSH" "MSRDP" "mstsc.exe"
```

22. Configure the default VPN Group Policy:

```
group-policy DfltGrpPolicy attributes  
downtime messages etc. NOT the AUP!  
wins-server value <WINS IP – If Required>  
dns-server value <DNS Server1> <DNS Server2>  
vpn-tunnel-protocol IPSec I2tp-ipsec svc webvpn  
password-storage enable  
ip-comp enable  
re-xauth enable  
pfs enable  
ipsec-udp enable  
split-tunnel-policy tunnelspecified  
split-tunnel-network-list value Split_Tunnel_List  
default-domain value camford.ac.uk  
secure-unit-authentication enable  
user-authentication enable  
user-authentication-idle-timeout none  
backup-servers clear-client-config  
address-pools value CAMFORD-LOCAL-POOL-v1  
webvpn  
url-list value Camford  
smart-tunnel enable RDP_SSH
```

file-entry disable

file-browsing disable

23. Configure the VPN Tunnel Groups:

tunnel-group DefaultRAGroup general-attributes

address-pool CAMFORD-LOCAL-POOL-v1

authentication-server-group CAMFORD-AD-v1

strip-realm

tunnel-group DefaultRAGroup webvpn-attributes

nbns-server <WINS Server> timeout 2 retry 2

nbns-server <WINS Server2> timeout 2 retry 2

tunnel-group DefaultRAGroup ipsec-attributes

pre-shared-key <SHARED SECRET>

tunnel-group DefaultWEBVPNGroup general-attributes

address-pool CAMFORD-LOCAL-POOL-v1

authentication-server-group CAMFORD-AD-v1

strip-realm

tunnel-group DefaultWEBVPNGroup webvpn-attributes customization CAMFORD-HOME PAGEv1

nbns-server <WINS Server> timeout 2 retry 2

nbns-server <WINS Server2> timeout 2 retry 2

group-alias Default enable

tunnel-group DefaultWEBVPNGroup ipsec-attributes

pre-shared-key <SHARED SECRET>

address-pool CAMFORD-POOL-v1

authentication-server-group CAMFORD-AD-v1

strip-realm

tunnel-group CAMFORD type remote-access

```
tunnel-group CAMFORD general-attributes  
address-pool CAMFORD-LOCAL-POOL-v1  
authentication-server-group CAMFORD-AD-v1  
default-group-policy CAMFORD  
tunnel-group CAMFORD ipsec-attributes  
pre-shared-key <SHARED SECRET>
```

24. Configure a default Class Map for inspection:

```
class-map inspection_default
```

```
match default-inspection-traffic
```

25. Configure an inspection Policy Map:

```
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  
policy-map type inspect dns migrated_dns_map_1  
parameters  
message-length maximum 512
```

26. Configure TACAS+ and default usernames if required:

```
aaa-server CAMFORD-TACACS-v1 protocol tacacs+  
reactivation-mode timed  
max-failed-attempts 5  
aaa-server CAMFORD-TACACS-v1 host <TACACS SERVER1>  
key <SHARED SECRET>  
aaa-server CAMFORD-TACACS-v1 host <TACACS SERVER2>  
key <SHARED SECRET>  
aaa authentication enable console CAMFORD-TACACS-v1 LOCAL  
aaa authentication http console CAMFORD-TACACS-v1 LOCAL  
aaa authentication ssh console CAMFORD-TACACS-v1 LOCAL  
aaa authentication serial console CAMFORD-TACACS-v1 LOCAL  
aaa accounting enable console CAMFORD-TACACS-v1  
aaa accounting serial console CAMFORD-TACACS-v1  
aaa accounting ssh console CAMFORD-TACACS-v1  
aaa accounting command CAMFORD-TACACS-v1  
aaa authorization exec authentication-server  
aaa authorization command CAMFORD-TACACS-v1 LOCAL
```

To verify that the device is in communication with the AAA server use the following command:

```
show aaa-server
```

27. Configure Active Directory LDAP authentication:aaa-server CAMFORD-AD-v1 protocol ldap

aaa-server CAMFORD-AD-v1 host <Domain Controller 1>

ldap-base-dn DC=camford,DC=ac,DC=uk

ldap-scope subtree

ldap-naming-attribute sAMAccountName

ldap-login-password <PASSWORD>

ldap-login-dn <Role Based AD Account>

server-type microsoft

ldap-attribute-map AD-Group-Mapping

aaa-server CAMFORD-AD-v1 host <Domain Controller 2>

ldap-base-dn DC=camford,DC=ac,DC=uk

ldap-scope subtree

ldap-naming-attribute sAMAccountName

ldap-login-password <PASSWORD>

ldap-login-dn <Role Based AD Account>

server-type microsoft

ldap-attribute-map AD-Group-Mapping

aaa-server CAMFORD-AD-v1 host <Domain Controller 3>

ldap-base-dn DC=camford,DC=ac,DC=uk

ldap-scope subtree

ldap-naming-attribute sAMAccountName

ldap-login-password <PASSWORD>

ldap-login-dn <Role Based AD Account>

server-type microsoft

ldap-attribute-map AD-Group-Mapping

28. The Cisco ASA requires an SSL VPN license to allow more than two SSL VPN sessions:

1. Go to: <http://www.cisco.com/go/license> [4]
 2. Enter the SSL VPN Product Authorisation Key (PAK) found on the License Claim Certificate.
 3. Select [All Done]
 4. Enter Serial Number from a 'sh ver | include Number' [Submit]
 5. [Submit]
 6. Once Registration is complete, await email confirmation.
 7. ciscoasa(config)# activation-key [key from email]
29. Once the VPN has been configured the Network Connect AnyConnect Images need to be uploaded:
1. Start the ASDM and connect to the ASA
 2. Configuration -> Remote Access VPN -> Network (Client) Access -> AnyConnect Connection Profiles
 3. Select Access Interfaces: Enable Cisco AnyConnect VPN Client
 4. Upload an AnyConnect Image
 5. Configuration -> Remote Access VPN -> Network (Client) Access -> Advanced -> SSL VPN -> Client Settings
 6. Click +Add
 7. anyconnect-win-2.3.0185-k9.pkg
 8. anyconnect-macosx-i386-2.3.0185-k9.pkg
 9. anyconnect-macosx-powerpc-2.3.185-k9.pkg
 10. anyconnect-linux-2.3.185-k9.pkg
30. The ASA can have a number of Client-Server Plugins for the Web-based VPN portal:
1. Start the ASDM and connect to the ASA
 2. Configuration -> Remote Access VPN -> Clientless SSL VPN Access -> Portal -> Client-Server Plug-ins
 3. Click +Import
 4. Plug-in Name: RDP

5. Remote Server tftp://<SERVER>/ASA/ASAPlugin/rdp-plugin.080130.jar
 6. Click +Import
 7. Plug-in Name: SSH,Telnet
 8. Remote Server tftp://<SERVER>/ASA/ASAPlugin/ssh-plugin.jar
 9. Click +Import
 10. Plug-in Name: SSH,Telnet
 11. Remote Server tftp://<SERVER>/ASA/ASAPlugin/vnc-plugin.080130.jar
28. Finally Miscellaneous configuration: pager lines 24

ftp mode passive

arp timeout 14400

no failover

no vpn-addr-assign aaa

no vpn-addr-assign dhcp

telnet timeout 5

console timeout 0

l2tp tunnel hello 30

service-policy global_policy global

prompt hostname context

no asdm history enable

Further Documentation

Cisco provides more detailed documentation at the following locations:

- Command Line Configuration Guide (v8.0):
<http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/asa80cfg.pdf> [5]
- ASDM User Guide (v6.0):
<http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/asdmug.pdf> [6]
- SSL VPN Certificates:
http://www.cisco.com/warp/public/471/asa_8.x_3rdpartyvendorcert.pdf [7]

Source URL: <https://community.jisc.ac.uk/library/advisory-services/ssl-vpn-configuration-cisco-asa-80>

Links

[1] <http://community.ja.net/system/files/images/tg-vpn-20.jpg>

- [2] <http://community.ja.net/system/files/images/tg-vpn-21.jpg>
- [3] <http://community.ja.net/system/files/images/tg-vpn-22.jpg>
- [4] <http://www.cisco.com/go/license>
- [5] <http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/asa80cfg.pdf>
- [6] <http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/asdmug.pdf>
- [7] http://www.cisco.com/warp/public/471/asa_8.x_3rdpartyvendorcert.pdf