IPSec interoperability between Palo Alto firewalls and Cisco ASA

Tech Note

PAN-OS 4.1

Revision A

Contents

Overview

The intent of this tech note is to show case IPSec interoperability between Palo Alto Network firewalls and Cisco ASA firewall series. We will also detail IPSec configuration, statistics and CLI outputs on both PAN-OS and Cisco ASA.

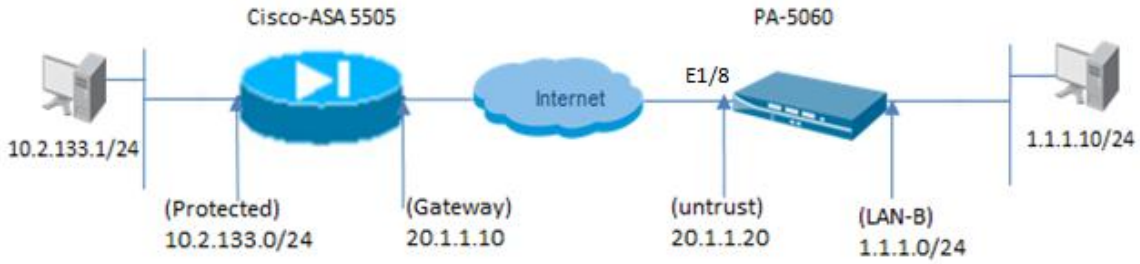
Platforms and Software Versions

The document applies to Cisco ASA and Palo Alto firewalls. However the configuration shown in this document was tested using the following platforms and software versions)

- PA-5060 device running PAN-OS 4.1
- Cisco ASA-5505 running ASA 8.2 with ASDM 6.2

Network topology

In this tech notes we will configure site to site IPSec VPN between Cisco-ASA-5505 and PA-5060 firewalls. We will use VPN wizard in the Cisco ASDM Software and Web-Interface in PAN-OS to configure the VPN configuration. This tech notes uses the following network topology.

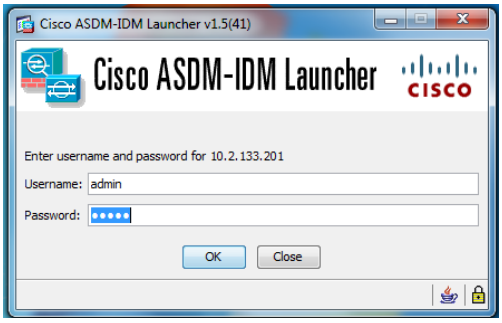


VPN Tunnel Configuration in Cisco ASA 5505

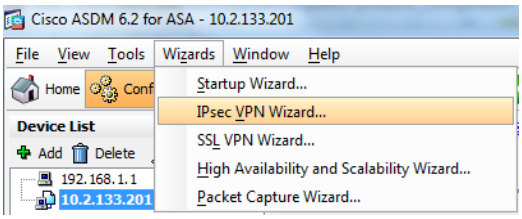
Perform the following steps in order to create a VPN tunnel

- Open your browser and enter https://10.2.133.201 to access the ASDM on Cisco-ASA device. Within browser ASA presents a window (details below) to download/run the ASDM software.

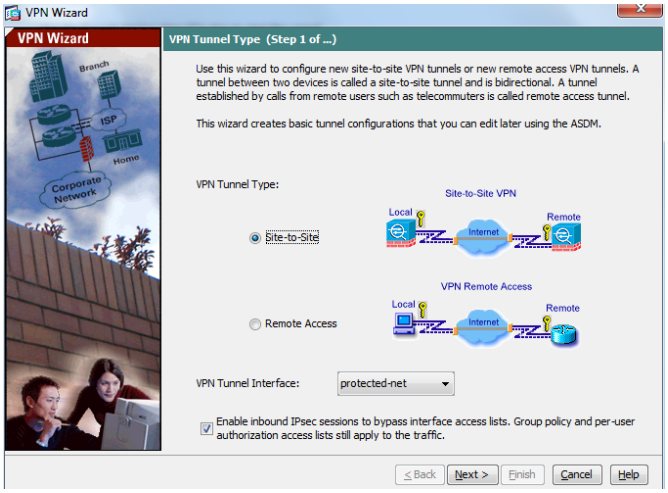
- Click "Run ASDM" and the ASDM installer will be downloaded. Follow the steps directed by the prompts in order to install the software and run the Cisco ASDM Launcher as shown below.



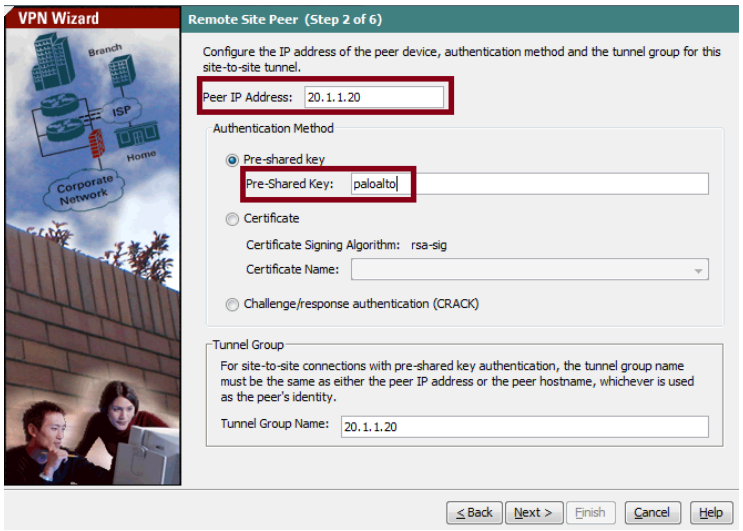
- Run the IPsec VPN Wizard from Wizards tab once the ASDM application connects to the ASA.



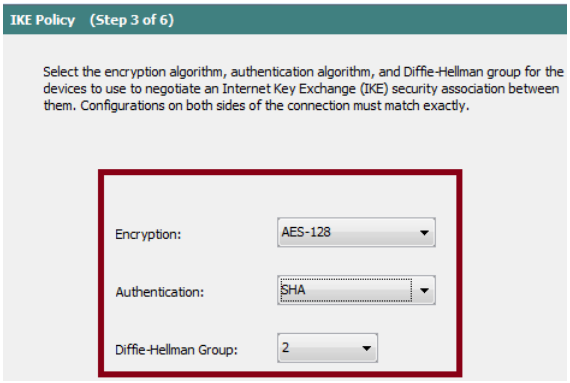
- Choose Site-to-Site for the IPSec VPN Tunnel type, and click Next



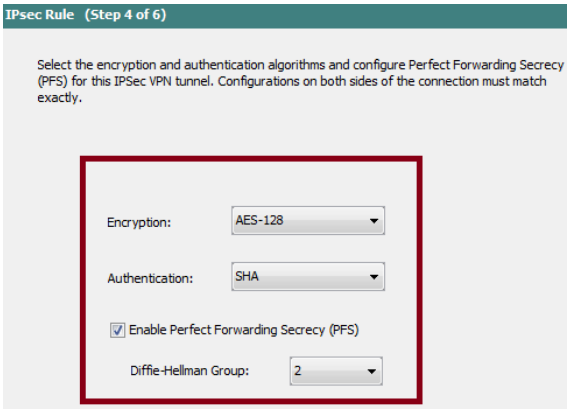
- Specify the outside IP address of the remote peer which is the IKE gateway. In this example this is the interface of the PA 5060 connected to the internet. Enter the authentication information to use, which is the pre-shared key in this example. The pre-shared key used in this example is "paloalto". By default the Tunnel Group Name will be your outside IP address. Click Next.



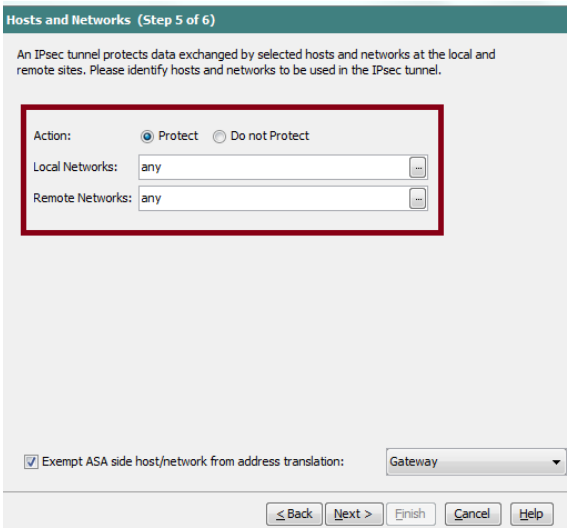
- Specify the attributes for phase 1 negotiation. These must be the same on both the PA-5060 and ASA. Click Next.



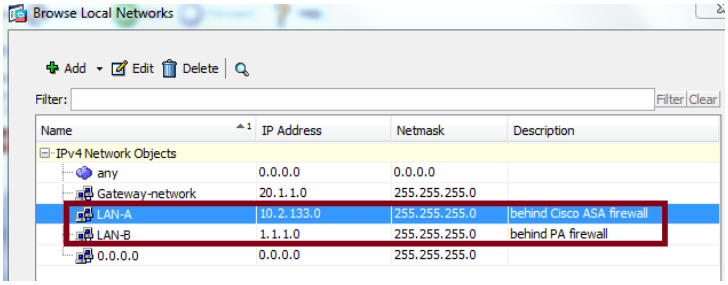
- Specify the attributes to use for Phase 2 negotiation. These attributes must match on both the PA-5060 and the ASA. We have also selected PFS.



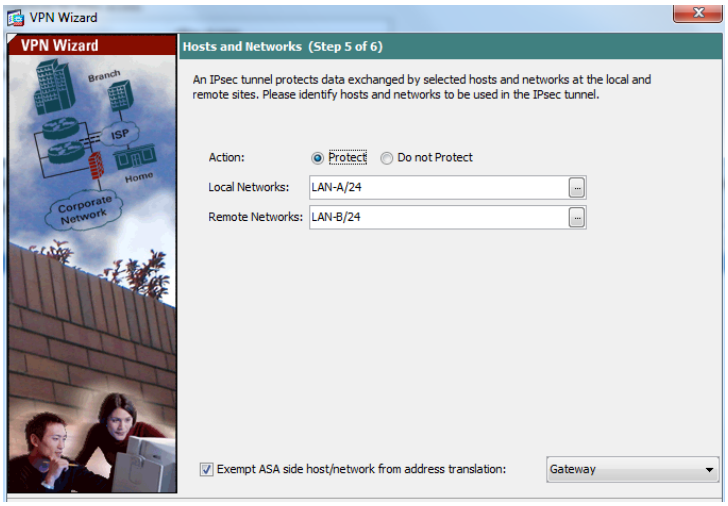
- Specify the network or hosts whose traffic should be allowed to pass through the VPN tunnel that we are about to setup. In this step, you have to provide the Local Networks and Remote Networks for the VPN Tunnel. Click the button next to Local Networks as shown here to choose the local network address from the drop-down menu.



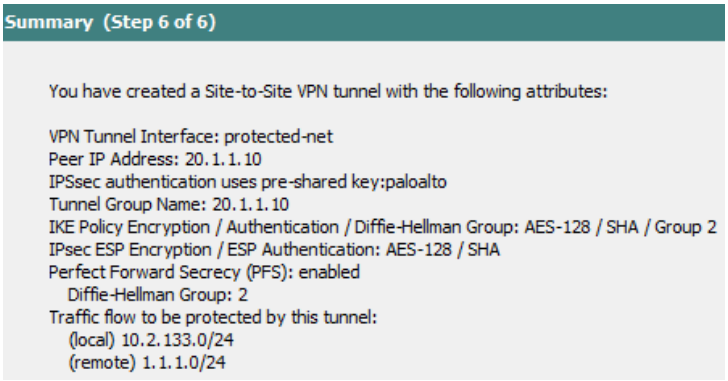
- Choose Local Networks and Remote Networks and click OK. Click Add button and add the Remote Networks. In this example we added LAN-A for the Local Networks and LAN-B for Remote Networks.



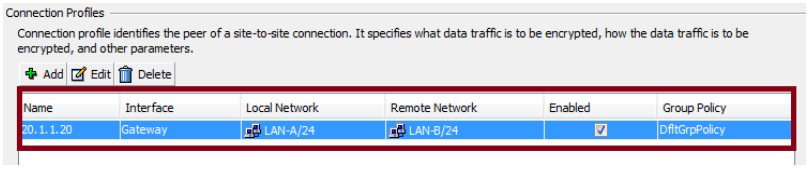
- After choosing the Local and Remote Networks click Next



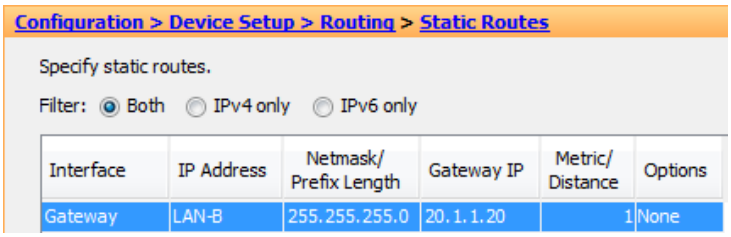
- The attributes defined by the VPN Wizard are displayed in this summary. Double check the configuration and click Finish when you are satisfied that the settings are correct.



- In the Configuration tab of Site-to-Site VPN select connection profiles and you will notice the remote network and local network that is protected via the VPN tunnel that we configured.



- The wizard configures the Firewall Access Rules by default. We have also configured a static route (in red) to access the one network sitting behind the PA-5060 firewall.

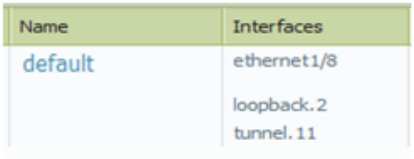


VPN Configuration in PA-5060

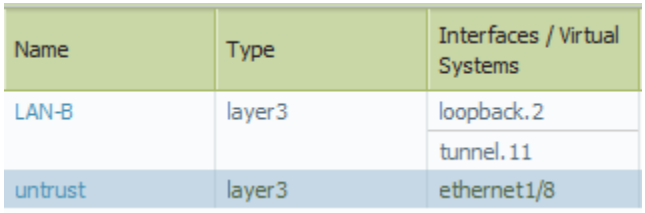
PAN-OS implements route based IPSec VPN's. The VPN traffic is routed by the tunnel interface through the IPSec tunnel. This requires creating a logical tunnel interface. The tunnel interface must be bound to security zone.

- The interface and zone configuration of the PA 5060 is shown below.

  VR Configuration (Network > Virtual Routers)



  Security Zone Configuration (Network > Zones)



Tunnel.11 is the tunnel interface for terminating IPSec tunnel.
Eth1/8 is the IKE gateway interface

- Specify the outside IP address of the remote peer. This is also called as the IKE gateway for the remote peer. Define an IKE crypto profile and specify the profile in IKE Gateway configuration. We need to specify the pre-shared key as well. The pre-shared key used in this example is "paloalto".

IKE Gateway Configuration (Network > Network Profiles > IKE Gateways)

		Local Address		IKE V1 Protocol				
Name	Peer Address	Interface	IP	Exchange Mode	IKE Crypto Profile	DPD Enabled	DPD Interval	DPD Retry
cisco-ASA	20.1.1.10	ethernet1/8		auto	default	☑	5	5

The default IKE crypto profile uses AES 128 or 3DES, SHA-1 and DH group2. To view the IKE crypto profile navigate to (**Network > Network Profiles > IKE Crypto**)

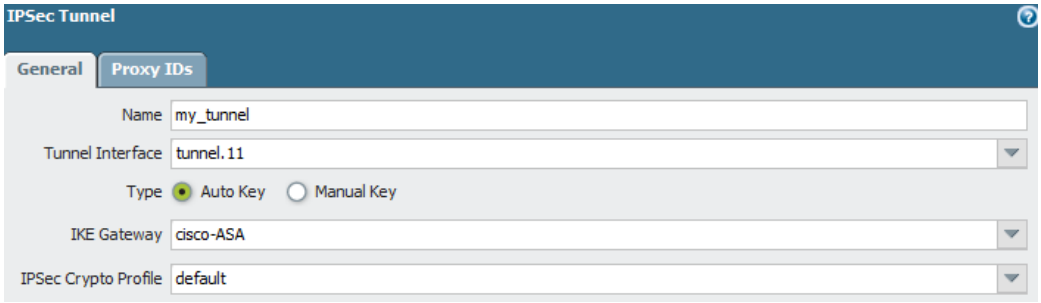
Name	Encryption	Authentication	DH Group
default	aes128, 3des	sha1	group2

- Specify the attributes to use for Phase 2 negotiation. These attributes must match on both the PA-5060 and the ASA. Create an IKE Crypto profile and reference it in IPSec Tunnel configuration.

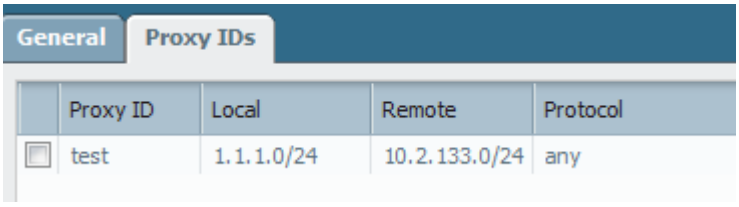
IPSec Crypto profile Configuration (Network > Network Profiles > IPSec Crypto)

Name	ESP/AH	Encryption	Authentication	DH Group	Lifetime
default	ESP	aes128, 3des	sha1	group2	1 hours

- IPSec Tunnel configuration- Specify the tunnel interface created, the IKE gateway and IPSec crypto profile to be used.



- Proxy IDs configuration is as below to match the local and remote network configuration on the Cisco ASA. By default PaloAlto firewalls uses are proxy-id of 0.0.0.0/0 for both local and remote neworks.Without proxy-id the phase2 negotiation will fail.



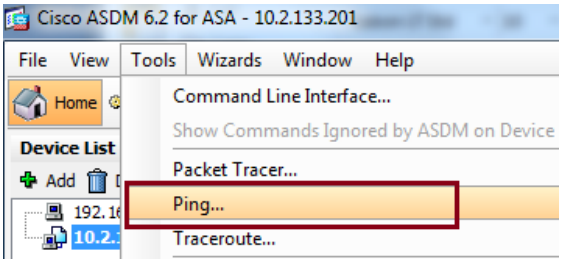
- This screen shot shows the completed IPSec tunnel configuration

Name	Status	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone
my_tunnel	🔴	ethernet1/8	20.1.1.20/24	20.1.1.10	🔴	tunnel.11	vr-cisco (Show Routes)	vsys17	LAN-B

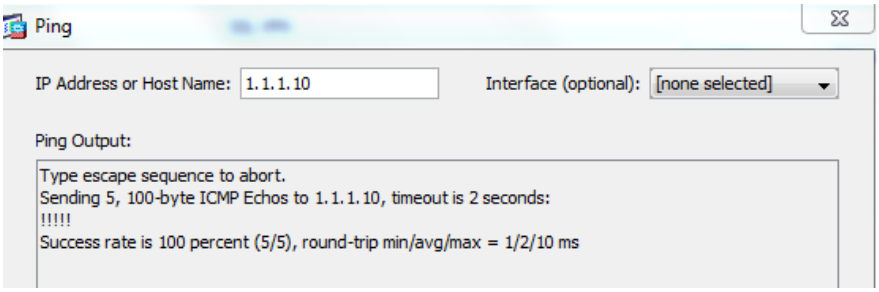
As you notice from the above screen shot, the IPSec tunnel my_tunnel is in "LAN-B" and in virtual router "vr-cisco". At this point of time, phase 1 and phase 2 Security Associations status are down

Verification

Initiate traffic from host protected by Cisco ASA to a host sitting behind PA-5060 firewall. Examine the logs on Cisco ASA and also in PA-5060. You can also run the Ping utility from the tools Tab of the ASDM application to initiate traffic from the ASA to verify the tunnel establishment



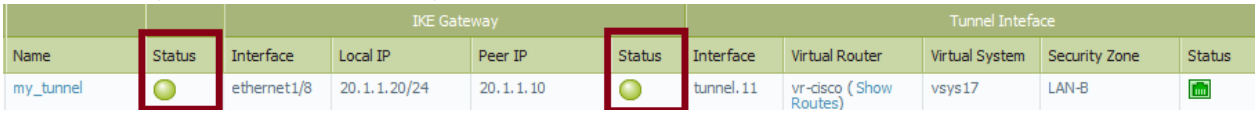
- Ping hosts in protected network sitting behind PA-5060



Confirmation on PA-5060

When the IPSec tunnel is up, the phase 1 and phase 2 statuses on the tunnel should turn to green color.

Tunnel status (Network > IPSec Tunnels)

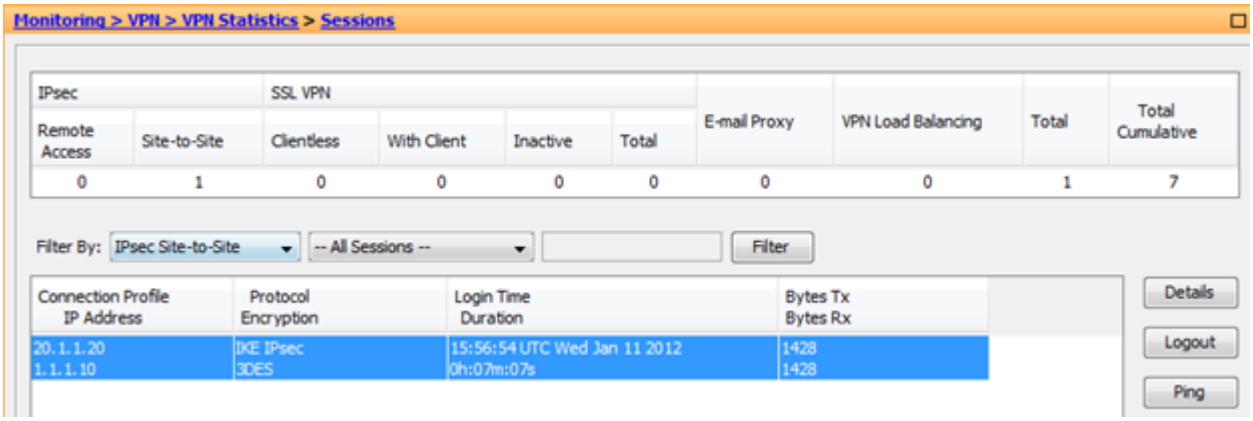


		IKE Gateway				Tunnel Inteface				
Name	Status	Interface	Local IP	Peer IP	Status	Interface	Virtual Router	Virtual System	Security Zone	Status
my_tunnel		ethernet1/8	20.1.1.20/24	20.1.1.10		tunnel.11	vr-cisco (Show Routes)	vsys17	LAN-B	

```
admin@PA-5060-1> show vpn flow

id    name                 state     monitor     local-ip        peer-ip         tunnel-i/f
------------------------------------------------------------------------------------------------------
6     my_tunnel:test       active    off         20.1.1.20       20.1.1.10       tunnel.11

admin@PA-5060-1> show vpn flow name my_tunnel:test

        state:                  active
        proxy-id local ip:      1.1.1.10/24
        proxy-id remote ip:     10.2.133.201/24

        encap packets:          1039
        decap packets:          586
        encap bytes:            108136
        decap bytes:            61024
```

Confirmation on Cisco ASA-5505

Check the Monitoring tab of ASDM for VPN Statistics and the sessions



Appendix

Cisco ASA Configuration (CLI)

```
ciscoasa(config)# show running-config
: Saved
:
ASA Version 8.2(1)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
name 1.1.1.0 one-network description behind PA firewall
name 10.2.133.0 AccessInternet
!
!--- Configure the IKE Gateway interface.
!
interface Vlan1
 nameif Gateway
 security-level 100
 ip address 20.1.1.10 255.255.255.0
!
!--- Configure interface for protected network
!
interface Vlan2
 nameif protected-net
 security-level 100
 ip address 10.2.133.201 255.255.255.0
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
```

```
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
!
ftp mode passive
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
access-list ouside_access_in extended permit tcp any any inactive
access-list inside_1_cryptomap extended permit ip AccessInternet
255.255.255.0 one-network 255.255.255.0
access-list inside_access_in extended permit ip any any
access-list ouside_access_in_1 extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu protected-net 1500
mtu Gateway 1500
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-621.bin
no asdm history enable
arp timeout 14400
access-group ouside_access_in in interface protected-net control-plane
access-group ouside_access_in_1 in interface protected-net per-user-override
access-group inside_access_in in interface Gateway per-user-override
route protected-net 0.0.0.0 0.0.0.0 10.2.0.1 1
route Gateway one-network 255.255.255.0 20.1.1.20 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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 protected-net
http authentication-certificate protected-net
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!--- PHASE 2 CONFIGURATION ---!
!--- The encryption types for Phase 2 are defined here.
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto map inside_map 1 match address inside_1_cryptomap
```

```
crypto map inside_map 1 set pfs group5
crypto map inside_map 1 set peer 20.1.1.20
crypto map inside_map 1 set transform-set ESP-3DES-SHA
crypto map inside_map 1 set nat-t-disable

!--- Specifies the interface to be used with
!--- the settings defined in this configuration.
crypto map inside_map interface Gateway

!--- PHASE 1 CONFIGURATION ---!
!--- This configuration uses isakmp policy 10.
!--- The configuration commands here define the Phase
!--- 1 policy parameters that are used.

crypto isakmp enable protected-net
crypto isakmp enable Gateway
crypto isakmp policy 10

 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400

crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
no crypto isakmp nat-traversal
telnet 10.0.0.0 255.0.0.0 protected-net
telnet timeout 5
ssh 0.0.0.0 0.0.0.0 protected-net
ssh timeout 5
console timeout 0
management-access protected-net

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username admin password eY/fQXw7Ure8Qrz7 encrypted
username krishna password 9GwhR3noRnfN5ayq encrypted privilege 15
tunnel-group 20.1.1.20 type ipsec-l2l
tunnel-group 20.1.1.20 ipsec-attributes
 pre-shared-key *
!
!
prompt hostname context
Cryptochecksum:36733e7ef09893db8966a4fc00899b2e
: end
```