

First Site : Result of « sh ru »

!

hostname XXXXXX

names

ip local pool POOL_VPN 192.168.5.150-192.168.5.190 mask 255.255.255.0

!

interface GigabitEthernet1/1

speed 1000

duplex full

nameif outside

security-level 0

ip address XXXXXXXX

!

interface GigabitEthernet1/2

speed 100

duplex full

nameif inside

security-level 100

ip address 192.168.5.254 255.255.255.0

!

interface GigabitEthernet1/3

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/4

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/5

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/6

shutdown

no nameif

no security-level

no ip address

!

interface GigabitEthernet1/7

speed 100

duplex full

nameif telephonie

security-level 100

no ip address

!

interface GigabitEthernet1/7.100

vlan 100

nameif tel

security-level 100

ip address 10.10.1.1 255.255.255.0

!

interface GigabitEthernet1/8

shutdown

no nameif

no security-level

```
no ip address
!
interface Management1/1
management-only
no nameif
no security-level
no ip address
!
ftp mode passive
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network obj_any
subnet 0.0.0.0 0.0.0.0
object network NETWORK_OBJ_192.168.1.0_24
subnet 192.168.1.0 255.255.255.0
object network NETWORK_OBJ_192.168.5.0_24
subnet 192.168.5.0 255.255.255.0
object network NETWORK_OBJ_192.168.3.0
host 192.168.3.0
object network NETWORK_OBJ_192.168.3.0_24
subnet 192.168.3.0 255.255.255.0
object network NETWORK_OBJ_192.168.5.128_26
subnet 192.168.5.128 255.255.255.192
object network Port_Sonicwall
subnet 192.168.5.0 255.255.255.0
description XXXXX
object network SERVEUR
host 192.168.5.101
object network IPBX
host 10.10.1.200
object service 5001
```

service tcp source eq 5001 destination eq 5001
object service https
service tcp source eq https destination eq https
object service 123
service tcp source eq 123 destination eq 123
object service 2528
service tcp source eq 2528 destination eq 2528
object service 15000
service tcp source eq 15000 destination eq 15000
object service sip
service udp source eq sip destination eq sip
object service ssh
service tcp source eq 2222 destination eq ssh
object service 5090
service tcp source eq 5090 destination eq 5090
object service 5090_udp
service udp source eq 5090 destination eq 5090
object service 2195
service tcp source eq 2195 destination eq 2195
object service 2196
service tcp source eq 2196 destination eq 2196
object network reseau_tel
subnet 10.10.1.0 255.255.255.0
object network obj_any_tel
subnet 0.0.0.0 0.0.0.0
object network IPBX_5001
host 10.10.1.200
object network IPBX_SSH
host 10.10.1.200
object network IPBX_5060
host 10.10.1.200

object network ipbx_5090

host 10.10.1.200

object network IPBX_5060_TCP

host 10.10.1.200

object network IPBX_5061

host 10.10.1.200

object network IPBX_5061_TCP

host 10.10.1.200

object network IPBX_443

host 10.10.1.200

object network LAN_CAVS

subnet 192.168.1.0 255.255.255.0

object network TEL_CAVS

subnet 10.10.2.0 255.255.255.0

object network IPBX_9000_9398

host 10.10.1.200

object network IPBX_10600_10998

host 10.10.1.200

object service Webclients3CX_9000_9398

service tcp source range 9000 9398 destination range 9000 9398

object service ClientWindows3CX_10600_10998

service tcp source range 10600 10998 destination range 10600 10998

object-group network VPN_CAVS

network-object object LAN_CAVS

network-object object TEL_CAVS

object-group network VPN

network-object 10.10.1.0 255.255.255.0

network-object 192.168.5.0 255.255.255.0

access-list outside_access_in extended permit ip any any

access-list outside_access_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list global_access extended permit ip any any

```
access-list inside_access_in extended permit ip any any
access-list 120 remark for NAT
access-list 120 extended deny ip 192.168.5.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list 120 extended deny ip 10.10.1.0 255.255.255.0 10.10.2.0 255.255.255.0
access-list VPN_ACCESS_splitTunnelAcl standard permit any4
access-list VPN_ACCESS_splitTunnelAcl standard permit 10.10.1.0 255.255.255.0
access-list outside_cryptomap extended permit ip object-group VPN object-group VPN_CAVS
access-list TEL_access_in extended permit ip any any
access-list TEL_access_in extended permit ip 10.10.1.0 255.255.255.0 192.168.5.0 255.255.255.0
access-list TEL_access_in extended permit icmp 10.10.1.0 255.255.255.0 192.168.5.0 255.255.255.0
access-list tel_access_in extended permit ip any any
access-list tel_access_in extended permit ip 10.10.1.0 255.255.255.0 192.168.5.0 255.255.255.0
access-list telephonie_access_in extended permit ip any any
access-list telephonie_access_in extended permit ip 10.10.1.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list 111 remark interesting traffic myside to remote side
access-list 111 extended permit ip 192.168.5.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list 111 extended permit ip 10.10.1.0 255.255.255.0 10.10.2.0 255.255.255.0
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu telephonie 1500
mtu tel 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
```

arp rate-limit 16384

nat (inside,outside) source static NETWORK_OBJ_192.168.5.0_24 NETWORK_OBJ_192.168.5.0_24
destination static NETWORK_OBJ_192.168.3.0 NETWORK_OBJ_192.168.3.0 no-proxy-arp route-
lookup

nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.5.128_26
NETWORK_OBJ_192.168.5.128_26 no-proxy-arp route-lookup

nat (inside,outside) source static any any destination static NETWORK_OBJ_192.168.1.0_24
NETWORK_OBJ_192.168.1.0_24 no-proxy-arp route-lookup

nat (inside,outside) source static NETWORK_OBJ_192.168.5.0_24 NETWORK_OBJ_192.168.5.0_24
destination static NETWORK_OBJ_192.168.1.0_24 NETWORK_OBJ_192.168.1.0_24 no-proxy-arp
route-lookup

nat (inside,outside) source static VPN VPN destination static VPN_CAVS VPN_CAVS no-proxy-arp
route-lookup

nat (inside,outside) source static VPN VPN destination static NETWORK_OBJ_192.168.1.0_24
NETWORK_OBJ_192.168.1.0_24 no-proxy-arp route-lookup

!

object network obj_any

nat (inside,outside) dynamic interface

object network obj_any_tel

nat (tel,outside) dynamic interface

object network IPBX_5001

nat (tel,outside) static interface service tcp 5001 5001

object network IPBX_SSH

nat (tel,outside) static interface service tcp ssh 2222

object network IPBX_5060

nat (tel,outside) static interface service udp sip sip

object network ipbx_5090

nat (tel,outside) static interface service tcp 5090 5090

object network IPBX_5060_TCP

nat (tel,outside) static interface service tcp sip sip

object network IPBX_5061

nat (tel,outside) static interface service udp 5061 5061

object network IPBX_5061_TCP

nat (tel,outside) static interface service tcp 5061 5061

```
object network IPBX_443
  nat (tel,outside) static interface service tcp https https
  access-group outside_access_in in interface outside
  access-group inside_access_in in interface inside
  access-group telephonie_access_in in interface telephonie
  access-group tel_access_in in interface tel
  access-group global_access global
  route outside 0.0.0.0 0.0.0.0 XXXXXXXXXXXXXXXXXXXxxx 1
  timeout xlate 3:00:00
  timeout pat-xlate 0:00:30
  timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 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
  timeout floating-conn 0:00:00
  timeout conn-holddown 0:00:15
  timeout igp stale-route 0:01:10
  user-identity default-domain LOCAL
  aaa authentication login-history
  http server enable
  http 192.168.5.0 255.255.255.0 inside
  http 10.10.1.0 255.255.255.0 tel
  no snmp-server location
  no snmp-server contact
  service sw-reset-button
  crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
  crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
  crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
  crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
  crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
```


crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
protocol esp encryption aes-192
protocol esp integrity sha-1 md5

```
crypto ipsec ikev2 ipsec-proposal AES
protocol esp encryption aes
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption 3des
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 65535 set ikev1 transform-set ESP-AES-128-
SHA ESP-AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-
3DES-SHA ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
crypto map outside_map 1 match address outside_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer XXXXXXXXX
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5 ESP-AES-192-
SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-MD5 ESP-DES-
SHA ESP-DES-MD5
crypto map outside_map 1 set ikev2 ipsec-proposal DES 3DES AES AES192 AES256
crypto map outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTOMAP
crypto map outside_map interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha
```

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 20

encryption aes

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 30

encryption 3des

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 policy 40

encryption des

integrity sha

group 5 2

prf sha

lifetime seconds 86400

crypto ikev2 enable outside

crypto ikev2 enable inside

crypto ikev2 enable telephonie

crypto ikev2 enable tel

crypto ikev1 enable outside

crypto ikev1 enable inside

crypto ikev1 enable telephonie

crypto ikev1 enable tel

crypto ikev1 policy 10

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 20

authentication rsa-sig

encryption aes-256

hash sha

group 2

lifetime 86400

crypto ikev1 policy 40

authentication pre-share

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 50

authentication rsa-sig

encryption aes-192

hash sha

group 2

lifetime 86400

crypto ikev1 policy 70

authentication pre-share

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 80

authentication rsa-sig

encryption aes

hash sha

group 2

lifetime 86400

crypto ikev1 policy 100

authentication pre-share

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 110

authentication rsa-sig

encryption 3des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 130

authentication pre-share

encryption des

hash sha

group 2

lifetime 86400

crypto ikev1 policy 140

authentication rsa-sig

encryption des

hash sha

group 2

lifetime 86400

telnet 10.10.1.0 255.255.255.0 tel

telnet timeout 5

ssh stricthostkeycheck

ssh timeout 5

```
ssh key-exchange group dh-group1-sha1
console timeout 0
no ipv6-vpn-addr-assign aaa
no ipv6-vpn-addr-assign local
dhcpd address 192.168.5.20-192.168.5.35 inside
dhcpd dns 192.168.5.210 interface inside
!
dhcpd address 10.10.1.10-10.10.1.20 tel
dhcpd dns 1.0.0.1 1.1.1.1 interface tel
dhcpd enable tel
!
threat-detection basic-threat
threat-detection statistics port
threat-detection statistics protocol
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
vpn-tunnel-protocol ikev1 ikev2
vpn-tunnel-protocol ikev1 ikev2
group-policy VPN_ACCESS internal
group-policy VPN_ACCESS attributes
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec
split-tunnel-policy tunnelspecified
split-tunnel-network-list value VPN_ACCESS_splitTunnelAcl
dynamic-access-policy-record DfltAccessPolicy
vpn-group-policy VPN_ACCESS
service-type remote-access
tunnel-group VPN_ACCESS type remote-access
tunnel-group VPN_ACCESS general-attributes
address-pool POOL_VPN
```

```
default-group-policy VPN_ACCESS
tunnel-group VPN_ACCESS ipsec-attributes
ikev1 pre-shared-key *****
ikev1 pre-shared-key *****
ikev2 remote-authentication pre-shared-key *****
ikev2 local-authentication pre-shared-key *****
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect netbios
inspect tftp
```

inspect ip-options

!

service-policy global_policy global

prompt hostname context

no call-home reporting anonymous

Cryptochecksum:e003a66d5c8b5f847e6c8ed843586401

: end