Subnets

10.x.x.x/24

10.x.x.x/24

10.x.x.x/24

10.x.x.x/24

10.x.x.x/24

--------------------------------------------

IKE Peer: 199.x.x.x

Type : L2L Role : initiator

Rekey : no State : MM\_ACTIVE

Encrypt : aes-256 Hash : SHA

Auth : preshared Lifetime: 14000

transform: esp-3des esp-sha-hmac no compression

in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }

--------------------------------------------

PSK:

XXXX

--------------------------------------------

\*\*\*\*\*\*\*add fw rule permit auth connector destination ???????\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Configuration > Firewall > Access Rule

-Edit 199.x.x.x & 199.x.x.x to desitnation needed and move up

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

PEER IP(s):

--------------------------------------------

(Miami,FL USA) 199.x.x.x

(Seattle,WA USA) 199.x.x.x

Important: Symantec has seen outages occur if the Phase 2 Timeout value is set to longer than four (4)

hours. If the current setting is less than four hours, you can leave that value. Otherwise, adjust the time. The

screenshots in the following procedure might not reflect this advisory.

###############################################################################################################

\*\*\*\*\*\*\*\*\*site-to-site profile\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

crypto ikev1 enable outside

crypto ikev1 policy 2

authentication pre-share

encryption aes-256

hash sha

group 5

lifetime 14000

\*\*\*\*\*\*\*\*\*\*\*\*\*group policy\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

group-policy BlueCoatCloud internal

group-policy BlueCoatCloud attributes

vpn-tunnel-protocol ikev1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*tunnel-group\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

tunnel-group 199.x.x.x type ipsec-l2l

tunnel-group 199.x.x.x general-attributes

default-group-policy BlueCoatCloud

tunnel-group 199.x.x.x ipsec-attributes

ikev1 pre-shared-key xxxxx

tunnel-group 199.x.x.x type ipsec-l2l

tunnel-group 199.x.x.x general-attributes

default-group-policy BlueCoatCloud

tunnel-group 199.x.x.x ipsec-attributes

ikev1 pre-shared-key xxxxxxxx

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*object groups\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

object-group network BlueCoatCloud\_traffic

network-object 10.x.x.x 255.255.255.0

network-object 10.x.x.x 255.255.255.0

network-object 10.x.x.x 255.255.255.0

network-object 10.x.x.x 255.255.255.0

network-object 10.x.x.x 255.255.255.0

object service http

service tcp destination eq www

object service https

service tcp destination eq https

\*\*\*\*\*\*\*\*\*\*\*\*\*ACL\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

access-list BlueCoatCloud\_VPN\_L2L extended permit ip object-group BlueCoatCloud\_traffic any

\*\*\*\*\*\*\*\*\*\*\*\*\*transform set\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

crypto ipsec ikev1 transform-set xxxx-3DES-SHA esp-3des esp-sha-hmac

\*\*\*\*\*\*\*\*\*\*\*\*\*crypto-map (apply on outside interface)\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

crypto map MAP 99 match address BlueCoatCloud\_VPN\_L2L

crypto map MAP 99 set peer 199.x.x.x 199.x.x.x

crypto map MAP 99 set pfs group5

crypto map MAP 99 set ikev1 transform-set xxxx-3DES-SHA

crypto map MAP 99 set nat-t-dis

crypto map MAP interface outside

\*\*\*\*\*\*\*\*\*\*\*\*\*NATs\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

nat (inside,outside) source static BlueCoatCloud\_traffic BlueCoatCloud\_traffic service http http

nat (inside,outside) source static BlueCoatCloud\_traffic BlueCoatCloud\_traffic service https https