Datastream Communications Specification Site to Site VPN

Copyright Notice:

Application	Datastream
Classification	UN-CLASSIFIED
Version	1.0.
Location	Sharepoint
Approval	Broker Enquiries

Status	Effective date	Review date	Expiry date	Owner	Inquiries contact
Final	15th May 2017	15th May 2018	N/A	ASIC IT	Broker Enquiries

1.   Contents

2.   Overview

This document specifies the method for connection to the Australian Securities And Investments Commission Datastream application.

The legacy connection method for Datastream has been achieved using Frame Relay technologies. This method is no longer used for new Datastream connections. The replacement technology approved for Datastream communication with ASIC is a Site to Site Virtual Private Network (VPN). Existing Frame Relay connections are in the process of being migrated over to new VPN's replacing the connection.

The sections below define the requirements for both ASIC and the Datastream customer. This ensures the VPN endpoint meets the preferred security specifications which are mandated by the Australian Signals Directorate for Australian Commonwealth agencies. The VPN's established use Internet Protocol security (IPsec) to protect communications over IP networks. The protocols are well defined and considered to be standard best practice for securing communications.

All VPN's established will terminate at our primary datacenter. If a secondary VPN link is required it will terminate at our secondary datacenter.

It should be noted that any costs incurred by the customer for internet services, associated equipment, configuration and support are the sole responsibility of the connecting customer.

3.   VPN Configuration Settings

The ASD specifies minimum requirements for protocol selection and key length etc (refer reference 5) which ASIC being a Commonwealth Agency must adhere to. Of course the preferred and/or minimum security settings are subject to change over time.

The tables below indicate the desired ASIC Site to Site VPN configuration settings. The cells shaded yellow indicates data needs to be added by the connecting agency and supplied to ASIC. Please contact ASIC if you are unsure about meeting the required settings or if you have questions around the protocol selections or settings.

Primary VPN Endpoint

| IP SEC TUNNEL MODE VPN PARAMETERS FOR CONNECTING TO ASIC			
Agency	**AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION**		*connecting agency*
VPN Device type	Checkpoint Firewall R75.40		
VPN Tunnel Endpoint address	119.225.115.131		
Encryption Domain	144.55.14.55, 144.55.14.70		
IKE - Phase 1			
IKE Version	Supports version 1 & 2 [preference is 2]		
Pre Shared Key	Normally provided by ASIC		Normally provided by ASIC
Hash Algorithm	SHA256		SHA256
Encryption Algorithm	AES-256		AES-256
Key Exchange Algorithm	Diffe Hellman Group 19 (256 bit - Elliptical Curve Group) Preferred		
Security Association (SA) Lifetime	7200 seconds		7200 seconds
Negotiation Mode	Main Mode		Main Mode
Use of XAUTH	Disabled		Disabled
IKE - Phase 2			
Encapsulation Mode	Tunnel		Tunnel
Hash Algorithm	SHA256		SHA256
Encryption Algorithm	AES-256		AES-256
Perfect Forward Secrecy	Diffe Hellman Group 19 (256 bit - Elliptical Curve Group) Preferred		
Security Association (SA) Lifetime	3600 seconds		3600 seconds
Contact Info			
VPN Setup	ASIC IT Security - Gateway Operations (co-ordinator)		
Agency Contacts	broker.enquiries@asic.gov.au, gateway.operations@asic.gov.au		

Secondary VPN Endpoint (only if required)

IP SEC TUNNEL MODE VPN PARAMETERS FOR CONNECTING TO ASIC			
Agency	**AUSTRALIAN SECURITIES AND INVESTMENTS COMMISSION**		*connecting agency*
VPN Device type	Checkpoint Firewall R75.40		
VPN Tunnel Endpoint address	203.192.66.157		
Encryption Domain	144.55.14.55, 144.55.14.70		
IKE - Phase 1			
IKE Version	Supports version 1 & 2 [preference is 2]		
Pre Shared Key	Normally provided by ASIC		Normally provided by ASIC
Hash Algorithm	SHA256		SHA256
Encryption Algorithm	AES-256		AES-256
Key Exchange Algorithm	Diffe Hellman Group 19 (256 bit - Elliptical Curve Group) Preferred		
Security Association (SA) Lifetime	7200 seconds		7200 seconds
Negotiation Mode	Main Mode		Main Mode
Use of XAUTH	Disabled		Disabled
IKE - Phase 2			
Encapsulation Mode	Tunnel		Tunnel
Hash Algorithm	SHA256		SHA256
Encryption Algorithm	AES-256		AES-256
Perfect Forward Secrecy	Diffe Hellman Group 19 (256 bit - Elliptical Curve Group) Preferred		
Security Association (SA) Lifetime	3600 seconds		3600 seconds
Contact Info			
VPN Setup	ASIC IT Security - Gateway Operations (co-ordinator)		
Agency Contacts	broker.enquiries@asic.gov.au, gateway.operations@asic.gov.au		

Further clarification on the configuration settings is available as required. Customers translating their source addresses to an ASIC assigned one will allow for existing routing and network configuration to function as intended.
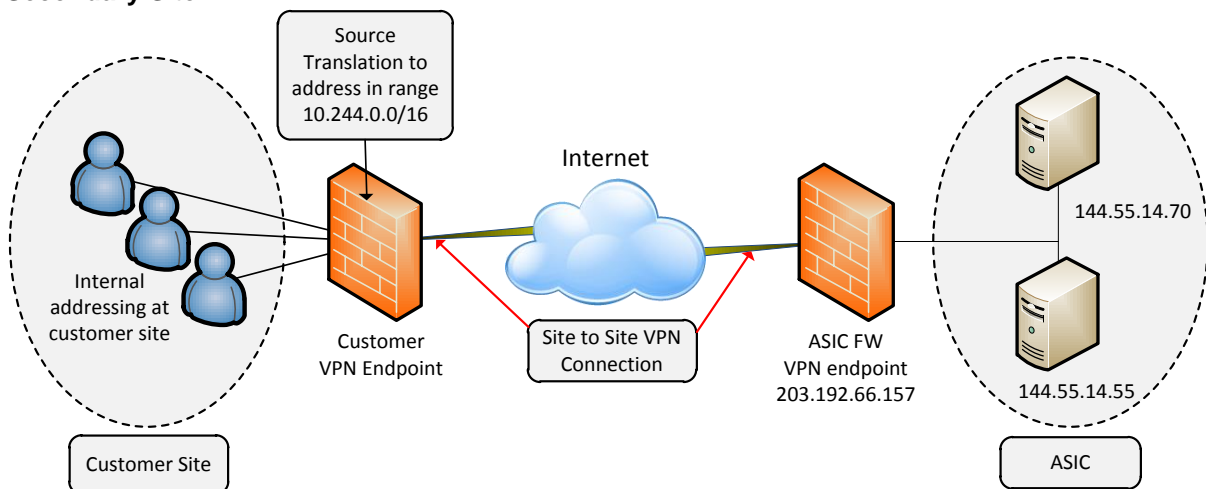
Pre shared keys are usually supplied by ASIC however depending upon configuration requirements the customer can supply the key.

4. Connection Diagram

Primary Site
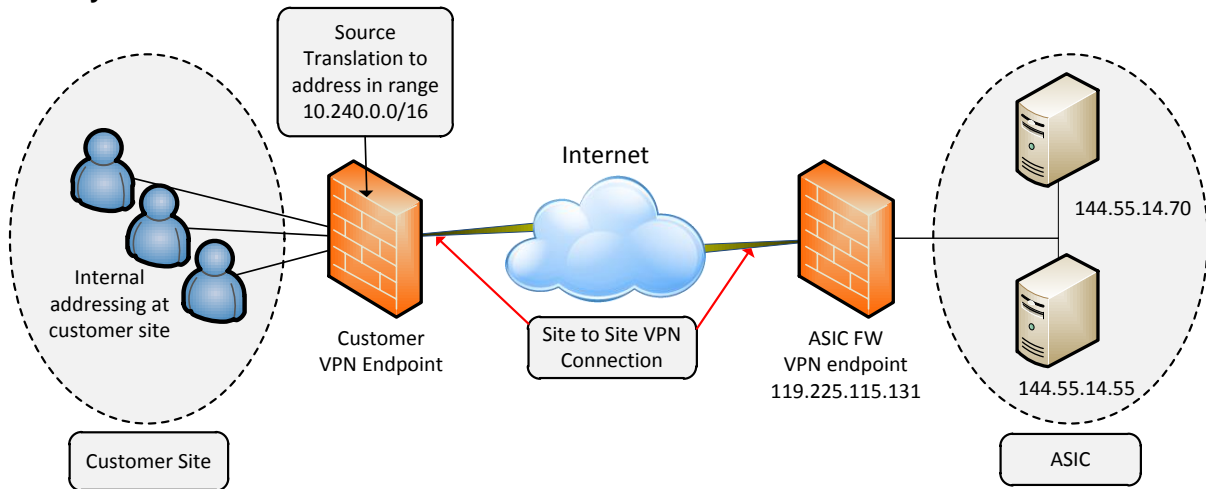
Secondary Site

5.   References

1   ASD Information Security Manual - http://www.asd.gov.au/infosec/ism/