

Black • Vault CA

WatchGuard Integration Guide

VPN Certificate

December 11, 2017

© Engage Black 9565 Soquel Drive Aptos, CA 95003 Phone +1 831.688.1021 1 877.ENGAGE4 (364.2434) <u>sales@engageblack.com</u> <u>support@engageblack.com</u>



About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

This guide describes the Black Vault Certificate Authority (CA) and the procedures to install, use, and troubleshoot the appliance.

Audience

This guide is for security professionals with knowledge of networking and basic security who configure and install the appliance, generate certificates, or monitor logs.

Purpose

The purpose of this guide is to explain how to configure, manage, and troubleshoot the Black Vault CA. This guide contains conceptual and reference information related to the procedures necessary to correctly operate this appliance.

Conventions

The Black Vault CA is configured and administered through a command line interface (CLI). The description of CLI commands follows these syntax conventions:

Curly brackets {} indicate required arguments.

A pipe symbol | indicates valid options for a command word or argument.

Windows sequences are shown as follows: Settings > Network Configuration

ENGAGE BLACK

Engage BlackVault CA WatchGuard Integration Guide

Introduction

VPNs are ubiquitous in enterprise networks. However, in today's age they are getting less and less secure. The most common method of authentication between two endpoints is through a pre-shared key, which can be guessed, or figured out through social engineering. The more secure way to authenticate is through x.509 certificates, this is only more secure though, if the Certificate Authority you obtained your certificates from is secure. The BlackVault CA is a CA with an integrated Hardware Security Module (HSM) that ensures both maximum security and operational simplicity.



The BlackVault CA can safely protect your VPN by providing a reliable and secure source of authentication for the two endpoints of your VPN. It is easy to setup and use Certificate Authority that is simple to weave into your existing WatchGuard VPN, or a brand-new VPN.



ENGAGE BLACK wa

Engage BlackVault CA WatchGuard Integration Guide

To setup the Firebox to use certificates from the BlackVault CA, the following procedures must be accomplished:

- Create a CSR on both Fireboxes.
- Have the BlackVault CA sign the certificates.
- Import the Chain of Trust into the Fireboxes at both ends.
- Import the certificate into the Fireboxes at both ends.
- Configure the Gateway of the Fireboxes at both ends.
- Configure the Tunnel of the Fireboxes at both ends.

This Guide will walk through all the necessary steps to set up a VPN



WatchGuard Web UI Instructions

Setting Up Certificates

The first part of this guide is configuring the certificates that will be used in the VPNs

Site A

Creating A CSR

- 1. Log into the website of the site A's Firebox.
- 2. In the left-hand side of the page select "System".

DASHBOARD Front Panel Subscription Services FireWatch Interfaces Traffic Monitor Gateway Wireless Controller Geolocation Mobile Security Network Discovery SYSTEM STATUS NETWORK FIREWALL SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM



3. In the drop-down menu select "Certificates".

SYSTEM Information Feature Key NTP SNMP WatchGuard Cloud Managed Device Logging Diagnostic Log Diagnostic Log Global Settings Certificates Proxy Auto-Configuration Global Settings Certificates Proxy Auto-Configuration Upgrade OS Backup Image Restore Image Restore Image Technology Integrations USB Drive USB Drive Users and Roles Configuration File Logon Disclaimer

4. In the Certificates web page click "Create Request".

Certificates





5. The Certificate Request Wizard will open. Click "Next" to continue.

Certificates / Create Request

Welcome to the Certificate Request Wizard



To create a third-party CSR (certificate signing request) for this device, complete the steps in this wizard.

6. On the Choose the certificate Function page, select IPSec, Web Server, Other. Then click "Next" to continue.

Certificates / Create Request

Choose the Certificate Function

- Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
- Proxy Server (server certificate for inbound SSL/TLS content inspection)
- IPSec, Web Server, Other



7. On the next page, fill out the details for the Subject Name, then click "Next" to continue.

Certificates / Create Request				
Specify Details for the Subject Name				
Name (CN)		(required)		
Department Name (OU)				
Company Name (O)		(required)		
City/Location (L)				
State/Province (ST)				
Country (C)	US	(required)		

8. On the following page, fill out the Domain Information, then click "Next" to continue.

Certificates / Create Request		
Specify Domain Info	ormation	
Subject Name	CN=Testing, OU=Demo, O=Acme, L=Smallville, S1	(required)
DNS Name	192.168.1.42	(required)
IP Address		
User Domain Name	admin@domain.com	



9. On the Next page select the Algorithm, Length, and Key Usage, then click "Next" to continue

Certificates / Create Request

Select the Algorithm, Length, and Key Usage

Algorithm	RSA ODSA
Length	1024
Key Usage	○ Encryption ○ Signature ● Both

When you click Next, your CSR (Certificate Signing Request) will be generated.

10. On the final Page, it will display the Certificate Signing Request. Copy it all to a notepad and save it. v

Certificate Request Wizard Completed



To generate a signed certificate, copy the text of this Certificate Signing Request and provide it to your Certificate Authority.

After you have submitted the Certificate Signing Request to the Certificate Authority and have received the signed certificate, you can import the certificate to your device. Make sure the CA certificate is also imported. To import a signed certificate now, click **Finish & Import**.

FINISH & IMPORT	FINISH



11. You have successfully completed creating a Certificate Signing Request.

Signing your CSR

- 1. Log into the BlackVault CA.
- 2. Select CA Utilities.

Putty 192.168.1.15 - Putty			
Welcome to th	ne Black Vault CA		
Create Certificate Request	Date:	2017-10-18	
Create Certificate	Time:	10:42:06	
CA Utilities	SSH Port:	22	
Server Utilities	Version:	09.00.05	
System Commands	Firewall:	Off	
Information			-
Revoke Certificate			
Show Certificates and Status			
Show CA Certificates			
Logout			
Press <enter> to select an option</enter>			
Arrow keys to navigate (F2 to go back	(/ Logout to Exit)		



3. Select Import CSR

學 192.168.1.15 - PuTTY		23	J
		^	
CA Utilities			
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR			
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>		*	



4. Paste in the CSR that you just created.

😰 192.168.1.15 - PuTTY	
	•
Copy / Paste CSR and press enter when done	
BEGIN CERTIFICATE REQUEST	
MIIDEDCCAfgCAQAwYzELMAkGA1UEBhMCVVMxDzANBgNVBAgTBkthbnNhczETMBEG	
A1UEBxMKU21hbGx2aWxsZTENMAsGA1UEChMEQWNtZTENMAsGA1UECxMERGVtbzEQ	
MA4GA1UEAxMHVGVzdGluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB	
AM3qivmosbp8KollbZKtzLJInW7c8IGRDARABvd6O4y9EKjGWs4VUayqi6+ng8V4	
3kciNuSFVFDcB15J6UnxVIbEWOBXNsmLA/gViAkmd2LgT46HA7hXA1nZuQ81G0z5	
DcJXzaur1DFAecIJf7AEiZZ9h/X/OjpA2jT7FdsZ6k9gbELQZDZF7VKeQrri8ttU	
9kJI2XXmYSh7SynOH2OOsDPOQvWEnHtDdNWN0CZFJksVGkOxbC7P5yKA2knnoPYr	
Wo13gFCzQ5fQ216MICAky3KFzXma60zDp4U/eFR67wHyVLTuG61n0rYdc9nMCIgE	
vwCVn5wwvWAzvogaOK/chF0CAwEAAaBoMGYGCSqGSIb3DQEJDjFZMFcwKQYDVR0R	
BCIwIIIMMTkyLjE20C4xLjQygRBhZG1pbkBkb21haW4uY29tMAsGA1UdDwQEAwIF	
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUIAgIwDQYJKoZIhvcNAQELBQAD	
ggEBAFwjQS8FCMG8x466Ni0WzJev18e4sDDuMQy2Yn0KQEKStMdtJ6pxHcNHNDGq	
v+OqMz1d63AXJk6X1vXVoAjRtMz08PYb938V8BS9ugbU7QESI4q0hujZeqU6xV9n	
9Iw3GekPoXR/OvyEcrxX5wcrNz03T1A64wcvWAHq5uHbHbtsq0TtrkK91sPJQZso	
V8pUXG8XwkYGiEFFY8uVQu1facTLNGoh9coaGTYj80qIEqlj4Vu36muAaXpAo7PQ	
yuZn1P1q4SpwEjVdL1/4VgAdeaCBNHXBuA6Cm6oIps87MHzkNqs2plIg9/bFepQb	
92TD0FVlqBDHypG0HPvNfZDUKwc=	
END CERTIFICATE REQUEST	-



5. Now back out to the Main Menu and Select Create Certificate

🛃 🛃	2.168.1.15 - PuTTY) <u>23</u>
				*
	Welcome to the Black Vault CA			
	Create Certificate Request Dat	e: 2017-10-18	3	
	Create Certificate Tim	e: 10:42:06		
	CA Utilities SSH Por	t: 22		
	Server Utilities Versio	n: 09.00.05		
	System Commands Firewal	l: Off		
	Information			=
	Revoke Certificate			
	Show Certificates and Status			
	Show CA Certificates			
	Logout			
Press	<pre>s <enter> to select an option</enter></pre>			
Arrow	w keys to navigate (F2 to go back / Logout to Exit)			
				-



6. Select the Common Name of the CSR you wish to sign

19 🛃	22.168.1.15 - PuTTY		23
			^
	Choose a csr to sign		
	as		
	WWWW		
	yhhy		
	aaaaa		
	वेवेवेवे		
	testing		
	TIMMEH		
	EngageBlack		
	TimothyDyck		
	TimDyck		
	Timmehd		
Drag	A (ENTER) to coloct an option		
Arro	s veniers to select an option we keys to payigate (F2 to go back / Logout to Exit)		
ALLO	w keys to havigate (rz to go back / hogout to hkit)		-



7. Select None when asked for extension type

B 192.168.1.15 - PuTTY	• ×
Choose an extension to add to certificate	
<pre>server_ext client_ext email_ext codesigning_ext None</pre>	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>	- -



8. Back out to the main Menu and Select CA Utilities

P 192.168.1.15 - PuTTY	23	J
		•
CA Utilities		
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR		
	=	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>		-



9. Select Export Certificate

🗗 192.168.1.15 - PuTTY	
	•
CA Utilities	
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>	-



10. Select the Certificate that you just created

₽	192.168.1.15 - PuTTY	_		
	Select a certificate t	o export.		
	(Valid/Revoked)	Serial	Subject Name	
	V	100C	CN=aaaaa	
	V	100D	CN=as	
	V	100E	CN=Tim Dyck	
	V	100F	CN=testing	
	V	1010	CN=Timmehd	
	V	1011	CN=testing	



11. Select PEM encoded (Without Key)

🚱 192.168.1.15 - PuTTY 📃	
	^
Select format to export certificate.	
Personal Information Exchange - PKCS#12 (With Key)	
PEM with password - (With Key) DER encoded (Without Key)	
PEM encoded (Without Key)	
Cryptographic Message Syntax Standard - PKCS#7 (Without Key)	
	-



12. Select To USB

و1 🛃	2.168.1.15 - PuTTY	The Owner water of the Owner		<u> </u>	J
				^	•
		Select where to export the (certificate.		
	to USB to SFTP				
				-	1



13. Insert a flash drive to the BlackVault CA and press enter

و1 🛃	2.168.1.15 - PuT	ſγ	-	-					- 0	x
										^
		Seled	ct where	to ex	port th	ne ce	rtific	cate.		
	to USB to SFTP									
		Please e	enter the	USB	device	and	press	<enter></enter>		
										-



Obtaining the CA certificates

1. On a client computer load the website : IP_Address_Of_BVCA/cacerts.pem

① 192.168.1.15/cacerts.pem

☆

2. Open the downloaded cacerts.pem in wordpad



3. Cut the first certificate and in a new document paste it. Save this one as Signing.crt

ENGAGE BLACK

Engage BlackVault CA WatchGuard Integration Guide



4. Save the remainder as root.crt



Importing the Certificates into Firebox

- 1. Log into the website of site A's Firebox.
- 2. In the left-hand side of the page select "System".

DASHBOARD

Front Panel Subscription Services

- FireWatch
- Interfaces
- Traffic Monitor
- Gateway Wireless Controller

Geolocation Mobile Security

- Network Discovery
- SYSTEM STATUS

NETWORK

FIREWALL

SUBSCRIPTION SERVICES

AUTHENTICATION

VPN

SYSTEM

ENGAGE BLACK

Engage BlackVault CA WatchGuard Integration Guide

3. In the drop-down menu select "Certificates".

SYSTEM Information Feature Key NTP SNMP WatchGuard Cloud Managed Device Logging Diagnostic Log Global Settings Certificates Proxy Auto-Configuration Upgrade OS Backup Image Restore Image Restore Image Technology Integrations USB Drive USB Drive Users and Roles Configuration File Logon Disclaimer

4. On the certificates webpage, click "import Certificate/CRL.

Certificates





5. On the Import a Certificate page.

Certificates / Import		
Import a Certificate	Import a CRL	
Certificate Type		
Base64 (PEM) certificate	Ŧ	
Certificate Function Proxy Authority (re-signi Proxy Server (server cer Trusted CA for Proxies IPSec, Web Server, Othe	ገ ing CA certificate for tificate for inbound S r	outbound SSL/TLS content inspection) SL/TLS content inspection)
Import Certificate File		
Choose File cacert1.pem If your certificate repaste the text from key in the text box.	equires a priva both the cert	te key, make sure to ificate and the private
Choose File cacert1.pem If your certificate repaste the text from key in the text box. BEGIN CERTIFICATE MIICL2CCAdSgAwIBAgIJAI AIVTMRMVEQYDVQQIDAY CgMRW5nYWdIIEJsYWN MB4XDTE3MDcyNjE4MDg; EzARBgNVBAgMCKNhbGIr bmdhZ2UgQmxhY2sxDTAL BgcqhkjOPQIBBggqhkjOPC ANDUXBhYviNudK/6SBGG HQ8BAf8EBAMCAQYwDw' v4VZV3Wn3E+LkSIwHwYD KoZIzj0EAwIDSQAwRgIAA AiEAmJuAShbZAZAYo1QG END CERTIFICATE	equires a priva both the cert LJ+IOZI14TxMAoGCC DYWxpZm9ybmlhMC rMQ0wCwYDVQQLD ZNIoXDTI3MDcyNDE mb3JuaWExDjAMBgN BgNVBASMBERIbW8 2MBBwNCAASrthfN6 +f0qnfLQXm2y0vTbN YDVR0TAQH/BAUwA V/R0jBBgwFoAUd3Xt DflvRNjA0aA4VjSiZri 4wmZEdgSfRnu+fcjq	te key, make sure to ificate and the private ARGSM49BAMCMGoxCzAJBgNVBAYT WWDAYDVQQHDAVBcHRvczEVMBMGA1UE AREZW1vMRAwDgYDVQQDDAdSb290IENB IMDgzNIowajELMAkGA1UEBhMCVVMx VBAcMBUFwdG9zMRUwEwYDVQQKDAxF xEDAOBgNVBAMMB1Jvb3QgQ0EwWTAT II3MUmiwwH8BL/1S2bGf80jJjTm DIo3oMLAIEQzB7bo2MwYTAOBgNV wEB/ZAdBgNVHQ4EFgQUd3XbNccQhETS NccQhETSv4VZV3Wn3E+LkSIwCgYI VTe4GgaT6zMU+VEbWzbkLbL2P 3/nI36pBb8=

- a. Under Certificate Function Select IPSec, Web Server, Other.
- b. Under Certificate File Click Choose file, then browse to where you saved Root.crt.
- c. Click Save.



6. On the Import a Certificate page.

Certificates / Import
Import a Certificate Import a CRL
Certificate Type
Base64 (PEM) certificate
 Certificate Function Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection) Proxy Server (server certificate for inbound SSL/TLS content inspection) Trusted CA for Provide
IPSec, Web Server, Other
Import Certificate File: Choose File cacert2.pem If your certificate requires a private key, make sure to paste the text from both the certificate and the private key in the text box.
 BEGIN CERTIFICATE MIICLTCCAdOgAwlBAgICEAAwCgYIKoZlzj0EAwlwajELMAkGA1UEBhMCVVMxEzAR BgNVBAgMCkNhbGImb3JuaWExDjAMBgNVBAcMBUFwdG9zMRUwEwYDVQQKDAxFbmdh Z2UgQmxhY2sxDTALBgNVBAsMBERIbW8xEDAOBgNVBAMMB1Jvb3QgQ0EwHhcNMTcw Nzl2MTgwOTU4WhcNMjcwNzI0MTgwOTU4WjBtMQswCQYDVQQGEwJVUzETMBEGA1UE CAwKQ2FsaWZvcm5pYTEOMAwGA1UEBwwFQXB0b3MxFTATBgNVBAoMDEVuZ2FnZSBC bGFjazENMAsGA1UECwwERGVtbzETMBEGA1UEAwwKU2InbmluZyBDQTBZMBMGByqG SM49AgEGCCqGSM49AwEHA0IABLYAIrhvKW/b4cniYTV6fkx9sDzrtaVdaxLuV7HT E3kRg6043uCt7dW9jkmrHrNqUPOXWbnJI/LB5mXZR2k7oWijZjBkMA4GA1UdDwEB /wQEAwlBBjASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA1UdDgQWBBR16MRydUrvV0w4 eGhu6K0pFic47zAfBgNVHSMEGDAWgBR3dds1xxCERNK/hVIXdafcT4uRIjAKBggq hkjOPQQDAgNIADBFAiBjsgzZ1XE4yLD7PJs6rZmiyDjC+m6L6BiK3SBaT9L0pQIh ALgGhkJ/dGpohL9psjWHSfeEDuU4LpaN4sCj729rgNKF END CERTIFICATE
SAVE CANCEL

- a. Under Certificate Function Select IPSec, Web Server, Other.
- b. Under Certificate File Click Choose file, then browse to where you saved Signing.crt.
- c. Click Save.



7. On the Import a Certificate page.

Certificates / Import			
Import a Certific	ate Import a C		
Certificate Typ	e		
Base64 (PEM) certif	icate 🔻		
Certificate Fun	ction		
Proxy Authority (r	e-signing CA certificat	te for outbound SSL/TLS content inspection)	
Proxy Server (server)	er certificate for inbo	ound SSL/TLS content inspection)	
Trusted CA for Pro	ixies		
IPSec, Web Server	, Other		
Import Certificate File	-		
Choose File No file	chosen		
Onoose The			
If your certifica paste the text key in the text	te requires a p from both the o box.	private key, make sure to certificate and the private	
BEGIN CERTIFI MIIC9TCCApugAwlB BgNVBAgMCkNhbG Z2UgQmxhY2sxDT4 MTcxMTA3MTY1ND A1UECBMISWxsaW bWUxEDAOBgNVB/ hkiG9w0BAQEFAAC TjW4TI9+hfLA0PND M2WWa8l0umEWB2 +Dqp2KFjtEDOJNfi8I Kb3px62J6H3saSiJf jmfqU6W81irAVFkzr YJAJBgNVHRMEAJA YWIuLmNvbTALBgN CAICMAoGCCqGSM Pqobg5W9jwlgGKVI END CERTIFICA	CATE BAGICEBkwCgYIKoZIz Imb3JuaWExDjAMBgN LBgNVBASMBERIbWi QyWhcNMTIxMTA3M '5vaXMxEzARBgNVBA AsrB1RIc3RpbmcxETA VCAQ8AMIIBCgKCAQI EgSDCDIJWAIkv4Dao 2AkSW08rj+UEeI7TmA tW87rFZ2XY+ot/DQWI NLERoydQVH0mJeSg AMCkGA1UdEQQIMC NHQ8EBAMCBaAwH0 M49BAMCA0gAMEUCI ImMvjrGrtNETWqC7of VTE	zj0EAwlwbTELMAkGA1UEBhMCVVMxEzAR INVBAcMBUFwdG9zMRUwEwYDVQQKDAxFbmdh /8xEzARBgNVBAMMCINpZ25pbmcgQ0EwHncN ITY1NDQWJBpMQswCQYDVQQGEwJVUzERMA8G /acTCINtYWxsdmlsbGUxDTALBgNVBAoTBEFj ?APBgNVBAMTCEppbSBEdWNrMIIBIjANBgkq 2EA24EK+/W+6hyc+YRZCO5K3vx0NcU/OwNa o+Cd/WMhbC0nNta8IBnmF8Gp+AuhB0PB A1y7KLTfvibfRQ7FBiwChHDXTwKNjE28/Z VMddHIZ+Iwk2QL80PGgDBaUa2hiVK gJ9sbh9zxHzny8uR6cDWcsPC+5iQxfyC iHc47azbkHrxoagli0j4ukwIDAQABo2Qw CCCDDE5Mi4xNjguMS40MoEQYWRtaW5AZG9t 4QYDVR0IBBYwFAYIKwYBBQUHAwEGCCsGAQUF 2IQCswQLVqp+n61CTCaGHrMw6PkogSFdhqYFP bCxz7y6HJZNCvwjhKL/Czivg=	<u>s</u>
SAVE	CANCEL		

- a. Under Certificate Function Select IPSec, Web Server, Other.
- b. Under Certificate File Click Choose file, then browse to where your flash drive and select the Certificate you exported from the BlackVault.
- c. Click Save.



Site **B**

Repeat Process stated in site a for site b.



Setting up VPN

Before setting up the VPN it is a good idea to collect the following information

- Site A and B external IP addresses
- Site A and B internal network IP addresses
- Site A and B CN from their certificates

Site A

Configuring VPN

- 1. Log into the website of site A's FireBox.
- 2. In the Left-hand side of the page select "VPN"

DASHBOARD SYSTEM STATUS NETWORK FIREWALL SUBSCRIPTION SERVICES AUTHENTICATION VPN SYSTEM



3. Again, in the left-hand side of the page select "Branch Office VPN"

VPN

Branch Office VPN BOVPN Virtual Interfaces Phase 2 Proposals IKEv2 Shared Settings Mobile VPN with IPSec Mobile VPN with SSL Mobile VPN with L2TP Global Settings

4. Under the Gateway section click "Add"

Gateways

a. In the General Settings Tab

ENGAGE BLACK

Engage BlackVault CA WatchGuard Integration Guide

IPSec / Web

General Settings	Phase 1 Settings		
Credential Met	hod		
Use Pre-Shared Key	/		
Use IPSec Firebox 0	Certificate		
Show All Certif	icates		
ID	CERTIFICATE NAME	ALGORITHM	ТҮРЕ
20002	c=US st=Illinois l=Smallville o=Acme ou=Testing cn=Jim Duck	RSA	IPSec / Web
20001	c=US st=Kansas l=Smallville o=DEMO ou=DEMO cn=DEMO	RSA	IPSec / Web
20000	o=Engage Black	DCA	IDCos (Wab

Gateway Endpoint

29000

	LOCAL INTERF	ACE	LOC	CAL TYPE		LOCAL ID	REM	OTE IP	REMOTE TYPE	REMOTE ID
ADD	EDIT	REMO	DVE	MOVE UP)	MOVE DOWN				

RSA

cn=192.168.1.42

Start Phase 1 tunnel when Firebox starts

SAVE CANCEL

- i. For Credential method select "Use IPSec Firebox Certificate" then select the certificate you imported
- ii. For Gateway Endpoint Click "Add"
 - 1. Under the Local Gateway Tab

ENGAGE BLACK Engage BlackVault CA WatchGuard Integration Guide

- a. Select Ecternal Interface as "external"
- b. Under the "Specify the gateway ID for tunnel authentication." Section select "By x500 Name"



2. Under the Remote Gateway Tab

Gateway Endpoint Settings *							
A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.							
Local Gateway	Remote Gateway						
Specify the remote gate	eway IP address for a tunnel.						
Static IP Address	192.168.1.43						
O Dynamic IP Address	5						
Specify the remote gate	eway ID for tunnel authentication.						
By Domain Name							
By User ID on Doma	ain						
By x500 Name	c=US st=Kansas I=Smallvill∈						
Attempt to resolve	domain						
	OK CANCEL						

- a. In the "Specify the remote gateway IP address for a tunnel." Section enter the remote IP address
- b. In the "Specify the remote gateway ID for tunnel authentication" select "By x500 Name" then enter in the Common Name of the remote site's certificate
- 3. Then click "Ok"
- b. In the Phase 1 Settings
 - i. Leave everything to their defaults
- c. Press Save



5. Under the Tunnels section click add

Tu	m	n		lc.
IU			e	ιS

NAME ≑			EDIT/	EDITABLE			
tunnel	.1				Yes		
ADD	CLONE	EDIT	REMOVE	REPORT	MOVE UP	MOVE DOWN	SAVE ORDER

d. In the Addresses Tab

Turinet Noute Sett		
Addresses NAT		
Local IP		
Choose Type	Network IPv4	
Network IP	192.168.241.0 / 24	
Remote IP		
Choose Type	Network IPv4	
Network IP	192.168.85.0 / 24	
Direction bi-directional	Ŧ	
Enable broadcast routing ov	/er the tunnel	
	ОК СА	NCEL

- i. Under Addresses click "Add"
 - 1. For Local IP
 - a. In Choose Type select Network IPv4,

ENGAGE BLACK

Engage BlackVault CA WatchGuard Integration Guide

- b. In Network IP add in the local network
- 2. For Remote IP
 - a. In Choose Type select Network IPv4,
 - b. In Network IP add in the remote network
- 3. For everything leave to defaults, then click "Ok
- ii. For everything else, leave to defaults then press "Save"

Site B

Repeat Process stated in Site A for Site B


WatchGuard System Manager Instructions

Setting Up Certificates

The first part of this guide is configuring the certificates that will be used in the VPNs

Site A

Creating A CSR

1. From the WatchGuard System Manager, open the system manager





2. In the Firebox System Manager, click the Certificates Button



3. In the Certificates window, click Create Request Button

Status	Туре	Algo.	Subject Name	Details
Signed	IPSec / Web	RSA	c=US st=Kansas I=Smallville o=DEMO ou=DEMO	Delete
Signed	IPSec / Web	RSA	o=Engage Black cn=192.168.1.42	Delete
Signed	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web C	Refresh
Signed*	CA Cert	RSA	o=asdf ou=asdf cn=asdf	
Signed	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Export
Signed	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	
Signed	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Update
Signed	Proxy Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=h	
Signed	Provy Authority III	DCA	n-WatchGuard Technologies ou -Fireware cn-Fi	
Show	w trusted CAs for	proxies		



4. In the Certificate Request Wizard, press Next





5. Select the IPSEC, Web Server, Other radio button and press Next





6. Fill out the fields for the Subject-Name and press Next

Certificate Request Wizard				
Configure the fields for the subject name.				
The information here will	be used to generate the subject name			
Name (CN):	Jim Duck	(required)		
Department Name (OU):	Testing			
Company Name (O):	Acme	(required)		
City/Location (L):	Smallville			
State/Province (ST):	Illinois			
Country (C):	US	(required)		
	< Back N	lext > Cancel		



7. Fill out the fields for the Domain Info and press Next

Certificate Request W	lizard	<u> </u>
Configure the remaining domain information.		Guard
Subject Name:	=Jim Duck, OU=Testing, O=Acme, L=Smallville, ST=Illinois, C=US	(required)
DNS Name:	192.168.1.42	(required)
IP Address:		
User Domain Name:	admin@domain.com	
	< Back Next >	Cancel



8. Configure the settings for generating the key and press next

Certificate Rec	quest Wizard	
Specify th	e algorithm, length and key usage	watchGuard
Algorithm:	RSA O DSA	
Length:	1024	
Key Usage:	🔘 Encryption 🔘 Signature 💿 Both	
		< Back Next > Cancel

9. In the Create Certificate Request Window that pops up, Press yes





10. Back in the Certificate Request Wizard window, the newly created certificate request will be displayed. Copy this into a notepad, save the notepad as certificaterequestsitea.csr then click Next

send out your certificate request.	WatchGuard
The following CSR (Certificate Signing Request) has been ger	nerated:
Dg8UPTBsRh3002s25B68aGoCItI+LpMCAwEAAaBoM KQYDVR0RBCIwIIIMMTkyLjE20C4xLjQygRBhZG1pb DwQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIK AQELBQADggEBAA519V/zRZynrpRLGK8wI/UAsOeNO sVFXzbMxBz4VUUk1r66b4oGVzGBp8DJolhf+fPYGb 6ZsU/DJCOeaC3IHr/07yp/SEK0aynRyrL1opaQBER MGEFctXHDRS6nkCCeDwHIr9ZVf03uaa4Uo2Jt2vsz PLhYuawmkZ6rw8fA8MmpR1sAv3mIvWD9/n7uGQ1cN IjW6A1JHMIPeTRKFMhPq4KZAxnhrAweuusM= END CERTIFICATE REQUEST	GYGCSqGSIb3DQEJDjF2MFcw kBkb21haW4uY29tMAsGA1Ud wYBBQUIAgIwDQYJKoZIhvcN UBddK/a8tEhVMkWgKMoMIQX 1BR/tC2VWToXizXMu4z13n7 cegjpGCzhhG8+NCSFg1LWM2 1JPLLFDhObjA+TGsqzt+GuY POmLnTMwLbP9iAJUK2fcBVm
Сору	
	< Back Next > Cancel

ENGAGE BLACK Engage BlackVault CA WatchGuard Integration Guide

11. Press Finish





Signing your CSR

- 1. Log into the BlackVault CA as a operator user.
- 2. Select CA Utilities.

🛃 🗗	2.168.1.15 - PuTTY			
				^
	Welcome t	o the Black Vault CA		
	Create Certificate Request	Date:	2017-11-27	
	Create Certificate	Time:	15:53:02	
	CA Utilities	SSH Port:	22	
	Server Utilities	Version:	09.00.05	
	System Commands	Firewall:	Off	
	Information			=
	Revoke Certificate			
	Show Certificates and Status	3		
	Show CA Certificates			
	Logout			
Press	<pre>s <enter> to select an option</enter></pre>	1		
Arrow	w keys to navigate (F2 to go	back / Logout to Exit)		
				-



3. Select Import CSR

學 192.168.1.15 - PuTTY		23	J
		^	
CA Utilities			
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR			
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>		*	



4. Paste in the CSR that you just created (saved in the file certificate request sitea.csr).

😰 192.168.1.15 - PuTTY	x
	-
Conv / Paste CSR and press enter when done	
BEGIN CERTIFICATE REQUEST	
MIIDEDCCAfgCAQAwYzELMAkGA1UEBhMCVVMxDzANBgNVBAgTBkthbnNhczETMBEG	
A1UEBxMKU21hbGx2aWxsZTENMAsGA1UEChMEQWNtZTENMAsGA1UECxMERGVtbzEQ	
MA4GA1UEAxMHVGVzdGluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB	
AM3qivmosbp8KollbZKtzLJInW7c8IGRDARABvd6O4y9EKjGWs4VUayqi6+ng8V4	
3kciNuSFVFDcB15J6UnxVIbEWOBXNsmLA/gViAkmd2LgT46HA7hXA1nZuQ81G0z5	
DcJXzaur1DFAecIJf7AEiZZ9h/X/OjpA2jT7FdsZ6k9gbELQZDZF7VKeQrri8ttU	
9kJI2XXmYSh7SynOH2OOsDPOQvWEnHtDdNWN0CZFJksVGkOxbC7P5yKA2knnoPYr	
Wo13gFCzQ5fQ216MICAky3KFzXma6OzDp4U/eFR67wHyVLTuG61n0rYdc9nMCIgE	
vwCVn5wwvWAzvogaOK/chF0CAwEAAaBoMGYGCSqGSIb3DQEJDjFZMFcwKQYDVR0R	
BCIwIIIMMTkyLjE20C4xLjQygRBhZG1pbkBkb21haW4uY29tMAsGA1UdDwQEAwIF	
oDAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUIAgIwDQYJKoZIhvcNAQELBQAD	
ggEBAFwjQS8FCMG8x466Ni0WzJev18e4sDDuMQy2Yn0KQEKStMdtJ6pxHcNHNDGq	
v+OqMz1d63AXJk6X1vXVoAjRtMzO8PYb938V8BS9ugbU7QESI4q0hujZeqU6xV9n	
9Iw3GekPoXR/OvyEcrxX5wcrNzO3T1A64wcvWAHq5uHbHbtsq0TtrkK91sPJQZso	
V8pUXG8XwkYGiEFFY8uVQu1facTLNGoh9coaGTYj80qIEqlj4Vu36muAaXpAo7PQ	
yuZn1P1q4SpwEjVdL1/4VgAdeaCBNHXBuA6Cm6oIps87MHzkNqs2p1Ig9/bFepQb	
92TD0FV1qBDHypG0HPvNfZDUKwc=	
END CERTIFICATE REQUEST	-



5. Now back out to the Main Menu and Select Create Certificate

192 🛃	2.168.1.15 - PuTTY		x
			*
	Welcome to the Black Vault CA		
	Create Certificate Request Date	: 2017-11-27	
	Create Certificate Time	: 15:53:02	
	CA Utilities SSH Port	: 22	
	Server Utilities Version	: 09.00.05	
	System Commands Firewall	: Off	
	Information		=
	Revoke Certificate		_
	Show Certificates and Status		
	Show CA Certificates		
	Logout		
Press	<pre>s <enter> to select an option</enter></pre>		
Arrow	<pre>keys to navigate (F2 to go back / Logout to Exit)</pre>		
			-



6. Select the Common Name of the CSR you wish to sign

19 🛃	22.168.1.15 - PuTTY		23
			^
	Choose a csr to sign		
	as		
	WWWW		
	yhhy		
	aaaaa		
	वेवेवेवे		
	testing		
	TIMMEH		
	EngageBlack		
	TimothyDyck		
	TimDyck		
	Timmehd		
Drag	A (ENTER) to coloct an option		
Arro	s veniers to select an option we keys to payigate (F2 to go back / Logout to Exit)		
ALLO	w keys to havigate (rz to go back / hogout to hkit)		-



7. Select None when asked for extension type

P 192.168.1.15 - PuTTY	
Choose an extension to add to certificate	
<pre>server_ext client_ext email_ext codesigning_ext None</pre>	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>	-



8. Back out to the main Menu and Select CA Utilities

P 192.168.1.15 - PuTTY	23	J
		•
CA Utilities		
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR		
	=	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>		-



9. Select Export Certificate

🗗 192.168.1.15 - PuTTY	
	•
CA Utilities	
Export Certificate Edit Extensions Add Extensions Remove Extensions Import CSR	
Press <enter> to select an option Arrow keys to navigate (F2 to go back / Logout to Exit)</enter>	-



10. Select the Certificate that you just created

₽	192.168.1.15 - PuTTY	_		
	Select a certificate t	o export.		
	(Valid/Revoked)	Serial	Subject Name	
	V	100C	CN=aaaaa	
	V	100D	CN=as	
	V	100E	CN=Tim Dyck	
	V	100F	CN=testing	
	V	1010	CN=Timmehd	
	V	1011	CN=testing	



11. Select PEM encoded (Without Key)

🔁 192.168.1.15 - PuTTY	
	<u>^</u>
Select format to export certificate.	
Personal Information Exchange - PKCS#12 (With Key) PEM with password - (With Key) DER encoded (Without Key) PEM encoded (Without Key) Cryptographic Message Syntax Standard - PKCS#7 (Without Key)	
	E
	~



12. Select To USB

و1 🛃	2.168.1.15 - PuTTY	The Owner water of the Owner		<u> </u>	J
				^	•
		Select where to export the (certificate.		
	to USB to SFTP				
				-	1



13. Insert a flash drive to the BlackVault CA and press enter

و1 🛃	2.168.1.15 - PuT	ΓY	-	-					- 0	x
										^
		Seled	ct where	to ex	port th	ne ce	rtific	cate.		
	to USB to SFTP									
		Please e	enter the	USB	device	and	press	<enter></enter>		
										-



Obtaining the CA certificates

1. On a client computer load the website : IP_Address_Of_BVCA/cacerts.pem

① 192.168.1.15/cacerts.pem

☆

2. Open the downloaded cacerts.pem in wordpad





3. Cut the first certificate and in a new document paste it. Save this one as Signing.crt



4. Save the remainder as root.crt



Importing the Certificates into Firebox

1. From the WatchGuard System Manager, open the system manager





2. In the Firebox System Manager, click the Certificates Button



3. In the Certificates window, click Import Certifcate/CRL Button

Status	Туре	Algo.	Subject Name	Details
Signed	IPSec / Web	RSA	c=US st=Kansas I=Smallville o=DEMO ou=DEMO	Delete
Signed	IPSec / Web	RSA	o=Engage Black cn=192.168.1.42	Delete
Signed	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web C	Refresh
Signed*	CA Cert	RSA	o=asdf ou=asdf cn=asdf	
Signed	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Export
Signed	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	
Signed	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Update
Signed	Proxy Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=h	
Signed	Provy Authority III	DCV	o-WatchGuard Technologies ou-Fireware co-Fi	
Shov	v trusted CAs for	proxies		
Shov	v trusted CAs for	proxies		

4. Click Import Certificate/CRL



5. In the Import Certificate/CRL window

Import Certificate / CRL
Import a Certificate Import a CRL
Certificate Type:
Base64(PEM) certificate 👻
Choose the function of the imported certificate:
Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
Proxy Server (server certificate for inbound SSL/TLS content inspection)
Trusted CA for Proxies
IPSEC, Web Server, Other
You may import a certificate from either the clipboard or a file. If you are importing a certificate and its private key, be sure to include both in the text area below.
Paste Load from File
bmdhZ2UgQmxhY2sxDTALBgNVBAsMBERlbW8xEDAOBgNVBAMMB1Jvb3QgQ0EwWTAT
BgcqhkjOPQIBBggqhkjOPQMBBwNCAASrthfN61l3MUmiwwH8BL/1S2bGf80jJjTm ANDLy8bYviNudK/6SBGG+fDapfLQXm2y0yTbNDTo3aMLATEQzBZbo2MwYTAQBaNV
HQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUd3XbNccQhETS
V4VZV3Wn3E+LkSIwHwYDVR0jBBgwFoAUd3XbNccQhETSv4VZV3Wn3E+LkSIwCgYI
AiEAmJuASnbZAZAYo1QG4wmZEdgSfRnu+fcjqB/nl36pBb8=
END CERTIFICATE
Help Import Certificate Cancel

- a. Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radios button
- b. Under Certificate File Click Choose file, then browse to where you saved Root.crt.
- c. Click Import Certificate
- d. An Import Certificate window will then appear, click Yes

Import Co	ertificate
?	Click Yes to import certificate now. Click No to cancel.
	Yes No



e. An Import Successful window next appears, click Yes



6. The Certificates windows will appear again, click Import Certifcate/CRL Button

Status	Туре	Algo.	Subject Name	Details
Signed	IPSec / Web	RSA	c=US st=Kansas I=Smallville o=DEMO ou=DEMO	Delete
Signed	IPSec / Web	RSA	o=Engage Black cn=192.168.1.42	
Signed	Web Client	RSA	o=WatchGuard ou=Fireware cn=Fireware web C	Refresh
Signed*	CA Cert	RSA	o=asdf ou=asdf cn=asdf	
Signed	Web Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Export
Signed	Web Client	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	
Signed	CA Cert	RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Update
Signed	Proxy Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=hi	
Signed (Provy Authority III	DCV	n-WatchGuard Technologies ou -Fireware cn-Fi	
Signed	Proxy Server	RSA	o=WatchGuard_Technologies ou=Fireware cn=ht -WatchGuard_Technologies ou=Fireware cn=Fi	

7. Click Import Certificate/CRL



8. In the Import Certificate/CRL window

Timport Certificate / CRL					
Import a Certificate Import a CRL					
Certificate Type:					
Base64(PEM) certificate 👻					
Choose the function of the imported certificate:					
Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)					
Proxy Server (server certificate for inbound SSL/TLS content inspection)					
Trusted CA for Proxies					
IPSEC, Web Server, Other					
You may import a certificate from either the clipboard or a file. If you are importing a certificate and its private key, be sure to include both in the text area below.					
Paste Load from File					
CAMING SUM 2 Vehilip H Leonawick 2020 min QADDOSINA HAT DGWDAOINDE VAL21 H 2000 bGFjazENMAsGA 1UECWWERGV tbzETMBEGA 1UEAwwKU2lnbmluZyBDQTBZMBMGByqG SM49AgEGCCqGSM49AwEHAOIABLYAlrhvKW/b4cniYTV6fkx9sDzrtaVdaxLuV7HT E3kRg6043uCt7dW9jkmrHrNqUPOXWbnJI/LB5mXZR2k7oWijZjBkMA4GA 1UdDwEB /wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMB0GA 1UdDpQWBBR 16MRydUrvV0w4 eGhu6K0pFic47zAfBgNVHSMEGDAWgBR3dds 1xxCERNK/hVlXdafcT4uRIjAKBggq hkjOPQQDAgNIADBFAiBjsgzZ 1XE4yLD7PJs6rZmiyDjC+m6L6BiK3SBaT9L0pQIh ALgGhkJ/dGpohL9psjWHSfeEDuU4LpaN4sCj729rgNKF END CERTIFICATE					
Help Import Certificate Cancel					

- a. Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radios button
- b. Under Certificate File Click Choose file, then browse to where you saved Signing.crt.
- c. Click Import Certificate
- d. A Import Certificate window will then appear, click Yes





e. An Import Successful window next appears, click Yes



9. The Certificates windows will appear again, click Import Certifcate/CRL Button

/Web RSA	c=US st=Kansas I=Smallville o=DEMO ou=DEMO	Delete
/Web RSA		Delete
1100 1000	o=Engage Black cn=192.168.1.42	
lient RSA	o=WatchGuard ou=Fireware cn=Fireware web C	Refresh
rt RSA	o=asdf ou=asdf cn=asdf	
erver RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Export
lient RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	
rt RSA	o=WatchGuard_Technologies ou=Fireware cn=Fi	Update
Server RSA	o=WatchGuard_Technologies ou=Fireware cn=h	
Authority DSA III	o-WatchGuard Technologies ou-Fireware co-Fi	
d CAs for proxies	c .	
	lient RSA erver RSA lient RSA it RSA Server RSA Authority DSA III	lient RSA o=WatchGuard ou=Fireware cn=Fireware web C t RSA o=asdf ou=asdf cn=asdf erver RSA o=WatchGuard_Technologies ou=Fireware cn=Fi lient RSA o=WatchGuard_Technologies ou=Fireware cn=Fi t RSA o=WatchGuard_Technologies ou=Fireware cn=Fi Server RSA o=WatchGuard_Technologies ou=Fireware cn=Fi Muthority_PSA o=WatchGuard_Technologies ou=Fireware cn=Fi III

10. Click Import Certificate/CRL



11. In the Import Certificate/CRL window

🔄 Import Certificate / CRL
Import a Certificate Import a CRL
Certificate Type:
Base64(PEM) certificate 👻
Choose the function of the imported certificate:
Proxy Authority (re-signing CA certificate for outbound SSL/TLS content inspection)
Proxy Server (server certificate for inbound SSL/TLS content inspection)
Trusted CA for Proxies
IPSEC, Web Server, Other
You may import a certificate from either the dipboard or a file. If you are importing a certificate and its private key, be sure to include both in the text area below.
Paste Load from File.
Kb3px6ZJ6H3saSiJnLERoydQvH0mgJeSgl9sbh9zxHzny8uR6cDWcsPC+5iQxfyC
jmfqU6W81irAVFkznrWiPLoODxQ9MGxGHc47azbkHrxoagIi0j4ukwIDAQABo2Qw
YJAJBGNVHKMEAJAAMICKGA LUGEQQIMCCCDDESMI4XNJGUMS4UM0EQYWKTAWSAZG9T YWluLmNvbTALBgNVHQ8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUF
CAICMAoGCCqGSM49BAMCA0gAMEUCIQCswQLVqp+n61CTCaGHrMw6PkogSFdhqYFP
Pqobg5W9jw1gGKVLmMvjrGrtNE1WqC/oCxz/y6HJ2NCvwjhKL/Czivg=
· · · · · · · · · · · · · · · · · · ·
Help Import Certificate Cancel

- f. Under Choose the function of the imported certificate, select the IPSEC, Web Server Other radios button
- g. Under Certificate File Click Choose file, then browse to where your flash drive and select the Certificate you exported from the BlackVault.
- h. Click Import Certificate
- i. A Import Certificate window will then appear, click Yes





j. An Import Successful window next appears, click Yes



Site B

Repeat Process stated in site a for site b.



Setting up VPN

Before setting up the VPN the following information should be collected

- Site A and B external IP addresses
- Site A and B internal network IP addresses
- Site A and B X.500 Distinguished Names from their certificates
 - This can also be known as the Subject name.

Site A

Configuring VPN

1. From the WatchGuard System Manager open the Policy Manager.





2. In the Policy Manager, click Branch Office Gateways



3. In the Gateways window, click add

K Gateways	×
gateway.1 (c=US st=Kansas I=Smallville o=Acme or	Add
	Edit
	Remove
	Enable
	Disable
	Report



4. In the New Gateway window select the radio button that says, "Use IPSec Firebox Certificate" then select the certificate that was just generated

	ential Method								
) U	Jse Pre-Share	d Key							
) u	Jse IPSec Fire	box Certific	cate	- O-t-					
ld	set the certifies	ate to be us	Certifica	te Name				Algorit	hm
200	01		c=US st=	Kansas I=Sma	Ilville o=DEMO ou	=DEMO cn=D	EMO	RSA	
290	102		c=US st= o=Engag	Illinois I=Smallv e Black cn=192	ille o=Acme ou= 2.168.1.42	esting cn=Jir	n Duck	RSA RSA	
	Show All Cert	tificates							
	Show All Cert	tificates							
atev	Show All Cert way Endpoints	tificates				Prests Oct			
atev	Show All Cert	tificates s Local G	≩ateway		IP Address	Remote Gat	eway		Add
atev	Show All Cert	tificates s Local G Type	3ateway	D	IP Address	Remote Gat	eway D		Add Edił
atev ŧ	Show All Cert	tificates s Local G Type	Sateway	D	IP Address	Remote Gat	eway D		Add Edit Delete
atev	Show All Cert way Endpoints	tificates s Local G Type	3ateway	D	IP Address	Remote Gat	eway D		Add Edit Delete
atev	Show All Cert way Endpoints	tificates s Local G	3ateway	D	IP Address	Remote Gat	eway D		Add Edit Delete Move up
atev #	Show All Cert way Endpoints	tificates s Local G	3ateway	D	IP Address	Remote Gat	eway D		Add Edit Delete Move up Move down



5. In the bottom half of the New Gateway window, under Gateway Endpoints click add

regential Method		ettings					
Use Pre-Shar	ed Key						
) Use IPSec Fir	ebox Certif	icate					
Select the certifi	cate to be u	ised for the Gatewa	y.				
ld .		Certificate Name	Carella a DEMO au	DENO 1	2510	Algorith	m
20001		c=US st=Illinois I=S	mallville o=Acme ou="	Festing cn=J	m Duck	RSA	
29000		o=Engage Black cr	=192.168.1.42			RSA	
ateway Endpoin	ts Local (Gateway		Remote Ga	teway		Add
# Interface	ts Local Type	Gateway	IP Address	Remote Ga	teway		Add
# Interface	Local Type	Gateway	IP Address	Remote Ga	teway ID		Add Edit
ateway Endpoir # Interface	Local (Type	Gateway	IP Address	Remote Ga	teway ID		Add Edit Delete
# Interface	ts Local (Type	Gateway	IP Address	Remote Ga	teway D		Add Edit Delete
# Interface	ts Local (Type	Gateway	IP Address	Remote Ga	teway D		Add Edit Delete Move up
ateway Endpoir # Interface	ts Local (Type	Gateway	IP Address	Remote Ga	teway D		Add Edit Delete Move up Move down



6. In the New Gateway Endpoints Settings Windows, do the following:

Loca	al Gateway	
Exte	rnal Interface:	External 🗸 🗸
Spe	cify the gatewa	ay ID for tunnel authentication.
	By IP Address	3
	IP Address	~
۲	By Domain Inf	ormation Configure
Rem	X.500 Name = note Gateway cify the remote	: c=US st=llinois I=Smallville o=Acme ou=Testing cn=Jim Duo gateway IP address for a tunnel.
Rem Spec	X.500 Name = note Gateway cify the remote 0 Static IP addres IP Address	c c=US st=llinois I=Smallville o=Acme ou=Testing cn=Jim Duo gateway IP address for a tunnel. ess
Rem Species Species	X.500 Name = inte Gateway - cify the remote Static IP addres IP Address Dynamic IP ad cify the remote	c = US st=llinois I=Smallville o=Acme ou=Testing cn=Jim Duo gateway IP address for a tunnel. ess
Rem Spei © Spei	X.500 Name = inte Gateway cify the remote Static IP address IP Address Dynamic IP ad cify the remote By IP Address	c c=US st=llinois I=Smallville o=Acme ou=Testing cn=Jim Duo gateway IP address for a tunnel. ess
Rem Species Species	X.500 Name = Note Gateway Cify the remote 1 Static IP address 1 Dynamic IP ad Cify the remote 1 By IP Address IP Address	c c=US st=llinois I=Smallville o=Acme ou=Testing cn=Jim Duo gateway IP address for a tunnel. ess ▼ Idress gateway ID for tunnel authentication. s

- a. In the Local Gateway subsection, Select the By Domain Information radio button, then click Configure
 - i. In the Configure Domain for Gateway ID window Select the X500 Name radio button the click OK
ENGAGE BLACK Engage BlackVault CA WatchGuard Integration Guide

I	Configure Domain for Gateway ID	×
	Select the method of domain configuration for tunnel gateway authentication O Domain Name User ID @ Domain X500 Name	
	X500 Name	
	OK Cancel H	elp

- b. In the Remote Gateway subsection, Select the Static IP Address radio button, then enter the IP Address of the remote gateway.
- c. Under Specify the remote gateway ID for tunnel authentication select the By Domain Information the click Configure
 - i. In the Configure Domain for Gateway ID select the X500 Name radio button then add in the X500 name of the certificate of the Site B then press OK

ENGAGE BLACK Engage BlackVault CA WatchGuard Integration Guide

1	Configure Domain for Gateway ID	×
	Select the method of domain configuration for tunnel gateway authentication	
	O Domain Name	
	🔘 User ID @ Domain	
	X500 Name	
	OK Cancel H	elp

d. In the New Gateway Endpoint Settings window click OK



Engage BlackVault CA WatchGuard Integration Guide

7. In the New Gateway window click OK

eneral Settings Phase 1 Settings								
Use Pre-Shared Key								
) Use I	IPSec Fireb	oox Certifica	ite					
elect th	ne certifica	te to be use	ed for the Gateway	у.				
ld		0	Certificate Name				Algorith	ım
0001		C	=US st=Kansas I=	Smallville o=DEMO o	u=DEMO cn=D	EMO	RSA	
90002		C	=05 st=minols i=5r =Engage Black on	=192.168.1.42	resung ch=Jir	DUCK	RSA	
Sho	w All Certi	ficates						
Sho	vw All Certi r Endpoints	ficates Local Ga	teway		Remote Gat	eway]	Add
Sho steway	w All Certi <u>Endpoints</u> erface	ficates Local Ga	teway	IP Address	Remote Gat	eway		Add
Sho ateway	erface	ficates Local Ga	teway D	IP Address	Remote Gat	eway		Add Edit Delete
Sho ateway	w All Certi r Endpoints erface	ficates Local Ga	teway D	IP Address	Remote Gat	eway ID		Add Edit Delete
Sho	w All Certi	ificates Local Ga	teway D	IP Address	Remote Gat	eway D		Add Edit Delete Move up
Sho iteway	w All Certi	ificates Local Ga Type	teway D	IP Address	Remote Gat	eway D		Add Edit Delete Move up Move down
Sho ateway	w All Certi	ificates	teway D	IP Address	Remote Gat	eway D		Add Edit Delete Move up Move down



8. In the Gateways window click Close

🔣 Gateways						
gateway.1 (c=US st=Kansas I=Smallville o=Acme ou	Add					
	Edit					
	Demove					
	Enable					
	Disable					
	Disable					
	Report					
4 III >						
Close	Help					



Engage BlackVault CA WatchGuard Integration Guide

9. In the Policy Manager, click Branch Office Tunnels

C:\l	Jsers\Timothy\[ocuments\My Wa	tchGuard\configs	WatchGuard-XTM	xml- Fireware XT	M Policy Manager			x
File Ed	File Edit View Setup Network FireCluster VPN Subscription Services Help								
1 🚊 .	🚊 🖻 🖷 🔍 + X 🗄 🖉 🐘 🗈 🍓 🔏 🗐 🖉 🔗 💷 🧠 ?								
Firewa	Firewall Mobile VPN with IPSec								
						r		1.	
						Filter: None		▼.	P 7.
Order	Action	Policy Name	Policy Type	From	То	Port	PBR	App Control	Tags
1	\checkmark	🖾 FTP	FTP	Any-Trusted, Any-O	pAny-External	tcp:21	N	one	
2	\checkmark	🗢 WatchGua	WG-Fireware-X	Any-Trusted, Any-O	pFirebox	tcp:8080	N	one	
3	~	(A) Ping	Ping	Any-Trusted, Any-O	pAny	ICMP (type: 8,	N	one	
4	\checkmark	🗢 WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-O	pFirebox	tcp:4105 tcp:4	N	one	
5	<i>.</i>	Outgoing	TCP-UDP	Any-Trusted, Any-O	pAny-External	tcp:0 (Any) u	N	one	
6	<i>.</i>	BOVPN-AII	Any	Any	tunnel.1	Any	N	one	
7	~	BOVPN-All	Any	tunnel.1	Any	Any	N	one	
•									- F
						Basic Mar	naned Devic	e l Fireware VI	M v12 0 0
	Basic Managed Device Fireware XTM v12.0.0								



10. In the Branch Office IPSec Tunnels window click Add

R Branch Office IPSec Tunnels	×
tunnel.1(gateway.1)	Add
	Clone
	Edit
	Remove
	Move Up
	Move Down
	Report
C	ose Help



Engage BlackVault CA WatchGuard Integration Guide

11. In the New Tunnel window do the following:

💦 New Tunnel				×		
Tunnel Name: Gateway: Addresses Addresses	tunnel.2 gateway.1 hase 2 Setting	s Multicast Se	▼)		
Local	Dir	Remote	Edit. Remo	 ve		
Helper Addre	esses					
Remote IP:						
Add this t	Add this tunnel to the BOVPN-Allow policies					
	(ок	Cancel	Help		



a. In the Address Tab click the Add button

I Tunnel I	Route Settings				
Local:	· · · · · · · · · · · · · · · · · · ·				
Remote:	✓ …				
(i) or ex is	you want to enter a network address in the Local Remote text box, you must include a netmask, ample: 10.0.0.0/8. An IP address without a netmask seen as host address.				
Direction:	Local <===> 🕶 Remote				
NAT Sett	tings				
. 1:1	NAT				
	AT				
Enable broadcast routing over the tunnel					
	OK Cancel Help				

- i. In the tunnel Route Settings window click the ellipse next to Local
 1. In the Add Address window
 - a. Under "Choose Type" select Network IPv4
 - b. Under "Value" add in the local network
 - c. Press Ok

K Add Address		-	-	-	
Choose Type:	Netwo	ork IPv4			•
Value:			•	1	
					OK Cancel



- ii. In the tunnel Route Settings window click the ellipse next to Remote
 - 1. In the Add Address window
 - a. Under "Choose Type" select Network IPv4
 - b. Under "Value" add in the remote network
 - c. Press Ok

K Add Address	
Choose Type:	Network IPv4
Value:	/
	OK Cancel

- b. In the New Tunnel Window, leave everything else in the other tabs then click OK
- c. In the Branch Office IPSec Tunnels window click Close

R Branch Office IPSec Tunnels						
tunnel.1(gateway.1)	Add					
	Clone					
	Edit					
	Remove					
	Move Up Move Down					
	Report					
	Halp					
	neip					



Site **B**

Repeat Process stated in Site A for Site B