Best Practices for Securing a Dell EqualLogic SAN

A Dell EqualLogic best practices paper

Dell Storage Engineering
April 2014

Revisions

Date	Description
April 2014	Initial release

Table of contents

Acknowledgements

This best practice white paper was produced by the following members of the Dell Storage team:

Engineering: Clay Cooper

Editing: Camille Daily

Additional contributors: Michael Kosacek, Richard Golasky and Danilo Feroce

Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this information by sending an email to SISfeedback@Dell.com.

SISfeedback@Dell.com

Executive summary

This paper explores the technologies available for building a secure Dell EqualLogic PS Series SAN with operational environment best practices, self-encrypting drives, and IPsec network layer security.

1 Introduction

Dell EqualLogic PS Series arrays provide a storage solution that delivers the benefits of consolidated networked storage in a self-managing iSCSI (Internet Small Computer System Interface) SAN (storage area network) that is affordable and easy to use, regardless of scale.

Data security is a primary concern in almost any IT environment. Business critical or confidential information must be protected from unauthorized access and properly disposed of when required. Many organizations are compelled to implement data protection technologies due to regulatory compliance.

This technical paper serves as a guide to deploying a secure EqualLogic SAN to prevent unauthorized access to the PS Series administrative interfaces and to protect data at rest using self-encrypting drives and data in flight using IPsec network layer security. IPsec is a set of standardized protocols designed to allow systems on IP-based networks to verify identities and create secured communication links.

It will also examine the performance impact of IPsec on four common SAN workloads.

Note: The performance data in this paper is presented relative to baseline configurations and is not intended to express maximum performance or benchmark results. Actual I/O workload, host to array port ratios, and other factors may also affect performance.

1.1 Audience

This technical white paper is for storage administrators, SAN system designers, storage consultants, network and security consultants, or anyone tasked with building a secure, production SAN using EqualLogic PS Series storage. It is assumed that all readers have experience in designing and/or administering a shared storage solution. Also, there are some assumptions made in terms of familiarity with all current Ethernet standards as defined by the IEEE (Institute of Electrical and Electronic Engineers) as well as TCP/IP (Transmission Control Protocol/Internet Protocol) and iSCSI standards as defined by the IETF (Internet Engineering Task Force).

2 Basic EqualLogic SAN security

Traffic on an EqualLogic PS Series SAN takes place over a switched Ethernet network. It consists mainly of iSCSI protocol communication among the PS Series array members and the iSCSI initiators of the storage hosts. The SAN traffic may also include management and monitoring traffic required to administer the SAN.

A PS Series group offers a variety of mechanisms for preventing unauthorized access to administrative access points or to iSCSI targets.

In addition, self-encrypting drives are available to provide security for data at rest and IPsec can be configured to secure data in flight.

2.1 Common Criteria certified

PS Series storage controller firmware has been certified to conform to the Common Criteria for IT Security Evaluation (CC), version 3.1 by the Federal Office for Information Security most recently in March 2013.

http://www.commoncriteriaportal.org/files/epfiles/0688a_pdf.pdf

The primary security features certified by Common Criteria are:

- **Event auditing:** For each event, the user identity, role, date and time are recorded. This includes administrative and iSCSI logins and logouts.
- **User identity and authentication:** Ensures that a user provides credentials to access administrative functions or iSCSI targets. User credentials can be stored locally in the firmware, on a RADIUS (Remote Authentication Dial-In User Service) server, or in Active Directory. PS Series firmware 7.0 now supports single sign on for administrative accounts using Active Directory. For iSCSI clients, credentials can be stored locally or on a RADIUS server.
- **Access control methods:** Control access to iSCSI targets by requiring CHAP (Challenge-Handshake Authentication Protocol) or by restricting access based on IP address or IQN (iSCSI qualified name).
- **Residual information protection:** Zeroes out each page of disk space at allocation time.
- **Security role management:** Allows users to have different levels of authorization. There are roles for administering the group, only certain pools, or only certain volumes. There is also a read-only administrator role that can view all information but cannot make changes. For auditing purposes, there is also an iSCSI client user role to track iSCSI logins and logouts.
- **Reliable time stamps:** Use an internal time source or an NTP (Network Time Protocol) server
- **Trusted channel:** Communication for administrative access over the Ethernet port. SSH (Secure Shell) is available for secure remote access to the CLI (Command Line Interface). Access to the web GUI (Graphical User Interface) is secured using TLS (Transport Layer Security).

2.2 Operational environment

Physical security is always the most basic form of protection for any business critical infrastructure. The PS Series SAN is designed to operate in a physically secure environment that is accessible only to system administrators.

Secondary services such as DNS (Domain Name System) and NTP should be from trustworthy sources.

The iSCSI network and the administrative network should be physically secure and logically protected using firewalling or network isolation. The iSCSI network should be physically separate from the end user application network unless Data Center Bridging (DCB) is used to converge the two networks.

Password complexity should be consistent with the authentication policy of the organization. The administrator must change the default password during initialization of the PS Series storage group. If the password is lost, the administrative password can be reset through the serial console, but only with real time assistance from Dell EqualLogic support.

Firmware, security and anti-virus updates should be applied regularly to all systems having access to the SAN. In particular, web browsers and SSH clients used for remote administrative access should be kept up to date.

CVE-2014-0160, also known as the "Heartbleed bug" is a serious vulnerability in the popular OpenSSL cryptographic software library. For more information on this vulnerability, see http://heartbleed.com. For a status of Dell products, workarounds and updates, see Dell's Heartbleed bug remediation page at http://www.dell.com/learn/us/en/04/campaigns/heartbleed-remediation

2.3 Administrative access points

Each PS Series array member can be accessed administratively using either the serial port or the Ethernet port. The CLI is available through the serial port using a terminal emulator or through the Ethernet port using SSH or Telnet. Both SSH and Telnet access are enabled by default, however disabling Telnet is recommended. Telnet transmits data in clear text and its use increases the risk exposure for that connection.

The Group Manager GUI is available through the administrative Ethernet port using a standard web browser. Initially a java application will be downloaded using the web browser over TCP port 80 or port 443. Once downloaded, the java application will securely connect to the PS Series group using the administrative credentials set during group initialization. The traffic will be encrypted using TLS.

The PS Series group also supports SCP (Secure Copy) for copying firmware updates and diagnostic files to and from the array. It is a secure alternative to FTP (File Transfer Protocol). As with Telnet, FTP transmits authentication information in clear text and it is not recommended.

The SAN Headquarters application can monitor the array members using SNMP (Simple Network Management Protocol). Additionally, a PS Series group can be configured to send email alerts to an SMTP (Simple Mail Transfer Protocol) server or to send system events to a syslog server.

2.4 Security access protocols

The PS Series group supports security protocols SSL/TLS and SSH, with a range of encryption algorithms. The protocols and algorithms enabled by default include some older protocols (such as SSH v1 and SSL v2) and encryption algorithms that are no longer recommended as best practices.

Unless it is necessary to enable access from older clients (web browsers or SSH clients) that do not support the current encryption protocols and authentication algorithms, Dell recommends disabling legacy protocols and algorithms for the best security.

You must use the CLI to disable the legacy protocols; see the *grpparams crypto-legacy-protocols* command in the *Dell EqualLogic Group Manager CLI Reference Guide*. You can also enable or disable SSH v1 protocol support; see the *grpparams cliaccess-ssh* command.

3 Protecting data at rest with self-encrypting drives

Data at rest is the data that resides on the physical hard drives within the array member chassis. In the case of a breach of physical security and the removal of a hard drive from an array member chassis, data could be extracted directly from a conventional hard drive.

Self-encrypting drives (SED) guard against this threat by encrypting data as it is written to the disk and decrypting data as it is read. EqualLogic PS Series arrays implement this technology in a manner that is fully transparent to the storage administrator and to the consumer of the data. Also, since the encryption is offloaded to the SED, performance impact should be negligible. Hard drives which are removed from the array member chassis will contain only encrypted data, impossible to access without the unique encryption key generated by the PS Series controller firmware during group initialization.

Another benefit of the EqualLogic implementation of SED technology is the Instant Secure Erase (ISE) feature. When hard drives or array members are re-commissioned, the controller firmware will reset the encryption key used to encrypt the data as it is written. Once the encryption key for a hard drive set changes, any data already on the drive is instantly and permanently inaccessible, obviating the need for time consuming hard drive data wiping.

For more on the EqualLogic implementation of SED technology, see *EqualLogic PS Series Architecture: Self Encrypting Drive Management with PS Series Storage Arrays* at http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/20382259.aspx

4 Protecting data in flight with IPsec

Data in flight is data as it is transmitted over the wire using the IP protocol. IP packets contain unencrypted data payloads that can be easily read if the packet is captured in transit. One method of securing data in flight is to encrypt IP packet payloads using IPsec network layer security.

IPsec is a set of standardized protocols designed to allow systems on IP-based networks to verify identities and create secured communication links. IPsec uses cryptographic security mechanisms for authentication and protection. IPsec validates the identity of devices communicating over IP-based networks, encrypts all data passing between participating systems, and protects against disclosure, modification, eavesdropping and attack. IPsec is supported for both IPv4 and IPv6 networks.

Note: For more information about IPsec, refer to the website of the Internet Engineering Task Force, the organization that originally developed the IPsec protocols.
http://ietf.org

In the context of an iSCSI SAN that uses EqualLogic PS Series storage arrays, IPsec secures communications between group member arrays and between iSCSI initiators and the group. You can use policies to configure your IPsec implementation to protect iSCSI traffic based on initiator IP address, initiators in a specific subnet, or network protocol. IPsec authentication is handled using certificates or pre-shared keys.

Note: IPsec is supported only for PS Series array models (PS6xxx, PS41x0, and PS-M4110), and can be enabled for a group only if all members support IPsec.

4.1 Types of protected traffic

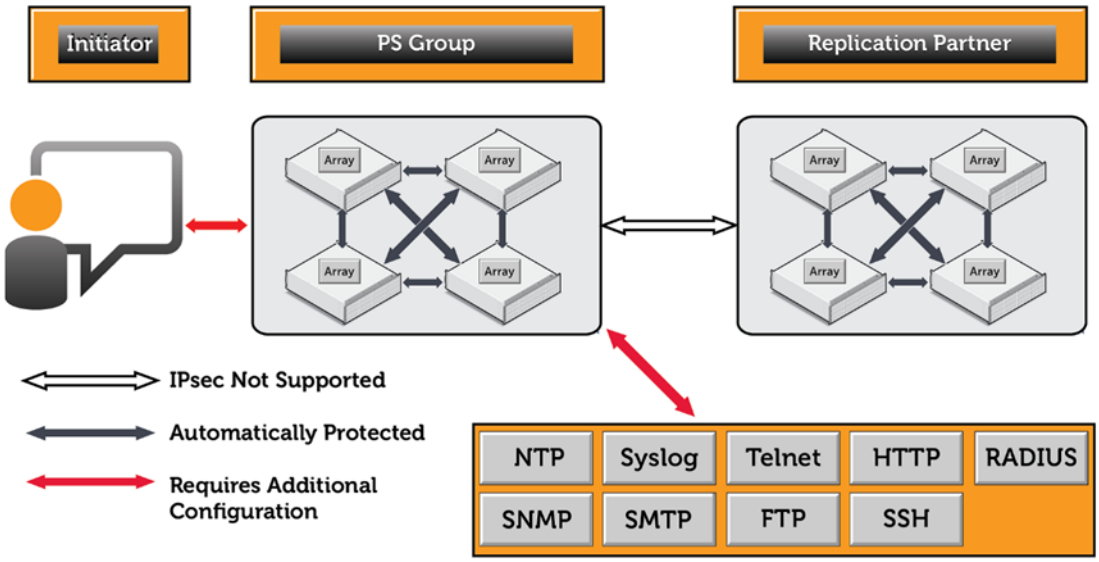

Figure 1 What IPsec Protects

After IPsec is enabled, all network traffic between group members is automatically protected with IPsec using IKEv2. No further configuration is required.

All incoming or outgoing IP traffic that travels between hosts and the group can be protected with IPsec. This traffic includes, but is not necessarily limited to:

- iSCSI traffic
- Telnet and SSH connections to the Group Manager CLI
- HTTP connections to the Group Manager GUI
- SMTP email notifications
- Syslog
- NTP
- RADIUS
- SNMP

Note: If IPsec is enabled but no security parameters or policies are in place, intragroup traffic is protected, and traffic to and from the group is allowed to pass without being protected or dropped.

4.2 Securing replication traffic

The PS Series firmware provides no mechanism for using IPsec to protect replication traffic to an offsite storage group. If securing WAN replication traffic is a requirement, it is recommended to secure the traffic with a virtual private network (VPN) using a WAN optimizer or router.

4.3 IPsec policies

Traffic that meets the conditions stipulated by the policy can either be passed, dropped, or protected using an IPsec security parameter associated with the policy.

You can use IPsec policies to apply IPsec protection to traffic that meets one or more of the following criteria:

- Data traveling to or from specific IP addresses, or a range of IP addresses defined by a specific subnet or netmask.
- IPv4 or IPv6 traffic
- Specific network protocols: TCP, UDP, or ICMP (either IPv4 or IPv6)

Unless explicitly specified by the policy, traffic is allowed to pass. To drop all traffic that is not explicitly protected or passed, create an IPsec policy that drops traffic by default.

If multiple IPsec policies are in place, the system determines their priority by the order in which they were created. Policies created first take precedence over policies created later.

IPsec policies can also be used to determine what traffic is being protected using IPsec, and what traffic is being passed or dropped without encryption.

4.4 IPsec certificates

Certificates are used in an IPsec configuration as one method of authenticating secured connections between iSCSI initiators and the group. Implementation of an IPsec-enabled SAN requires both a root-CA (Certificate Authority) certificate from the issuing authority and a local certificate to authenticate the group.

You can generate certificates suitable for use in IPsec connections to the PS Series using any Windows, OpenSSL, or other commercial Certificate Authority product.

From the Group Manager CLI, you can import, display, and delete certificates, using the IPsec certificate commands. See the *Dell EqualLogic Group Manager CLI Reference Guide* for more information.

4.5 IPsec security parameters

IPsec security parameters control the authentication and key negotiation carried out using the Internet Key Exchange IKEv1 or IKEv2 protocol.

Security parameters specify the following features:

- Using IKEv1, IKEv2, or manual keying

Note: You can configure IPsec to use manual keys. However, manual keying provides significantly weaker security than IKEv1 or IKEv2, and is also significantly more difficult to configure. Consequently, Dell strongly discourages the use of manual keying in any production environment. IKEv1 or IKEv2 are the preferred keying methods.

- Using certificates and pre-shared keys (PSK)
- Establishing Transport Mode or Tunnel Mode connections

Note: Unless specifically configured, IKEv1 and Transport Mode are used by default.

IPsec security parameters are managed using the ipsec security-params commands. See the *Dell EqualLogic Group Manager CLI Reference Guide* for more information.

4.6 IPsec security associations

The pairing of an IPsec security parameter with an IPsec policy forms an IPsec security association (SA), which formalizes the secured connection between the group and a host connected to it. Each protected connection to the group is a unique security association, and each system can have multiple security associations, allowing it to have authenticated communications with many other systems.

Note: You can view or delete security associations using the IPsec security-association commands. See the *Dell EqualLogic Group Manager CLI Reference Guide* for more information.

4.7 IPsec pre-shared keys

In addition to using certificates, you can use pre-shared keys to authenticate secured connections. Pre-shared keys are identical strings that are specified at both ends of the communications pathway. The keys enable the systems to correctly identify each other.

Either ASCII or hexadecimal strings can be used. ASCII can be used in most situations. However, you can also use hexadecimal strings if your organization mandates their use, if you have systems that do not support the use of ASCII strings, or if you want to use unsupported characters.

4.8 IPsec configuration limitations

The limitations listed in the sections below apply when implementing IPsec.

- IPsec is only supported for certain PS Series array models, and can only be enabled for a group if all members support IPsec. See the Dell EqualLogic PS Series Storage Arrays Release Notes for more information.
- IPsec can only be enabled and configured using the Group Manager CLI. The Group Manager GUI provides no facility for configuring or monitoring IPsec.
- The PS Series array does not serve as an IPsec-secured gateway; it only behaves as an IPsec-secured host.
- You cannot use the save-config CLI command to preserve the group's IPsec certificates and pre-shared keys. The save-config command saves the CLI commands that were used to configure IPsec, but it does not save certificates that have been transferred to the array using FTP. Therefore, when you restore a configuration, you must manually restore any configuration options set using the IPsec certificate load, IPsec security-params create certificate, and IPsec security-params pre-shared-key commands.
- Kerberos-based authentication is not supported.
- Multiple Root Certificate Authorities (CA) are not supported.
- Certificate Revocation Lists (CRL) are not supported.
- Only users with group administrator privileges can configure IPsec.
- Perfect Forward Secrecy (PFS) is not supported.
- Encrypted private keys are not supported for X.509 format certificates.
- Dell recommends using a minimum of 3600 seconds and 10GB lifetime-rekey values.
- IKE mobility is not supported
- NAT Traversal (NAT-T) is not supported. Dell recommends against placing a firewall that performs address translation between the PS Series group and its IPsec peers.
- If you use the Windows default IPsec lifetime rekey values, the high rekey rates may be disruptive for protected iSCSI traffic. Values in the range of 1GB to 100GB, depending on iSCSI traffic, are recommended instead.

4.9 Host connectivity considerations

Enabling or disabling IPsec for the group using the IPsec enable and IPsec disable commands might disrupt host connectivity to the group for several minutes. To prevent unplanned outages, IPsec should be enabled or disabled during a planned maintenance window when there are no active iSCSI volume connections.

Consult the documentation for your host operating systems, HBAs, and iSCSI initiators to verify that they support IPsec. There might also be known issues and idiosyncrasies with the initiator IPsec support that require additional planning or configuration.

When configuring IPsec with Windows hosts, note the following:

- IPsec traffic is not always handled correctly if the IPsec policy is configured to protect only a subset of traffic between the host and the group. For example, if the IPsec policy protects only iSCSI traffic on port 3260, a Windows Server 2008 R2 host may not perform reliably when connecting to the group. As a workaround, IPsec policies should apply to all traffic passing between the group and Windows systems. Microsoft KB article 2665206 discusses this in detail at http://support.microsoft.com/kb/2665206
- IPsec must be configured using the Windows Firewall with Advanced Security. Do not use the IPsec option in the Microsoft iSCSI initiator, which does not have the capability to fully configure an IPsec configuration between the host and the group. Further, if you attempt to configure an IPsec connection using the iSCSI initiator, the system might not allow you to remove the partial configuration and replace it with a complete configuration created with Windows Firewall.
- IPsec policies defined using the Local Security Policy Manager are not supported.

4.10 Configuring IPsec

See Appendix A for how to enable IPsec communication between a single storage host running Windows Server 2012 and an EqualLogic PS Series storage group.

For more information on the EqualLogic implementation of IPsec and for other examples of configuring IPsec with different operating systems, different authentication methods and different connection modes see the *EqualLogic Group Manager Administrator's Manual*.

To find exact command line usage for configuring IPsec at the EqualLogic Group Manager CLI see the *EqualLogic Group Manager CLI Reference Guide*.

Both of the above documents can be found at the Dell EqualLogic support site (login required):

http://support.equallogic.com

5 IPsec performance impact

The performance impact of IPsec varies by host and network configuration, and increases with the number of IPsec-protected iSCSI connections to the group. Even if IPsec is only used to protect traffic between group members, I/O performance is still affected. Based on these factors, you can expect that using IPsec may degrade I/O performance.

Although PS Series array members use hardware to accelerate cryptographic operations, many initiators perform these operations in software using host CPU resources which can cause a further reduction in the speed of communications between iSCSI initiators and the group.

The following performance testing was intended to quantify the performance impact to four common SAN workloads.

5.1 Test configurations and methodology

The following section addresses the reasoning behind the test environment design and details the SAN configurations. Performance testing methodology, test case sequence, and results analysis are also explained.

5.1.1 Simplified SAN

Every effort was made to simplify and optimize the test configurations to provide a baseline for observing performance effects. The following SAN design and configuration elements helped to achieve this goal.

SAN design:

- An isolated SAN with iSCSI traffic only
- DCB disabled

At the host:

- Single Function NIC (no NIC partitioning)
- No IPsec offload features
- NDIS mode
- Jumbo frames enabled
- Flow control enabled
- NIC receive and transmit buffers maximized
- Host Integration Tools for Microsoft installed with default MPIO settings
- For each SAN adapter, IPv4 protocol enabled, all other protocols and services disabled

At the array member:

- Eight 100 GB volumes within a single storage pool, evenly distributed across two array members
- Load balancing (volume page movement within pools) disabled on the array members

Array member load balancing is recommended for production environments because it can improve SAN performance over time by optimizing volume data location based on I/O patterns. It was disabled for performance testing to maintain consistent test results. It is enabled by default.

The SAN design is described in the following section. See Appendix A for the hardware and software infrastructure details.

5.1.2 SAN design

The SAN has a redundant fabric with an equal number of host and storage ports. Equivalent host and storage bandwidth helps to ensure optimal I/O rates. Figure 2 shows only the active ports of the PS Series array members.

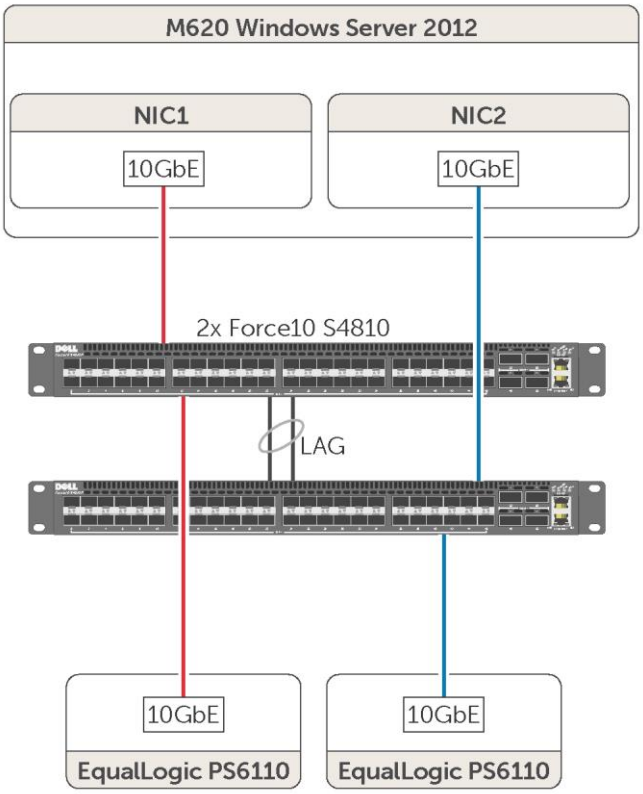

Figure 2 Diagram of the SAN design

- Two 10 GbE switches
- Two PS Series array members, each with a single port
- A single host with two 10 GbE NIC ports
- A 1:1 storage/host port ratio

5.1.3 I/O execution and evaluation

Prior to each test run, the even distribution of iSCSI connections across host and storage ports and of active array member ports across SAN switches was confirmed.

The following four vdbench workloads were run:

- 8 KB transfer size, random I/O, 67% read, 33% write
- 64 KB transfer size, random I/O, 67% read, 33% write
- 256 KB transfer size, sequential I/O, 100% read
- 256 KB transfer size, sequential I/O, 100% write

For every test case, each vdbench workload was run two times for 20-minute durations and the results were averaged.

Vdbench IOPS results were used to evaluate 8 KB and 64 KB random workload performance. Vdbench throughput results were used to evaluate 256 KB sequential workload performance. Host CPU utilization was also examined.

See Appendix C for a list of vdbench parameters used during testing.

5.1.4 Test case sequence

To evaluate the performance impact of using IPsec to secure iSCSI traffic, each of the four vdbench workloads listed above were run with and without IPsec enabled. The results are explained in Section 5.2.

5.2 Performance results

All test case performance results for each workload are presented in this section. Figure 3 charts the performance of each workload with and without IPsec enabled.

For the 8 KB and 64 KB random read/write workloads, IOPS were used to quantify performance. For the 256 KB sequential read and write workloads, throughput was used.

Results are expressed in percentage terms where having IPsec disabled is the baseline (100%).

As seen in Figure 3, performance decreases for every workload, particularly with larger block sizes and with sequential I/O.

The performance results illustrated below may not reflect all EqualLogic PS Series SAN environments. It is recommended that each potential configuration change be evaluated in the environment prior to implementation.

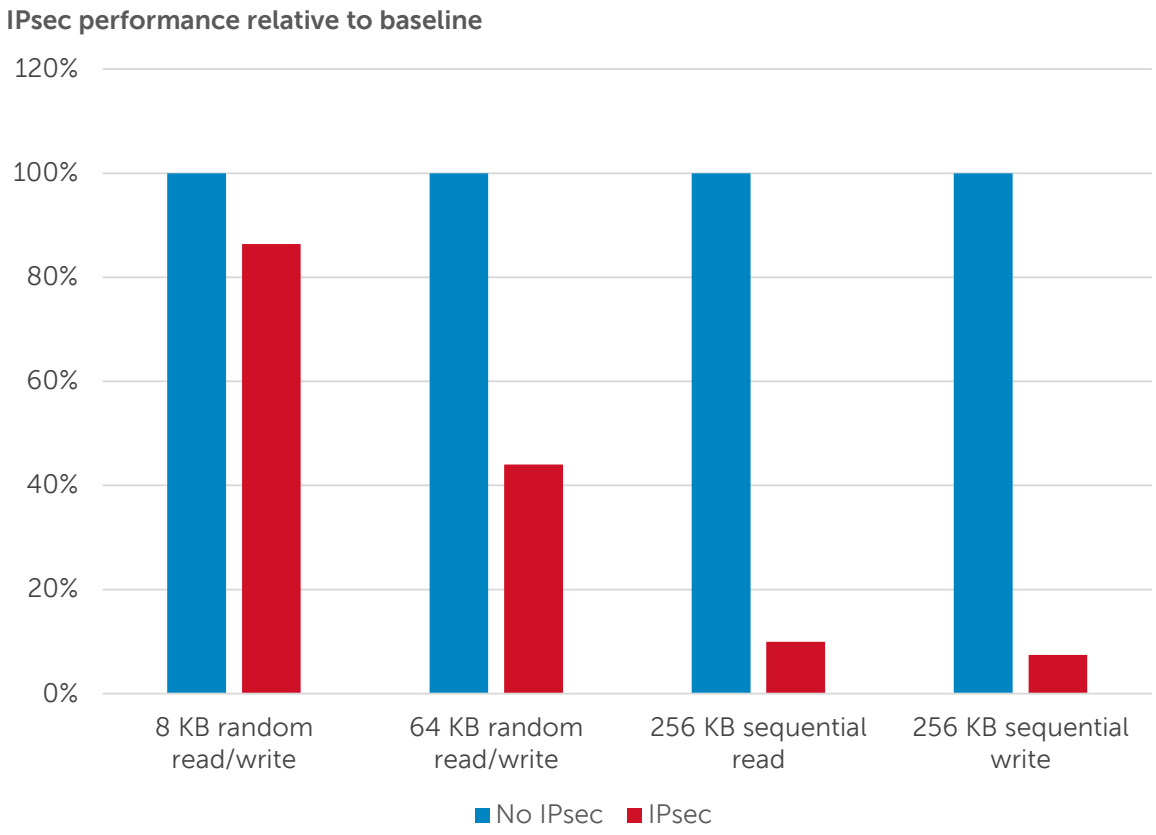

Figure 3 Performance with and without IPsec for each SAN workload

Figure 4 charts the CPU utilization of the storage host during each workload with and without IPsec enabled.

In general, enabling IPsec causes host CPU utilization to increase while performance decreases. During the random read/write workloads, this effect increased with a larger block size.

A different effect can be observed with the 256 KB sequential read workload. During sequential reads, the array members are responsible for virtually all packet encryption and transmission; I/O latency increases with IPsec enabled. The result is an increase in the host I/O wait time. This means that the host CPU spends a greater percentage of its total cycles waiting for I/O operations to complete, causing host CPU utilization to decrease with IPsec enabled.

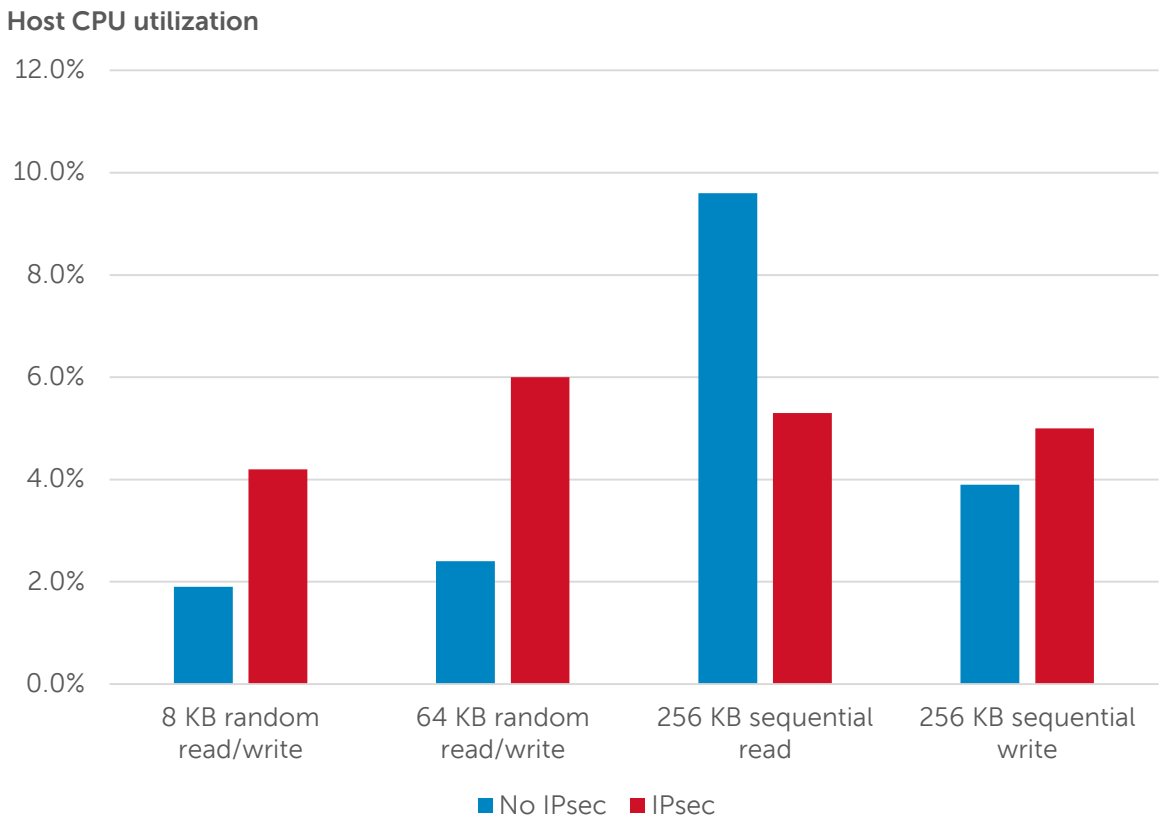

Figure 4 CPU utilization at the storage host with and without IPsec for each SAN workload

6 Security scanning

No security analysis would be complete without a review of open IP network protocol ports for a given system. Nmap, the open source network discovery and security auditing tool, was used for this purpose. The tables below list all TCP and UDP ports and services for a PS Series storage group. Not all services are enabled by default. Others, such as Telnet, can be disabled. For each port, the service description as reported by Nmap is listed as well as the actual port usage by a PS Series storage group.

In order for the PS Series storage and its associated services to function as expected, these ports must remain open through any firewalls or switch access control lists that reside in between the array members and the iSCSI initiators, the management servers or secondary services such as NTP.

6.1 Administrative interface port list

Table 1 and Table 2 list the ports and services available through the management network IP address. If the management interface is not enabled, then these ports and services will be available through the group IP address on the SAN.

Table 1 TCP ports and services available through the administrative interface

TCP Port	Nmap	EqualLogic PS Series storage group
21	ftp	FTP
22	ssh	SSH
23	telnet	Telnet
25*	smtp	SMTP
80	http	Web GUI (Java app download only)
443	http	Web GUI (Java app download only)
2606	netmon	Support Assist client for SANHQ
3002	exlm-agent	GUI communication
3003	cgms	GUI communication (encrypted)
20002	commtact-http	Group event logging
20003	commtact-https	Group event logging

* Not enabled by default

Table 2 UDP ports and services available through the administrative interface

UDP Port	Nmap	EqualLogic PS Series storage group
123	ntp	NTP
161	snmp	SNMP
500*	isakmp	IPsec key exchange
514*	syslog	Syslog

* Not enabled by default

6.2 Group interface port list

Table 3 and Table 4 list the ports and services available through group IP address on the SAN even when the management interface is enabled. When the management interface is not enabled, the ports and services in Table 1 and Table 2 are available through the group interface.

Table 3 TCP ports and service available through the group interface

TCP Port	Nmap	EqualLogic PS Series storage group
3260	iscsi	iSCSI
9876	sd	iSCSI intra-system control
20002	commtact-http	Group event logging
20003	commtact-https	Group event logging
25555	unknown	Group communications

Table 4 UDP ports and services available through the group interface

UDP Port	Nmap	EqualLogic PS Series storage group
123	ntp	NTP
500*	isakmp	IPsec key exchange

* Not enabled by default

6.3 Array member interface port list

Table 5 and Table 6 list the ports and services available through array member IP address on the SAN.

Table 5 TCP ports and services available through the array member interface

TCP Port	Nmap	EqualLogic PS Series storage group
3260	iscsi	iSCSI
9876	tcpwrapped	iSCSI intra-system control
20002	commtact-http	Group event logging
20003	commtact-https	Group event logging
25555	unknown	Group communications

Table 6 UDP ports and services available through the array member interface

UDP Port	Nmap	EqualLogic PS Series storage group
123	ntp	NTP
500*	isakmp	IPsec key exchange

6.4 Common security scanner warnings

Although TCP port 443 is only available on a PS Series storage group for downloading the secure java client and not for administrative access, some commercial security audit applications report an open TCP port 443 as a security risk.

To prevent these warnings from occurring, Dell plans to close TCP port 443 in a future firmware release. The secure java client will continue to be available for download over the default HTTP port 80.

7 Conclusion

A PS Series group offers a variety of mechanisms for preventing unauthorized access to administrative access points or to iSCSI targets.

PS Series storage controller firmware has been certified to conform to the Common Criteria for IT Security Evaluation (CC), version 3.1 by the Federal Office for Information Security most recently in March 2013.

The following actions are recommended to ensure the security of a PS Series SAN:

- Restrict physical access to the SAN.
- Ensure password complexity is consistent with the organizational security policy.
- Logically isolate and firewall the iSCSI and administrative networks.
- Ensure all host systems and applications on the SAN are kept up to date with firmware and software updates, particularly web browsers and SSH clients used for administrative access.
- Ensure secondary services such as DNS and NTP are trustworthy.
- Use SSH for administrative CLI access and disable Telnet access.
- Use SCP rather than FTP for copying files to and from the array members.
- Enable the encryption of administrative GUI traffic.
- Disable legacy cryptographic protocols.
- Use self-encrypting drives (SED) to ensure that no data is lost in the event of a physical security breach.
- If required, use IPsec to secure management traffic and data in flight.
- If required, use a VPN to secure replication traffic.

IPsec will impact performance, particularly for workloads with larger block sizes or workloads that are highly sequential.

A Configuring IPsec

The instructions below enable IPsec communication between a single storage host running Windows Server 2012 and an EqualLogic PS Series storage group using IPv4 addressing.

Pre-shared keys are used as the IPsec authentication method. The security association (SA) will be created using the IKEv1 (Internet Key Exchange) protocol and the IPsec connection will be in Transport Mode.

For more information on the EqualLogic implementation of IPsec and for other examples of configuring IPsec with different operating systems, different authentication methods and different connection modes see the *EqualLogic Group Manager Administrator's Manual*.

To find exact command line usage for configuring IPsec at the EqualLogic Group Manager CLI see the *EqualLogic Group Manager CLI Reference Guide*.

Both of the above documents can be found at the Dell EqualLogic support site (login required):

http://support.equallogic.com

A.1 Configuring a Windows Server 2012 storage host for IPsec

The following instructions will configure the Windows Server 2012 storage host to communicate with a PS Series storage group using IPsec.

A.1.1 Configuring the Windows Server 2012 firewall

Once the below instructions are performed, all inbound traffic from the PS Series storage group and each array member will be allowed to pass through the Windows Server 2012 firewall. Note that outbound traffic from the host to the storage group is allowed by default.

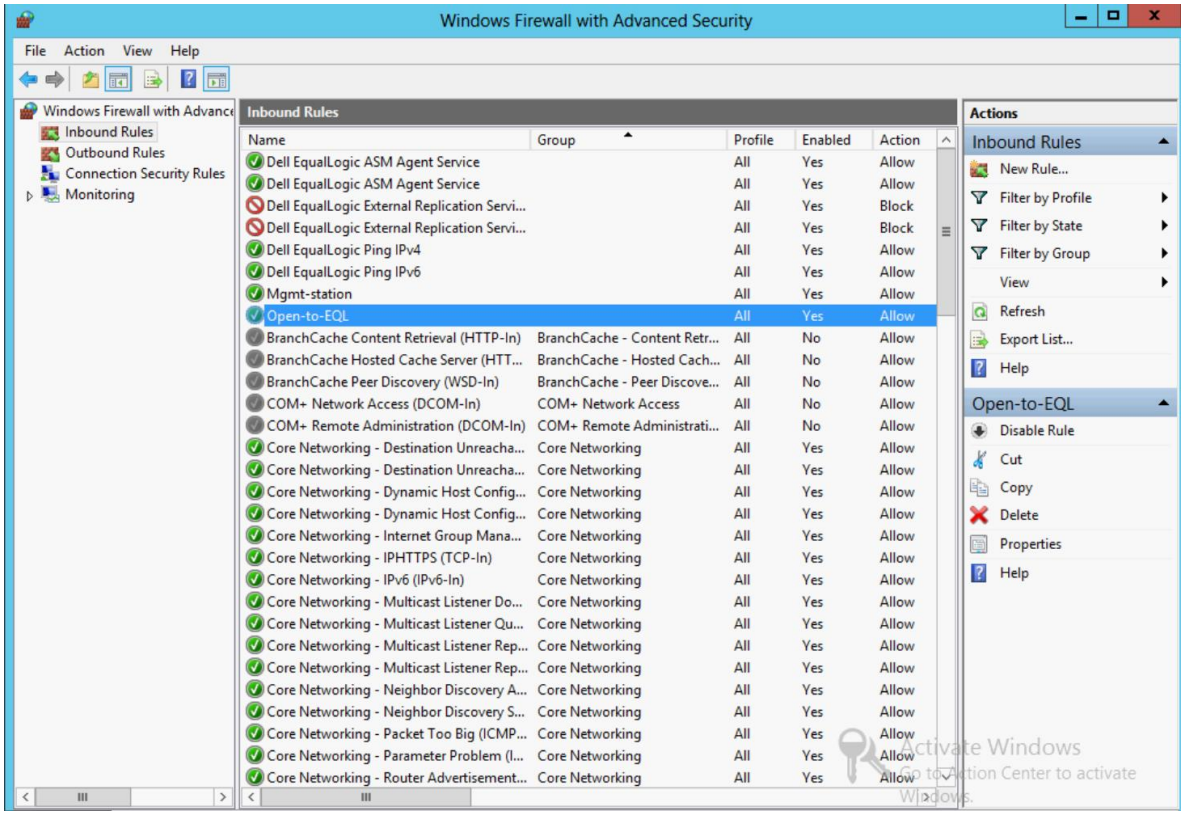

Figure 5 The Windows Firewall with Advanced Security management tool

1. Open the **Windows Firewall with Advanced Security** management tool.
2. Click on **Inbound Rules** and choose to create a new rule.
3. Create a custom rule that applies to all programs and any protocols.
4. Add a SAN interface IP address for needed hosts to the local IP address list.
5. Add the storage group IP address and the IP address of each array member to the remote IP address list.
6. Choose to **Allow the connection**. Do not choose to **Allow the connection if it is secure**.
7. Make the rule apply to the Domain, Private, and Public profiles.
8. Give the new rule a name.

A.1.2 Configuring Windows Server 2012 IPsec defaults

Since it is recommended that legacy cryptographic protocols be disabled (see Section 2.4), it is necessary to add a new security method to the IPsec main mode key exchange. Disabling legacy cryptographic protocols prevents the use of Diffie-Hellman groups shorter than 2048 bits. The new security method will use the Diffie-Hellman Group 14 key exchange algorithm that uses a modular exponentiation group with a 2048 bit modulus.

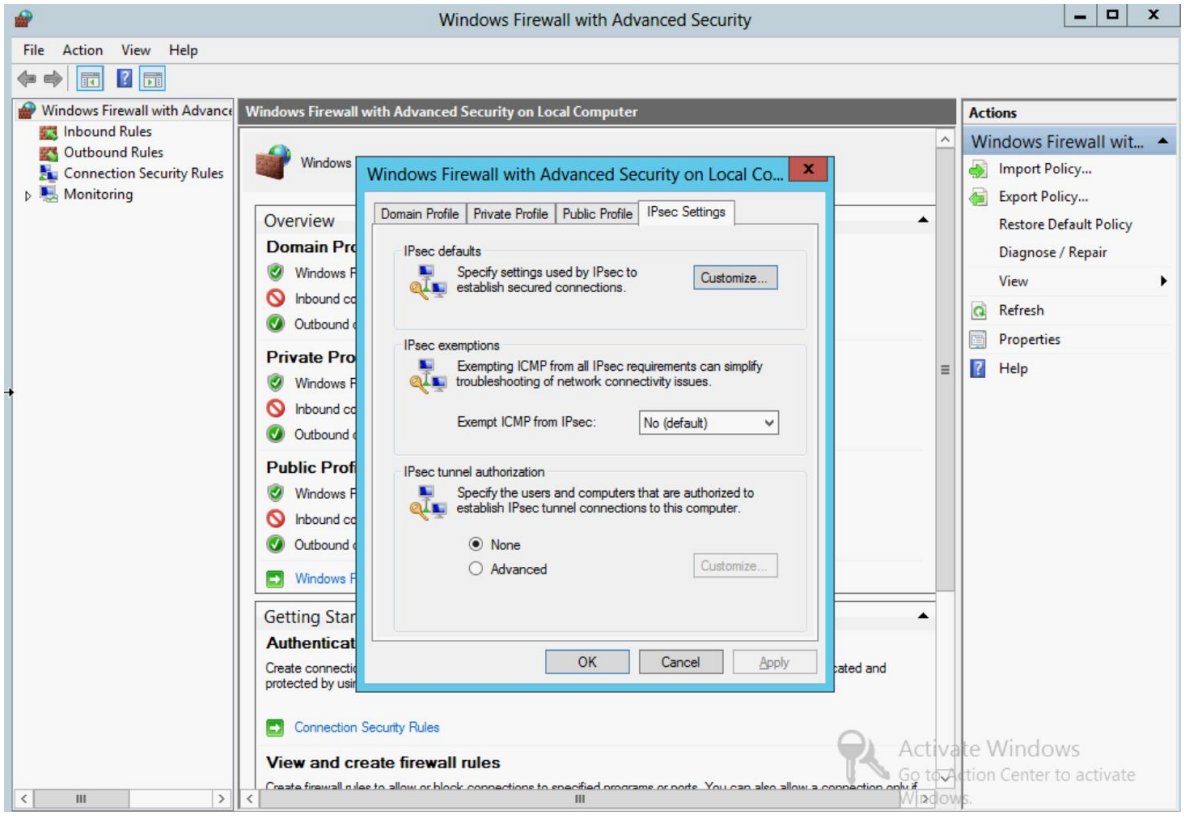

Figure 6 The Windows Firewall with Advanced Security firewall properties window

1. Open the firewall properties window from within the **Windows Firewall with Advanced Security** management tool.
2. Select the **IPsec Settings** tab and choose to customize IPsec defaults.
3. Set **Key exchange (Main Mode)** to **Advanced** and choose to customize.
4. Choose to add a security method and select **Diffie-Hellman Group 14** as the key exchange algorithm.
5. Move the newly created security method to first in the list using the arrow buttons.
6. Dell recommends setting the key lifetime to a minimum of 60 minutes to prevent frequent key exchanges from affecting network performance.
7. Click **Ok** in each open window to save changes.

A.1.3 Configuring a Windows Server 2012 Connection Security Rule

Creating a Windows Server 2012 Connection Security Rule is the equivalent of creating an IPsec security policy. Once the rule is created and enabled, Windows Server 2012 will only communicate with the remote system at a specified IP address if it can successfully establish a security association.

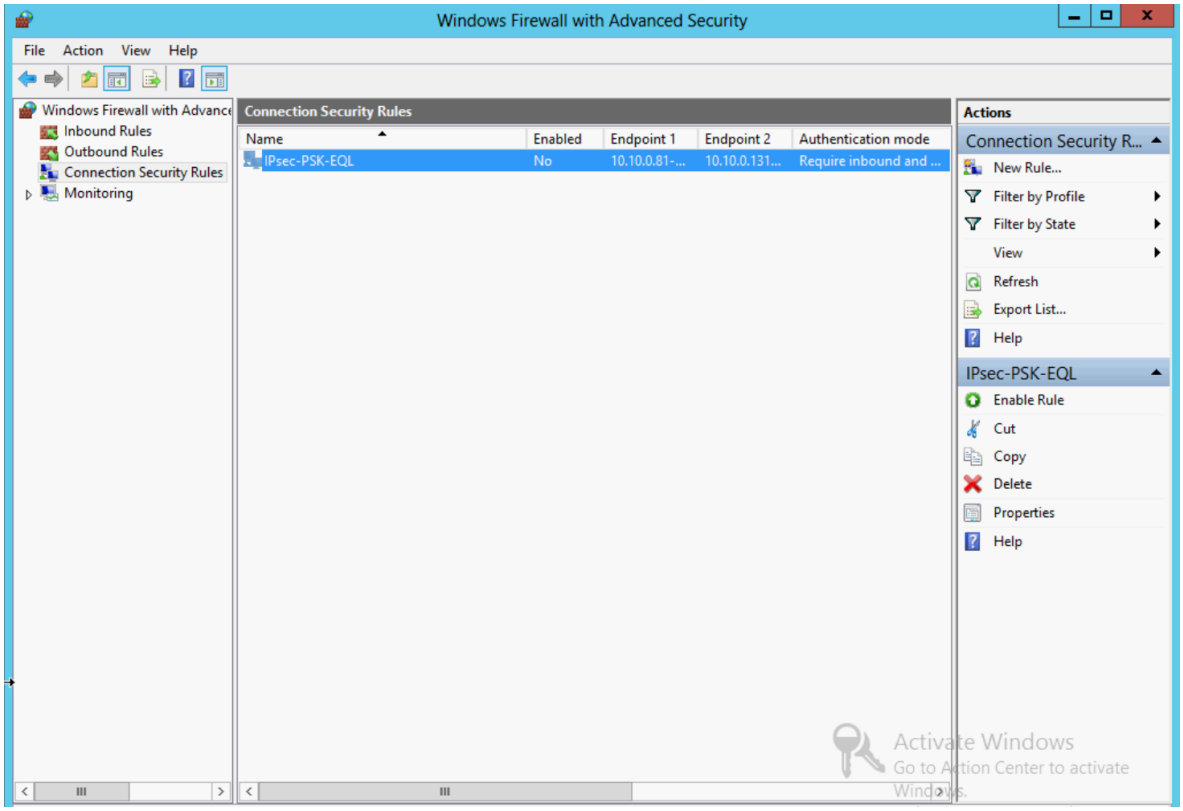

Figure 7 Creating a Connection Security Rule in the Windows Firewall with Advanced Security management tool

1. Open the **Windows Firewall with Advanced Security** management tool.
2. Select **Connection Security Rules** and choose to create a new rule.
3. Create a custom rule.
4. Add a SAN interface IP address for the needed hosts to the local IP address list.
5. Add the storage group IP address and an IP address of each array member to the remote IP address list.
6. Choose to **Require authentication for inbound and outbound connections**.
7. Select the **Advanced** authentication method and choose to customize.
8. Choose to add a first authentication method.
9. Select **Preshared key**, type in the value of the key and click **Ok**.
10. Apply the rule to all ports and protocols.
11. Make the rule apply to the Domain, Private, and Public profiles.
12. Give the new rule a name.

A.2 Configuring a PS Series storage group for IPsec

The following instructions will configure a PS Series storage group to communicate with the previously configured Windows Server 2012 storage host.

1. Enable IPsec globally:

   ```
   psa_group> ipsec enable
   ```

   At this point, all traffic among the storage group array members will be protected with IPsec.

2. Create an IPsec security parameter:

   ```
   psa_group> ipsec security-params create <parameter-name> pre-shared-key
   key <password>
   ```

   The new security parameter will use the preshared key authentication method. The key specified in this command will need to match the key specified in the Windows Server 2012 Connection Security Rule.

3. Create an IPsec security policy:

   ```
   psa_group> ipsec policy create <policy-name> type v4 ip-addr <ip-address>
   protocol any action protect <parameter-name>
   ```

   At this point, all IP traffic (regardless of port or protocol) between the storage group and the remote IP address will be secured with IPsec.

Note: An IPsec security policy can be made to apply to an entire IP subnet by using the netmask parameter. For example:

```
psa_group> ipsec policy create <policy-name> type v4 ip-addr <ip-network>
netmask <netmask> protocol any action protect <parameter-name>
```

B Test configuration details

Hardware	Description
Blade enclosure	Dell PowerEdge M1000e chassis: • CMC firmware: 4.5
Blade server	Dell PowerEdge M620 server: • Windows Server 2012 • BIOS version: 2.1.6 • iDRAC firmware: 1.51.51 • (2) Intel® Xeon® E5-2650 • 64GB RAM • Dual Intel x520-k 10GbE CNA — Driver: 3.7.5.0 — Firmware: 15.0.28 • Dell EqualLogic Host Integration Tools for Microsoft 4.6.0
Blade I/O modules	(2) Dell 10Gb Ethernet Pass-through module
SAN switches	(2) Dell Force10 s4810 • Firmware: 9.3.0.0
SAN array members	(2) Dell EqualLogic PS6110 • (1) 10GbE controllers • (24) SED Seagate ST900MM0036 900GB 10K — Firmware: LEF5 • Firmware: 7.0.1

C I/O parameters

Vdbench SAN workloads were executed using the following parameters in the parameter file.

Common parameters:

```
hd=default
hd=one,system=localhost
```

iSCSI volumes (random IO):

```
sd=sd1,host=*,lun=\\.\PhysicalDrive1,size=102400m,threads=5
sd=sd2,host=*,lun=\\.\PhysicalDrive2,size=102400m,threads=5
sd=sd3,host=*,lun=\\.\PhysicalDrive3,size=102400m,threads=5
sd=sd4,host=*,lun=\\.\PhysicalDrive4,size=102400m,threads=5
sd=sd5,host=*,lun=\\.\PhysicalDrive5,size=102400m,threads=5
sd=sd6,host=*,lun=\\.\PhysicalDrive6,size=102400m,threads=5
sd=sd7,host=*,lun=\\.\PhysicalDrive7,size=102400m,threads=5
sd=sd8,host=*,lun=\\.\PhysicalDrive8,size=102400m,threads=5
```

iSCSI volumes (sequential IO on two arrays):

```
sd=sd1,host=*,lun=\\.\PhysicalDrive1,size=30m,threads=5
sd=sd2,host=*,lun=\\.\PhysicalDrive2,size=30m,threads=5
sd=sd3,host=*,lun=\\.\PhysicalDrive3,size=30m,threads=5
sd=sd4,host=*,lun=\\.\PhysicalDrive4,size=30m,threads=5
sd=sd5,host=*,lun=\\.\PhysicalDrive5,size=30m,threads=5
sd=sd6,host=*,lun=\\.\PhysicalDrive6,size=30m,threads=5
sd=sd7,host=*,lun=\\.\PhysicalDrive7,size=30m,threads=5
sd=sd8,host=*,lun=\\.\PhysicalDrive8,size=30m,threads=5
```

iSCSI volumes (sequential IO on four arrays):

```
sd=sd1,host=*,lun=\\.\PhysicalDrive1,size=45m,threads=5
sd=sd2,host=*,lun=\\.\PhysicalDrive2,size=45m,threads=5
sd=sd3,host=*,lun=\\.\PhysicalDrive3,size=45m,threads=5
sd=sd4,host=*,lun=\\.\PhysicalDrive4,size=45m,threads=5
sd=sd5,host=*,lun=\\.\PhysicalDrive5,size=45m,threads=5
sd=sd6,host=*,lun=\\.\PhysicalDrive6,size=45m,threads=5
sd=sd7,host=*,lun=\\.\PhysicalDrive7,size=45m,threads=5
sd=sd8,host=*,lun=\\.\PhysicalDrive8,size=45m,threads=5
```

8 KB random 67% read workload:

```
wd=wd1,sd=(sd1-sd8),xfersize=8192,rdpct=100,skew=67
wd=wd2,sd=(sd1-sd8),xfersize=8192,rdpct=0,skew=33
```

64 KB random 67% read workload:

```
wd=wd1,sd=(sd1-sd8),xfersize=65536,rdpct=100,skew=67
wd=wd2,sd=(sd1-sd8),xfersize=65536,rdpct=0,skew=33
```

256 KB sequential read workload:

```
wd=wd1,sd=(sd1-sd8),xfersize=262144,rdpct=100,seekpct=sequential
```

256 KB sequential write workload:

```
wd=wd1,sd=(sd1-sd8),xfersize=262144,rdpct=0,seekpct=sequential
```

Runtime options:

```
rd=rd1,wd=wd*,iorate=max,elapsed=1200,interval=5
```

Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and your installations.

Referenced or recommended Dell publications:

- EqualLogic Group Manager Administrator's Manual (site requires login): http://support.equallogic.com
- EqualLogic Group Manager CLI Reference Guide (site requires login): http://support.equallogic.com
- EqualLogic Configuration Guide: http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19852516/download.aspx
- EqualLogic Compatibility Matrix (ECM): http://en.community.dell.com/techcenter/storage/w/wiki/2661.equallogic-compatibility-matrix.aspx
- EqualLogic Switch Configuration Guides: http://en.community.dell.com/techcenter/storage/w/wiki/4250.switch-configuration-guides-by-sis.aspx
- The latest EqualLogic firmware updates and documentation (site requires a login): http://support.equallogic.com
- EqualLogic PS Series Architecture: Self Encrypting Drive Management with PS Series Storage Arrays. http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/20382259.aspx
- Force10 Switch documentation: http://www.force10networks.com/CSPortal20/KnowledgeBase/Documentation.aspx

For EqualLogic best practices white papers, reference architectures, and sizing guidelines for enterprise applications and SANs, refer to Storage Infrastructure and Solutions Team Publications at:

- http://dell.to/sM4hJT

Common Criteria publications:

- http://www.commoncriteriaportal.org/