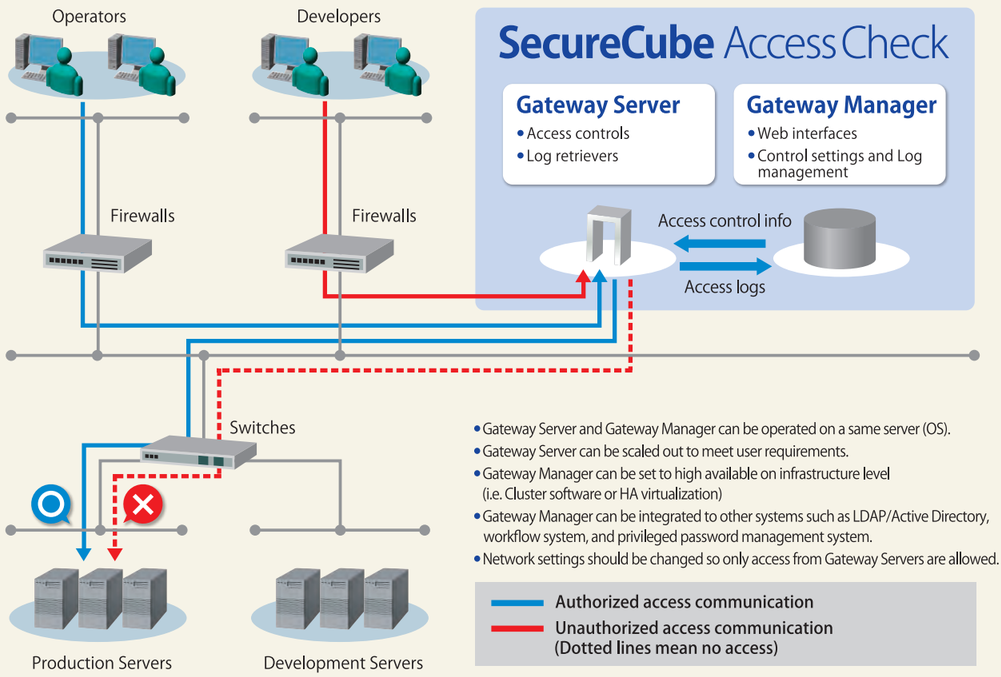
SecureCube / Access Check System Configuration

SecureCube / Access Check comprises two type of servers: Gateway Manager to manage access logs and settings for access control, and Gateway Server that acts as a step server to relay access.



SecureCube / Access Check Operating Environment

Compatible OS	Red Hat Enterprise Linux 6 (6.2 or later, 64 bit) * Virtual environments that ensure operation on the OS above are also supported. * It is also necessary to install and set up the middleware (MySQL, OpenLDAP, etc.) supplied with the OS above.)
Recommended hardware	Hardware or virtual platform on which the OS above runs * CPU: 2.5 GHz × Quad Core or higher (x86_64) * Memory: 4 GB or more * If Gateway Server and Gateway Manager are installed on same server, more than 8GB * HDD: 146 GB or more * Depending on the log storage requirements * Network: 1 or more network interface cards
Supported Languages	Japanese, English, Chinese (Simplified)
Supported Protocols	TELNET, SSH, FTP, SFTP, SCP, RDP, HTTP(S), CIFS, Oracle SQL *Plus, Other TCP

RDP: Remote Desktop Protocol
CIFS: Common Internet File System (Protocol for Microsoft Windows shared folder connection)

NRI Secure Technologies Corp.

Tokyo Sankei Bldg, 1-7-2 Ootemachi Chiyoda Tokyo 100-0004
Homepage http://www.nri-secure.com/
Mail address info@nri-secure.co.jp

Contact us

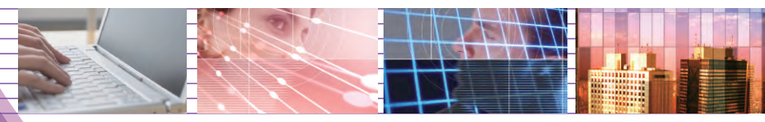
9225-0005-03-1505e

NRI Dream up the future.

SecureCube

Privileged ID Access Management Tool

SecureCube Access Check



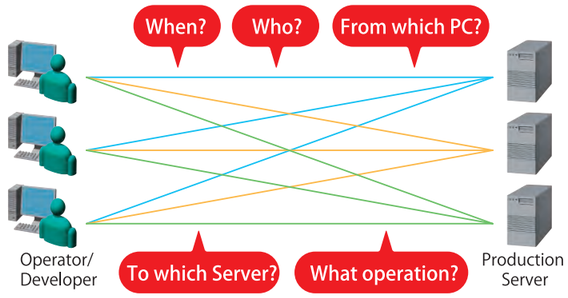
Agent-Less Gateway Type to Realize Short Time, Low Cost, Low Risk Deployment

NRI SecureTechnologies

Privileged ID & Access Management is Critical for Effective Control. **Take Realistic Measures** to Overcome the Great Risk **Now!**

Many information leakage incidents due to privileged ID misuse have told us that a strict management of privileged ID is mandatory. In terms of IT general control, privileged ID management is an emphasized point. In terms of PCI DSS, a security standard for card industry, access management including segregation of duties is an essential requirement. However, when it comes to implementation measures for each system, many challenges emerge: high cost, long time implementation, impact to production systems, and work load on the system operation after implementation. Now, it is necessary more than ever to have cost-effective realistic mechanisms to flexibly deal with continuously growing systems while ensuring the security of the systems.

Before Limitation of conventional method.



Challenge 1 Shared privileged ID/password
- Managing individual IDs for each server are highly burdensome.
- It is difficult to identify individuals if IDs are shared.

Challenge 2 Anyone can access at anytime
- It is difficult to control access for each user.
- Access control setting for each servers /clients is complicated.

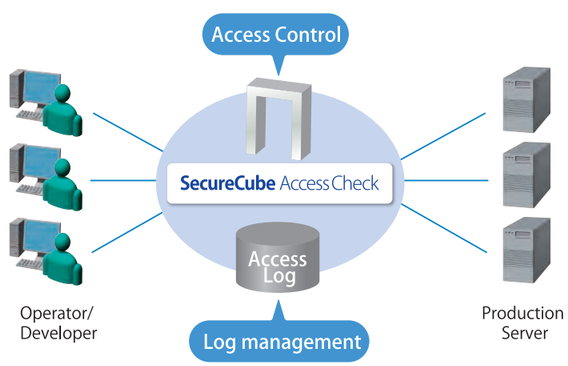
Challenge 3 Logs are placed in each servers
- Matching and monitoring requests and operation logs is a hassle

Gateway Type Privileged ID Management System
SecureCube / Access Check provides the solution!

Best practice of access management based on system development & operation real experience

SecureCube / Access Check is a gateway type access management tool that has characteristic of being able to be deployed in short time without affecting the existing environment because it is completely agentless. Gateway is placed in between of privileged ID users and production servers. In this gateway, users identification, strict access control, and log management are performed. It is also equipped with workflow feature. It improves the efficiency of audit work because all processes from access requests until log auditing are centrally managed.

After Central management of IDs and logs



Solution1 Identifying users on gateway
- Individual identification is performed at the entrance before production servers and ID management will be simpler.

Solution2 Least privileged on gateway
- Access authorization is given based on users or group
- Access control based on access request /approval on gateway

Solution3 Central log management on gateway
- The system improves the efficiency of matching requests and operation logs

SecureCube / Access Check product overview

Preventive Control

Access Control

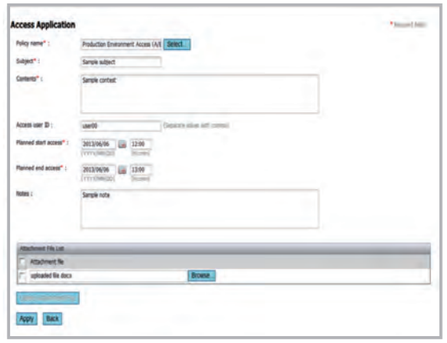
- **Eliminate unauthorized access with granular settings**

Access control is provided in accordance with pre-set policy. The policy defines the permitted access of each role (user group) and system (server group), IP addresses of the connecting terminal, protocols, access approval setting, and so on.

Access Request/Approval

- **Realize the necessary segregation of duties**

Access request/approval feature limits users access rights. When users request for access, administrators will be notified to perform access approval/rejection. This will realize the segregation of duties that is necessary for internal control. All access requests and approvals will be logged. It is effective as audit trail.

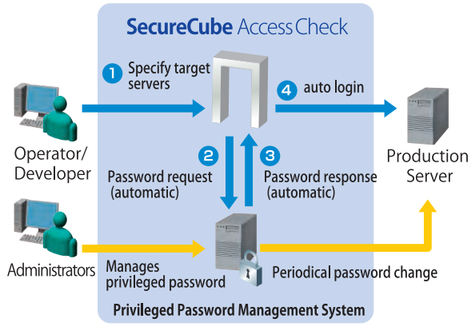


Access request application screen

Privileged Password Management (Optional)

- **Operation without sharing privileged ID passwords**

By integrating it with a privileged password management system, the operation of periodical password change, and non-disclosure of passwords to users can be realized. Concealing the privileged ID password enables a more robust access control because unauthorized login from other than SecureCube / Access Check can also be prevented.

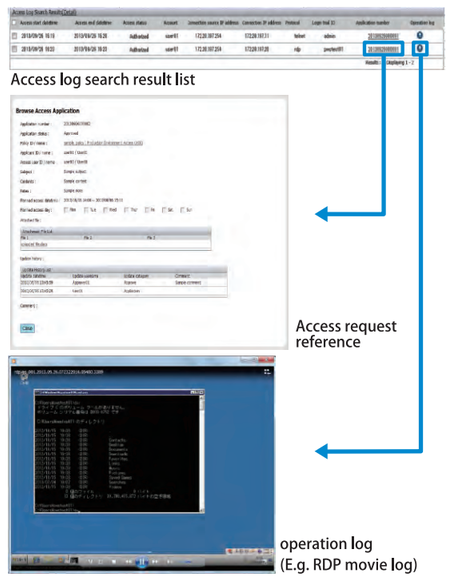


Detective Control

Access Relay and Log Retriever

- **Central management of access log to identify the privileged ID users**

Before accessing servers, users first need to login to SecureCube / Access Check. Only if authenticated, then users can specify the server to access. After the access finish, summary logs (who, when, from where, to which server, under which access request) that show the access overview and operation logs can be retrieved.



Access Log Audit

- **Efficiency of checking of large volume logs and access requests**

Each access log is automatically linked to registered access request. These logs can only be searched and viewed from web interface by authorized administrators. The system can also record the confirmation trails towards the access request and access logs.