Huawei Terminal Security Management Solution
— Create Enterprise Intranet Security
Introduction

According to the third-party agencies such as the Computer Security Institute (CSI), Federal Bureau of Investigation (FBI), International Data Corporation (IDC), and the National Computer Network Emergency Response Technical Team/Coordination Center of China information (CNCERT/CC), most security incidents occur in the enterprise intranet. Security at the terminal of an intranet has become the biggest challenge for enterprise IT managers. Incidents involving information leaks, unauthorized access, slowdown or breakdown of machines, core service interruption, and network disconnection cause huge losses for enterprises. Traditional desktop management or terminal security management (TSM) solutions are insufficient in forcibly deploying TSM clients on terminals and preventing malicious attacks from occurring. The following problems must be solved to seek a new solution:

- It is hard to find a right network access control (NAC) solution that can adapt to the highly complex access environments (HUB access, wireless access, VPN, NAT, and remote branch offices, with devices from multiple manufactures) while supporting system upgrades and reconstruction at the same time.
- It is hard to keep up with the constant requirements of terminal security at the lowest cost.
- It is hard to deploy and manage the TSM system with limited resources and unskilled IT administrators.

Based on years of experience in the TSM field, Huawei TSM team has developed an intuitive and user-friendly NAC solution that not only provides flexible security to access gateways but also basic network devices such as switches and routers. A document security management (DSM) system has also been added in the solution providing users with powerfully enhanced document management services. In this solution, operators can directly control user access to the network by using switches and routers in the basic network without affecting the network performance and reliability. In scenarios where access control points cannot be deployed on switches or routers, a security access gateway is added to the live network for access control. As a result, devices do not need to be replaced during network reconstruction.

By using identity-based networks, Huawei TSM solution provides the following basic functions:
- Access control
- Security management
- Desktop management
- Document management

These functions are closely integrated to ensure terminal security. Security management acts as the core function, while the access control provides active measures for the solution, and desktop management and document management are supplementary functions. This solution equips enterprises with a completed end-to-end TSM system, which is cost-effective to construct and easy to maintain.

Huawei TSM solution has the following features:
- Reduces the risks involved in IT systems, such as information leaks, malicious code spreading, network or service interruption, compliance risks, and asset loss
- Improves the overall performance of terminals, network, and applications
• Reduces hidden costs in asset management and maintenance

Once Huawei TSM solution is applied, the following tasks are fully operational:

• Improving IT availability and security
• Reducing the cost in intranet security management
• Improving intranet management efficiency

Figure 1-1 TSM design

The TSM system and the DSM system constitute the Huawei TSM solution.

The TSM system consists of:

• Terminal management center (TMC)
• Security agent (SA)
• Security manager (SM)
• Security controller (SC)

NAC devices, including switches, routers, and security access control gateway (SACG)

The DSM system consists of:

• Document management center (DMC)
• Document management server (DS)
• Document proxy client (DC)
Table 1-1 TSM system component

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMC</td>
<td>The TMC software is used for layered management and deployment. As the management center for Huawei TSM solution, TMC is used to make overall security policy, deliver the policy to TSM nodes, and monitor the policy implementation on these nodes.</td>
</tr>
<tr>
<td>SA</td>
<td>The SA software is installed on terminal hosts to automatically collect information about terminal assets and security status, and help users in identity authentication and security check. SA occupies a small number of terminal resources and consumes a small amount of system resources. The CPU usage is less than 2%, and the maximum memory usage is 15 MB.</td>
</tr>
<tr>
<td>SM</td>
<td>The SM software is the core security management module for Huawei TSM solution, and provides services such as assets management, software distribution, patch management, log audit, TSM policy management, identity management, and report management. An SM adopts a Browser/Server (B/S) structure for the administrator to control the system on web pages. An SM can manage multiple SCs. The SM and the SC constitute the server for the TSM system.</td>
</tr>
<tr>
<td>SC</td>
<td>The SC software manages the SA based on data configured by the SM. The SM gives instructions for the SC to coordinate related devices and provide management services. After a user pass the SA authentication, the SC controls devices such as switches, routers, and the SACG at the access control point to enable the user to access the network.</td>
</tr>
<tr>
<td>Switch</td>
<td>The switch is the network hardware that controls terminal access to the network and enables different access rights to terminal users of different identities in different security state. Switches used for security access control can be deployed at the access layer or the aggregation layer, and is necessary in basic networking.</td>
</tr>
<tr>
<td>Router</td>
<td>The router is the network hardware for terminal access control, and is also necessary in basic networking. You can select routers or switches as NAC devices based on network deployment requirements.</td>
</tr>
</tbody>
</table>
The DS software is in charge of handling terminal users' requests, user authentication, user authorization, encryption, decryption, and log audit. The DS also saves and manages document permissions and keys.

The DMC software is deployed at the first layer in the DSM architecture and functions as the management server. The DMC controls the access of servers on the second layer. The DMC manages users, alarms, servers, and policies.

The DC software provides functions such as document encryption, document permission control, offline reading, and document recovery.

The SACG is a security access gateway that controls terminal access to the network and enables different access rights to terminal users of different identities in different security states. When switches and routers cannot be deployed, you can add SACG devices for access control.

The DSM system consists of the DS, DMC, and DC.

### Table 1-2 DSM system component

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DC</strong></td>
<td>The DC software provides functions such as document encryption, document permission control, offline reading, and document recovery.</td>
</tr>
<tr>
<td><strong>DMC</strong></td>
<td>The DMC software is deployed at the first layer in the DSM architecture and functions as the management server. The DMC controls the access of servers on the second layer. The DMC manages users, alarms, servers, and policies.</td>
</tr>
</tbody>
</table>
Solution Features

The TSM solution provides comprehensive network access modes for different access terminals in enterprises.

- Supports 802.1x, portal, and firewall access control modes based on switches, routers, or Security Access Control Gateways (SACGs).
- Supports the deployment of NAC across multiple connection modes such as wireless network adapter, network cable, Virtual Private Network (VPN), and dial-up network.
- Uses switches and routers to control user access. Devices do not need to be replaced during network reconstruction. Therefore, the network performance, reliability, and scalability are not affected.
- Offers various authentication modes to flexibly control terminal access between various operating systems, between enterprise employees, affiliated partners, and customers. This ensures consistent and friendly user experience.

The TSM solution greatly reduces management and maintenance costs.

- Allows users to deploy terminals by stages and flexibly control the deployment progress.
- Provides server push technology for convenient deployment on a client terminal.
- Provides integrated configuration management interfaces to automatically identify non-PC devices. This alleviates engineers from collecting, registering, and maintaining non-PC devices.
- Provides identity authentication and guest management services to control the access of extranet and Internet users to intranet resources, reducing the administrator’s workload.
- Provides automatic warning for unauthorized behavior, one-key automatic recovery or guided recovery. This realizes self-management on a terminal.
- Identifies a terminal’s location and automatically selects security policies for employees in remote offices to conveniently access the intranet.
- Scores network management and terminal compliance, and evaluates the terminal security status and security trend.

The TSM solution provides excellent security management functions, implementing end-to-end security protection.

- Provide an all-around TSM system for enterprises that integrates identity authentication, network access control, terminal security hardening, office operation and network access management, network protection, information leak protection, asset management, software deployment, remote assistance, and message bulletins.
- Integrates document security management and portable storage device management, forming the most dependable end-to-end security solution in the TSM field.
The TSM solution meets personalized and customized requirements of enterprises.

- Supports expansion of the database size to meet requirements for auditing logs in large-scale databases.
- Supports self-defined checking policies including self-defined checking items, terminal prompt messages, violation reporting messages, and automatic recovery actions.
- Pre-defines a large number of security policies and daily management reports. Users can also self-define and collect a library of security policies and daily management reports from Huawei cloud security center to meet personalized and constant security requirements.
- Monitors the intranet security situation based on intelligent analysis and deep data mining, which provides maintenance and policy supports for IT management.

The TSM solution features excellent reliability and ensures that the network runs properly.

- Uses carrier-class hardware devices and supports the two-node cluster and network interruption survival functions. The reliable and secure solution ensures service continuity.
- Provides distributed file storage and rapid file distribution on a subnet for large files, which realizes minimum bandwidth occupation and high-efficiency distribution.
- Provides a monitoring platform that can detect potential faults and generate alarms in the case of faults. The system administrator can remotely monitor the system’s running status.
- Provides online fault diagnosis and rectifies client faults in batches.

The TSM solution and the DSM system constitute as an end-to-end Huawei TSM solution.

The powerful DSM system can manage document permissions, and effectively control access to certain documents that may be shared between enterprise employees, affiliated partners, and customers by implementing restrictions on users, access modes, and access time. The real-time permission control allows users to change or retrieve document permissions at any time.
Huawei TSM Solution Components

Figure 1-4 Huawei TSM solution components

<table>
<thead>
<tr>
<th>Item</th>
<th>Component</th>
<th>Product Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAC devices</td>
<td>Access switch</td>
<td>S5700, S3700, and S2700</td>
</tr>
<tr>
<td></td>
<td>Aggregation switch</td>
<td>S7700 and S5700</td>
</tr>
<tr>
<td></td>
<td>Core switch</td>
<td>S9300</td>
</tr>
<tr>
<td></td>
<td>UTM firewall or the integrated device</td>
<td>E200E-X and E1000E-X</td>
</tr>
<tr>
<td>Software</td>
<td>Access control server</td>
<td>TSM Server</td>
</tr>
<tr>
<td></td>
<td>Access control client</td>
<td>TSM Agent</td>
</tr>
<tr>
<td></td>
<td>DSM sever</td>
<td>DSM Server</td>
</tr>
<tr>
<td></td>
<td>DSM client</td>
<td>DSM Client</td>
</tr>
</tbody>
</table>

Order Information

Table 1-3 Order information

<table>
<thead>
<tr>
<th>Item</th>
<th>Component</th>
<th>Product Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch</td>
<td>The switch is a basic network device that includes the terminal access control module and is not restricted by the license control. You can select a proper model based on the actual networking.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Router</td>
<td>The router is a basic network device that includes the terminal access control module and is not restricted by the license control. You can select a proper model based on the actual networking.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>TSM server</td>
<td>The TSM server provides control items for the following functions: Access control Security policy management Access management Software distribution Patch management Personnel operation management You can select the functions based on the actual requirements.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>Item</td>
<td>Component</td>
<td>Product Model</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>TSM terminal licenses</td>
<td>Each function has a terminal license, the number of which is the same as that of terminals on the live network. Licenses for all functional modules must be the same.</td>
<td>Mandatory</td>
</tr>
<tr>
<td>DSM server</td>
<td>The DSM server provides services to manage documents and ensure document security.</td>
<td>Optional</td>
</tr>
</tbody>
</table>
| DSM terminal licenses | The quotation prices of the DSM terminal license vary with the following sections of terminal numbers:  
1–99  
100–199  
200–499  
500–999  
1000–1999  
2000–4999  
5000 and more  
The number of licenses is the same as those of terminals on the live network. | Optional      |
| SACG               | You can select a proper model based on the NAC plan.                       | Optional      |
| Purchased products | You can select a host server, an operating system, a database, or prepare these products by yourself. | Optional      |
| Service            | System installation and commissioning services for security devices        | Optional      |