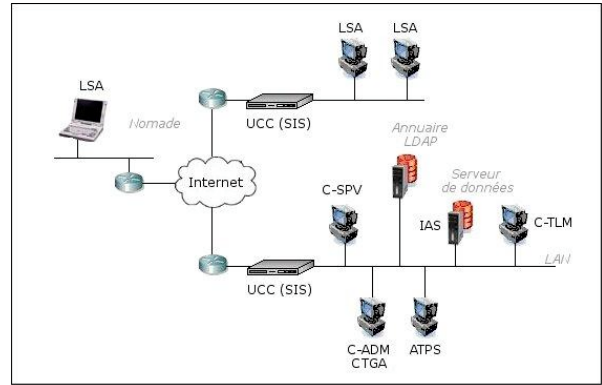


SIS : Système d'Interconnexion Sécurisé

Certifié ITSEC E3



La présence de cet équipement garantit un service de contrôle d'accès efficace « en entrée » et « en sortie » du réseau protégé.



Ouvrir votre réseau, en toute sécurité

Vous souhaitez raccorder votre réseau d'entreprise à Internet, accéder aux autoroutes de l'information ...

L'évolution de votre système d'information nécessite l'interconnexion de vos sites via un réseau public ...

Pourtant, la sensibilité de vos installations et de vos données vous impose de garantir une protection efficace, alors même que l'interconnexion avec des réseaux publics multiplie les risques d'intrusion dans votre système d'information.

Pour ouvrir de manière fiable votre réseau d'entreprise vers l'extérieur, vous devez le doter d'un système de sécurisation vous permettant d'une part de contrôler les accès externes à votre entreprise, et d'autre part de réguler le trafic sortant.

SIS : une sécurisation efficace

Le SIS est un ensemble matériel et logiciel offrant une gamme étendue de services de sécurité. Il est notamment composé d'un équipement dédié, appelé UCC (Unité de Contrôle et de Commutation) placé en coupure Ethernet, « à l'entrée » du sous-réseau à sécuriser, comme un point de passage obligé, et donc incontournable.

Les points forts du SIS

- Filtrage niveau protocoles et services (Firewall),
- Gestion des vlans,
- Traitement de la Qos IP
- Authentification forte des utilisateurs, administrateurs et serveurs : carte à puce, tokens USB, certificats...
- Sécurisation de site à site avec chiffrement fort (VPN-GFM) et tunnel IP inter-sites (IP-VPN)
- VPN SSL entre station (cliente ou serveur) et UCC
- Haute disponibilité des UCC et tunnel IP-VPN
- Filtrage des communications des VPN
- Authentification forte via les VPN
- Translation d'adresses IP
- Détection d'intrusions et gestion d'alarmes
- PKI de génération des moyens d'authentification
- Administration, supervision et maintenance à distance

Pour plus d'informations :

www.acetiming.fr

contact@acetiming.fr

ACE TIMING
COMMUNICATIONS DE DONNEES

Solutions d'authentification forte

Le SIS dispose de différentes solutions d'authentification renforcées permettant d'authentifier à la fois l'utilisateur d'une station cliente et le serveur destinataire de la communication.

- ◆ Authentification à **clé secrète** par carte à puce physique, token ASKey, carte à puce virtuelle, token USB ActivKey®, calculette ActivCard.
- ◆ Authentification par **certificat numérique X509** stocké sur carte à puce ASCard, token ASKey, disque dur ou clé USB.

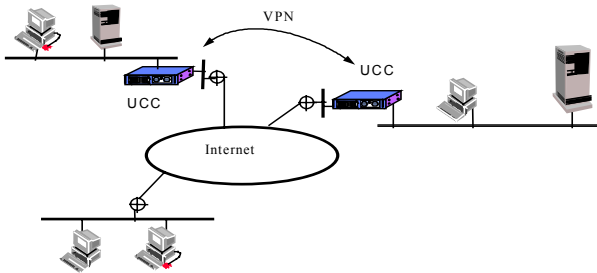
Techniques de contrôle d'accès

- Filtrage des communications LAN et VLAN,
- Commutation conditionnelle sur protocole,
- Filtrage logiciel au niveau IP/IPSEC,
- Filtrage de la Qos IP,
- Filtrage des données des services TCP et UDP.

Services de confidentialité (VPN)

La confidentialité des données des datagrammes transitant sur des réseaux ouverts, entre différents sites équipés de **SIS** est obtenue par la création d'un **VPN** (Virtual Private Network) entre deux UCC ou entre une station cliente une UCC et ou entre un serveur et une UCC

- ◆ **Service GFM-VPN** (Groupe Fermé de Machines – VPN)
Chiffrement à la volée des données de chaque datagramme UDP et TCP d'une communication transitant entre deux UCC. Ce chiffrement est réalisé de manière indépendante pour chaque communication (clé de chiffrement différente).
- ◆ **Service TIP-VPN** (Tunnel IP VPN)
Encapsulation et chiffrement des datagrammes IP ou ARP des communications transitant via un tunnel IP établi préalablement entre les deux UCC.



- ◆ **Service OVPN-SSL**
Confidentialité des communications transitant entre un poste client (fixe ou nomade) ou serveur et une UCC. Ce service est basé sur la création d'un **VPN** entre un « client *OpenVPN®* » et l'UCC.

Imputabilité

Afin d'effectuer la traçabilité des communications, une UCC journalise en local, et à distance via la console de supervision, l'ensemble des tentatives de communications filtrées.

Services de télégestion

- ◆ **Administration distante**
Une console d'administration déportée permet de centraliser la configuration et la définition de la politique de sécurité d'une ou plusieurs UCC. Ces données sont ensuite téléchargées sur l'UCC concernée. Cette application peut également interroger un annuaire LDAP pour récupérer les données centralisant les données d'environnement (utilisateurs, machines, etc...). Elle permet également, après rapatriement, l'audit des journaux d'imputabilité générés sur une UCC.
- ◆ **Supervision distante**
Une console de supervision permet la visualisation à distance et en temps réel des communications ou tentatives de communications réalisées au travers d'une UCC.
- ◆ **Télémaintenance**
Afin de faciliter la configuration et la maintenance d'une UCC après son installation et sa mise en exploitation, une console de télémaintenance permet d'exécuter à distance certaines opérations de configuration et d'audit.

Ces opérations sont entourées de mesures particulières de sécurité (authentification de l'administrateur par carte à puce physique ou virtuelle, chiffrement des données).

Détection d'intrusion

Afin d'alerter en temps réel l'administrateur d'une tentative d'intrusion, la console de supervision est en mesure de générer des alarmes permettant entre autres, l'exécution d'un programme ou l'envoi d'un mail à un administrateur.

Haute disponibilité

Afin de garantir une continuité de service, l'UCC dispose d'un système de détection de défaillances matérielles et logicielles permettant le basculement du trafic sur une autre UCC de relais sans perte des communications en cours. La synchronisation des données entre UCC est réalisée automatiquement en temps réel.

PKI

Bien que le SIS permette l'exploitation des certificats générés par une PKI publique, il dispose d'un atelier de personnalisation permettant de gérer ses propres certificats X509 et de personnaliser les cartes à puce ASCard (de type MPCOS-EMV ou GemXpresso), les tokens ASKey et les tokens USB ActivKey®.