seclāb

Sécurisation de vos interconnexions réseaux

DENELIS SECURE XCHANGE

La preuve par 4 |

seclāb
Next-gen cybersecurity
for critical systems

LA SÉCURISATION DE VOS INTERCONNEXIONS RÉSEAUX

Seclab propose une solution unique de haut niveau de sécurisation de vos échanges réseaux par simple interposition (plug and play) d'un boîtier électronique paramétrable DENELIS®.

PROTEGEZ VOS SYSTEMES DES CYBERATTAQUES CIBLEES

Une cyberattaque débute par une phase préalable, d'autant plus dangereuse qu'elle est le plus souvent invisible, indétectable et qu'elle peut durer plusieurs mois ainsi. C'est la phase au cours de laquelle les cybercriminels recueillent, à votre insu, de l'information sur votre infrastructure : réseaux et systèmes (serveurs, automates, objets connectés).

Ils procèdent généralement en 3 étapes : une étape de reconnaissance (footprinting), une étape de découverte (scanning) et une étape de qualification des vulnérabilités (enumeration).

La démarche est identique à celle de cambrioleurs qui procèdent d'abord à un repérage passif des allers et venues dans une rue («reconnaissance») avant de définir une ou plusieurs cibles et d'identifier les points d'entrée possibles («découverte») puis de repérer les points de vulnérabilité (serrures, alarmes, …) afin d'évaluer la capacité à pénétrer par effraction («qualification»).

Cette phase préalable est toujours présente dans les attaques ciblées (ex. un Etat, une entreprise, une installation). Malheureusement les victimes ne s'en aperçoivent qu'après coup car cette phase n'est généralement pas détectable.

Le seul moyen efficace de prévention est de masquer votre installation. Pour une robustesse maximale, le procédé de masquage Seclab ne se limite pas à du logiciel et combine également des protections électroniques brevetées*.

PROTÉGEZ VOS SYSTÈMES DES CYBERATTAQUES MASSIVES

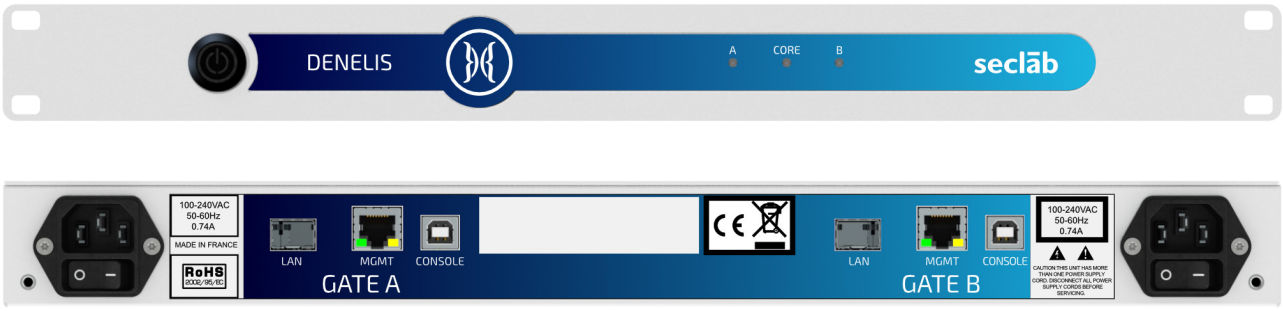
Pour les attaques massives qui agissent à l'aveugle, elles n'ont pas besoin, par définition, d'une phase de reconnaissance préalable. Elles vont contaminer directement tous les systèmes interconnectés. Le seul moyen de prévention 100% efficace consiste à isoler les systèmes pour éviter la propagation. Mais dans le même temps, les systèmes doivent pouvoir continuer à échanger pour fonctionner. Il faut donc résoudre une double contrainte : isoler pour éviter d'être contaminé mais rester ouvert pour maintenir les équipements en condition de fonctionnement.

Nous y parvenons grâce à notre boîtier DENELIS® qui fait office de bouclier électronique entre vos réseaux et interdit ainsi toute propagation d'une éventuelle attaque par les couches de transport.

En résumé, grâce à nos boîtiers DENELIS®, votre infrastructure est :

- Indétectable (masquée), ce qui interdit tout repérage en préalable à une attaque ciblée ;
- Isolée, afin d'empêcher toute propagation par les couches de transport en cas d'attaque massive ou "en aveugle".

** Brevet WO2010076514 - 2010-07-08*



Faces avant et arrière d'un boîtier DENELIS®

RENFORCEZ ENCORE LA SÉCURITÉ DE VOS INTERCONNEXIONS

Au-delà du masquage et de l'isolation de vos réseaux et systèmes (serveurs, automates, objets connectés) par l'interposition de nos boîtiers DENELIS®, vous pouvez avoir besoin d'un niveau de sécurisation supplémentaire, garantissant que seuls certains flux puissent passer.
Ce point est particulièrement important dans les systèmes critiques qui doivent ne recevoir que certains types de flux, connus et identifiés d'avance.

Nos puissantes fonctions de filtrage portent sur 2 niveaux :
- Filtrage du type de protocole (ex. un industriel peut vouloir que seul le protocole MODBUS puisse passer) ;
- Vérification des commandes ou valeurs transmises (ex. seules des commandes de lecture doivent pouvoir passer, celles en écriture étant bloquées afin de protéger les systèmes de toute modification).

ASSUREZ L'ÉCHANGE SÉCURISÉ DE FICHIERS ENTRE DEUX RÉSEAUX ISOLÉS PAR DENELIS®

Nos boîtiers DENELIS® répondent à vos besoins de transfert fichiers tout en conservant vos réseaux isolés pour une sécurité optimale. En effet, l'électronique embarquée permet, avec cette option, de faire passer des fichiers d'un réseau A vers un réseau B sans les interconnecter pour autant. Cela supprime l'usage risqué de clefs USB entre 2 réseaux isolés. De plus, cette fonction de "Transfert de fichiers", combinée avec l'option "Filtrage", rend possible la signature électronique de fichiers (cryptographie) et sa vérification. C'est pour vous la garantie de l'intégrité des fichiers transportés et l'assurance de leur provenance.

Cette vérification de provenance et d'intégrité peut concerner :
- Des réseaux internes de votre installation ou organisation ;
- Des réseaux tiers (sous-traitants, fournisseurs, partenaires), comme par exemple dans le cas de mises à jour de logiciels.

1 INTERDIRE TOUTE PHASE PRÉALABLE À UNE ATTAQUE CIBLÉE, EN MASQUANT VOTRE RÉSEAU

DOMAINES D'APPLICATION

Situations nécessitant de dissimuler un réseau sensible relié à un réseau de niveau de sécurité moindre pour assurer des échanges nécessaires à l'exploitation, comme par exemple :

- Entre un réseau protégé et un réseau d'un niveau de sécurité moindre ;
- Entre un réseau isolé et un réseau public (Internet) ;
- Entre un réseau d'exploitation et un réseau de supervision.

CAS D'USAGE

Les routeurs, serveurs, postes de travail et automates d'un réseau sensible doivent restés indétectables afin de résister aux attaques directes de type :

- scanning (découverte du matériel connecté) ;
- sniffing (capture du trafic réseau pour analyse) ;
- DNS hijacking (usurpation de service réseau utilitaire pour découvrir du matériel communicant).

Garder confidentielle la topologie, la profondeur et la configuration d'un réseau sensible même en considérant que l'attaquant, maître du réseau le moins sûr, peut observer le trafic pour :

- Capturer des adresses IP (découverte du matériel connecté) ;
- Analyser à quels serveurs du réseau protégé sont envoyés et reçues les données ;
- Savoir combien de systèmes sont connectés dans le réseau protégé.

Être invulnérable aux attaques réseau conçues pour atteindre des systèmes du réseau protégé à travers les firewalls :

- ICMP crafting (forge des paquets de couche 3 du modèle OSI pour déclencher des pannes) ;
- IP Address spoofing (ursurpation d'identité) ;
- Toute attaque réseau tentée depuis un firewall corrompu (impossible avec DENELIS®).

2 ISOLER VOTRE RÉSEAU AFIN D'ÉVITER TOUTE PROPAGATION D'UNE ATTAQUE

DOMAINES D'APPLICATION

Situations nécessitant l'isolation réseau d'une zone protégée entourée de réseaux de niveau de sécurité et de criticité plus faible, comme par exemple :

- Entre un réseau protégé et un réseau d'un niveau de sécurité moindre ;
- Entre un réseau isolé et un réseau public (internet) ;
- Entre un réseau d'exploitation et un réseau de supervision.

CAS D'USAGE

- Protection contre les attaques par déni de service.
- Protection contre les attaques réseau de la couche transport :
  - Couche 4 : Transport Layer - TCP syn flooding, UDP flooding (déni de service) ;
  - Couche 3 : Network Layer - IP modification, DHCP attack, ICMP attack (usurpation, détournement de trafic) ;
  - Couche 2 : Data Link Layer - MAC modification, MAC attack, MAC flooding (usurpation, détournement. de trafic).
- Protéger un réseau contre la propagation de malware utilisant des attaques de la couche transport pour prendre le contrôle de routeurs, de serveurs, de postes de travail afin de s'étendre depuis un réseau contaminé vers un réseau isolé.

3 INVISIBLE ET ISOLÉ MAIS TOUJOURS COMMUNIQUANT : LA SECURITÉ TOUT EN RESTANT PERFORMANTS

DOMAINES D'APPLICATION

Situations nécessitant d'échanger des flux entre 2 réseaux isolés, même s'ils ont des niveaux de confiance différents, comme par exemple :

- Réseau industriel (A) et réseau de gestion (B) ;
- Réseau confidentiel interne tel que R&D, cellule de crise, PC-Sécurité (A) et réseau général de l'entreprise (B) ;
- Réseau interne (A) et réseau d'un fournisseur ou d'un partenaire (B) ;
- Réseau interne (A) vers un réseau public (web).

CAS D'USAGE

- Accès à des applicatifs réseau ou web (ex. donner accès à un intranet de support ou publier des mises à jour pour des clients, applications clients/serveur, http, https, TLS 1.2) ;
- Communications industrielles de type ModBus, BacNet, S7, OPC-UA, ... ;
- Accès à des bases de données :
  - application métier dans le réseau A qui dialogue avec une base de données dans le réseau B ;
  - réplication de bases de données en exploitation comme en plan de reprise d'activité ;
  - réplication de bases de données dans une zone sécurisée ;
  - etc.
- Communications "machine to machine" ;
- Services réseau de type Syslog, SNMP, NTP, DHCP, DNS :
  - Centralisation des logs pour analyse (SIEM, SOC) ;
  - Mise à jour du temps (horloge) sur des serveurs ou des automates isolés depuis un serveur public
  - Monitoring des serveurs et automates isolé depuis un réseau distant ;
  - Gestion centralisée des plans d'adressage réseau ;
  - etc.

4 TRANSFERT DE FICHIERS HAUTEMENT SÉCURISÉ

DOMAINES D'APPLICATION

Situations nécessitant des échanges de fichiers maîtrisés entre deux réseaux isolés, même s'ils ont des niveaux de confiance différents, comme par exemple :

- Un réseau industriel protégé et un réseau de gestion ;
- Un réseau d'exploitation et un réseau d'administration IT (sauvegardes et restaurations) ;
- Un réseau isolé et Internet ;
- Un réseau isolé ou protégé et le réseau d'un tiers.

CAS D'USAGE

- Export de journaux de logs (décharge de logs de systèmes isolés, export de dump d'erreur) ;
- Récupération de statistiques de fonctionnement ;
- Export de fichiers de sauvegarde et leur rechargement avec contrôle d'intégrité ;
- Chargement de fichiers de mises à jour (OS, firmware, logiciel…) vers un réseau isolé ;
- Import de fichiers de configuration ou d'exploitation dans un réseau isolé ;
- Echange de fichiers entre tiers sans création d'interconnection réseau.

DENELIS® BY SECLAB : LA PREUVE PAR QUATRE (RESUME)

DOMAINES D'APPLICATION	CAS D'USAGE
1. INTERDIRE TOUTE PHASE PREALABLE A UNE ATTAQUE CIBLEE, EN MASQUANT VOTRE RESEAU Situations nécessitant de dissimuler un réseau sensible relié à un réseau de niveau de sécurité moindre pour assurer des échanges nécessaires à l'exploitation, comme par exemple : • Entre un réseau protégé et un réseau d'un niveau de sécurité moindre ; • Entre un réseau isolé et un réseau public (Internet) ; • Entre un réseau d'exploitation et un réseau de supervision.	• Les routeurs, serveurs, postes de travail et automates d'un réseau sensible doivent restés indétectables afin de résister aux attaques directes de type : ◦ scanning (découverte du matériel connecté) ; ◦ sniffing (capture du trafic réseau pour analyse) ; ◦ DNS hijacking (usurpation de service réseau utilitaire pour découvrir du matériel communicant). • Garder confidentielle la topologie, la profondeur et la configuration d'un réseau sensible même en considérant que l'attaquant, maître du réseau le moins sûr, peut observer le trafic pour : ◦ Capturer des adresses IP (découverte du matériel connecté) ; ◦ Analyser à quels serveurs du réseau protégé sont envoyés et reçues les données ; ◦ Savoir combien de systèmes sont connectés dans le réseau protégé. • Être invulnérable aux attaques réseau conçues pour atteindre des systèmes du réseau protégé à travers les firewalls : ◦ ICMP crafting (forge des paquets de couche 3 du modèle OSI pour déclencher des pannes) ; ◦ IP Address spoofing (ursurpation d'identité) ; ◦ Toute attaque réseau tentée depuis un firewall corrompu (impossible avec DENELIS®).
2. ISOLER VOTRE RESEAU AFIN D'EVITER TOUTE PROPAGATION D'UNE ATTAQUE Situations nécessitant l'isolation réseau d'une zone protégée entourée de réseaux de niveau de sécurité et de criticité plus faible, comme par exemple : • Entre un réseau protégé et un réseau d'un niveau de sécurité moindre ; • Entre un réseau isolé et un réseau public (internet) ; • Entre un réseau d'exploitation et un réseau de supervision.	• Protection contre les attaques par déni de service ; • Protection contre les attaques réseau de la couche transport : ◦ Couche 4 : Transport Layer - TCP syn flooding, UDP flooding (déni de service) ; ◦ Couche 3 : Network Layer - IP modification, DHCP attack, ICMP attack (usurpation, détournement de trafic) ; ◦ Couche 2 : Data Link Layer - MAC modification, MAC attack, MAC flooding (usurpation, détournement de trafic). • Protéger un réseau contre la propagation de malware utilisant des attaques de la couche transport pour prendre le contrôle de routeurs, de serveurs, de postes de travail afin de s'étendre depuis un réseau contaminé vers un réseau isolé.
3. INVISIBLE ET ISOLE MAIS TOUJOURS COMMUNIQUANT POUR POUVOIR TRAVAILLER : LA SECURITE TOUT EN RESTANT PERFORMANTS Situations nécessitant d'échanger des flux entre 2 réseaux isolés, même s'ils ont des niveaux de confiance différents, comme par exemple : • Réseau industriel (A) et réseau de gestion (B) ; • Réseau confidentiel interne tel que R&D, cellule de crise, PC-Sécurité (A) et réseau général de l'entreprise (B) ; • Réseau interne (A) et réseau d'un fournisseur ou d'un partenaire (B) ; • Réseau interne (A) vers un réseau public (web).	• Accès à des applicatifs réseau ou web (ex. donner accès à un intranet de support ou publier des mises à jour pour des clients, applications clients/serveur) ; • Communications industrielles de type ModBus, BacNet, S7, OPC-UA, ... ; • Accès à des bases de données : ◦ application métier dans le réseau A qui dialogue avec une base de données dans le réseau B ; ◦ réplication de bases de données en exploitation comme en plan de reprise d'activité ; ◦ réplication de bases de données dans une zone sécurisée ; ◦ etc. • Communications «machine to machine» ; • Services réseau de type Logs, SNMP, NTP, DHCP, DNS : ◦ centralisation des logs pour analyse ; ◦ mise à jour du temps (horloge) sur des serveurs ou des automates isoés depuis un serveur public ; ◦ monitoring des serveurs et automates isolé depuis un réseau distant ; ◦ gestion centralisée des plans d'adressage réseau ; ◦ etc.
4. TRANSFERT DE FICHIERS HAUTEMENT SECURISE Situations nécessitant des échanges de fichiers maîtrisés entre deux réseaux isolés, même s'ils ont des niveaux de confiance différents, comme par exemple : • Un réseau industriel protégé et un réseau de gestion ; • Un réseau d'exploitation et un réseau d'administration IT (sauvegardes et restaurations) ; • Un réseau isolé et Internet ; • Un réseau isolé ou protégé et le réseau d'un tiers.	• Export de journaux de logs (décharge de logs de systèmes isolés, export de dump d'erreur) ; • Récupération de statistiques de fonctionnement ; • Export de fichiers de sauvegarde et leur rechargement avec contrôle d'intégrité ; • Chargement de fichiers de mises à jour (OS, firmware, logiciel…) vers un réseau isolé ; • Import de fichiers de configuration ou d'exploitation dans un réseau isolé ; • Echange de fichiers entre tiers sans création d'interconnection réseau.

seclāb

Spécialiste de la sécurisation des interconnexions réseaux

www.seclab-security.com

contact@seclab-security.com
(+33) 04 11 93 08 59

40 avenue Théroigne de Méricourt
34000 Montpellier FRANCE