



Présentation Technique

LANDefender™

**Observatoire de la Sécurité
des Systèmes d'Information
et des Réseaux**

**OSSIR,
le 06 février 2007**

Intervenants EXCELIANCE

**Benoit DOLEZ
Willy TARREAU**

<http://www.exceliance.fr>

Société



- ❑ **EXOSEC créée en octobre 2002**
- ❑ **Spécialisée dans les métiers de la supervision, sécurité et expertise réseau**
- ❑ **10 personnes, fortes compétences Linux**
- ❑ **Clients : Conseils Généraux, mairies, banques, opérateurs, grande distribution, PME**

Constat - dès début 2004



- ❑ Plusieurs clients infectés par des vers depuis l'intérieur (portables, WAN).
⇒ **Slammer, Blaster, etc.**
- ❑ Plusieurs jours d'indisponibilité du réseau WAN et des postes utilisateurs
- ❑ Seule solution en vue : firewalls poste. Non satisfaisante pour nos clients, car onéreuse, lourde et contraignante à gérer.
⇒ **Recherche d'une solution plus adaptée**

Besoins identifiés



- ❑ **Empêcher toutes les communications non désirées entre les postes**
 - **Ne pas impacter les performances sur le réseau local**
 - **Préserver les investissements effectués sur l'infrastructure**
 - **Maîtriser les postes au plus tôt pendant la phase de connexion**

Méthodes possibles



Firewalls postes :

- **Déployer un agent sur chaque poste**
 - ⇒ risques d'effets de bords
- **Prérequis système d'exploitation**
- **Contraignants à gérer même avec une console centralisée**
- **Désactivables par l'utilisateur et par de nombreux virus/vers (MyDoom, Bagle)**
- **Limités au parc connu**
- **Coût par poste élevé**

Méthodes possibles (*suite*)



Filtrage au niveau 2 :

- **Très efficace: sécurité appliquée par les switches au niveau port ou MAC**
- **Nécessite un matériel spécifique, offrant des possibilités de filtrage avancées.**
- **Pas d'impact sur les performances**
- **Solution onéreuse**

Méthodes possibles (*suite*)



Cloisonnement au niveau 3 :

- **Efficace : un réseau IP par poste, un firewall entre tous ces réseaux**
- **Consommation de grandes plages d'adresses IP**
- **Si possible, un VLAN par poste pour éviter le contournement**
- **Mobilité réduite**
- **Gestion complexe (relations postes/IP/VLAN/ports de switches)**
- **Le firewall est un point d'engorgement**
 - ⇒ **Difficulté à conserver un bon niveau de performance**
 - ⇒ **Non scalable**

Notre proposition



- ❑ **Non intrusive : aucun changement d'équipement ni d'adressage nécessaire, sans agent.**
- ❑ **Isoler les postes au niveau 3 par l'affectation d'une adresse IP associée à un masque en /32**
 - ⇒ **Les postes ne voient plus personne**
- ❑ **Toutes les communications s'effectuent alors à travers une gateway sur le réseau local**
- ❑ **Cette gateway ne doit pas permettre le rebond non contrôlé vers le réseau local**
- ❑ **Permettre aux postes de conserver un accès local à certaines ressources du réseau**
 - ⇒ **Faible impact sur les performances**
- ❑ **Inconvénient : pas de contrôle des flux de niveau 2**

Principe d'adressage en /32



□ Windows : ipconfig /all

```
c:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrateur>ipconfig /all

Configuration IP de Windows

    Nom de l'hôte . . . . . : winxp-01
    Suffixe DNS principal . . . . . :
    Type de noud . . . . . : Hybride
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non

Carte Ethernet Réseau local:

    Suffixe DNS propre à la connexion : mydomain.local
    Description . . . . . : VMware Accelerated AMD PCNet Adapter
#2
    Adresse physique . . . . . : 00-0C-29-9C-3B-EE
    DHCP activé . . . . . : Oui
    Configuration automatique activée . . . . . : Oui
    Adresse IP . . . . . : 192.168.2.139
    Masque de sous-réseau . . . . . : 255.255.255.255
    Passerelle par défaut . . . . . : 192.168.2.1
    Serveur DHCP . . . . . : 192.168.2.250
    Bail obtenu . . . . . : lundi 27 février 2006 12:28:31
    Bail expirant . . . . . : lundi 27 février 2006 13:28:31

C:\Documents and Settings\Administrateur>
```

Principe d'adressage en /32 (*suite*)



- ❑ Accès à la gateway défini par une route de host sur l'interface locale
- ❑ Filtrage par routage ou absence de route
- ❑ Affinage du filtrage possible par mise en place d'un firewall sur la gateway

Limites de l'adressage en /32



- ❑ Interdit les broadcasts
- ❑ Compatibilité des OS
- ❑ Sans outil, lourd à déployer
- ❑ Nécessite le respect de la configuration par le poste

Configuration des postes en /32



- ❑ **Configuration manuelle**
 - **Fastidieuse, limitée au parc connu**
 - **Sans outil, compatible avec peu d'équipements**
- ❑ **Configuration automatique via DHCP**
 - **Simplicité de déploiement**
 - **Distribution de configurations de routage propres à chaque poste**
 - **Annonce par le serveur d'une configuration spécifique aux options supportées par le client DHCP (Windows, PXE, Linux, MacOS-X, ...)**
 - **Facilité de mise à jour des configurations**
 - **Prise en compte des postes inconnus**

Config des postes en /32 (*suite*)



DHCP : les limites

- **Limité aux postes configurés pour faire du DHCP.**
- **Pas de support pour les alias IP**
- **Configuration complexe, difficile à écrire**
- **Gérer les cas d'incompatibilité des OS avec le /32**
 - ⇒ **Cas par défaut**
 - ⇒ **Matrice de compatibilité des clients avec différentes options DHCP liées au routage (options 33, 121, 249), support ou non du netmask en /32**
- **Limite du protocole à 31 routes statiques par option**

Rôle de la gateway



- ❑ Tous les flux pour lesquels il n'existe aucune route statique locale lui sont envoyés
 - ⇒ **Besoin de filtrage**
- ❑ Son positionnement est adapté à un filtrage fin
- ❑ A remplacer de préférence par un firewall

Firewall en guise de gateway



- ❑ Nécessité de supporter le one-leg routing
- ❑ Nécessité de supporter les flux asymétriques
- ❑ Configuration difficile à écrire car le filtrage est précis au niveau du poste
 - ⇒ **Centralisation**
- ❑ Besoin de filtrer sur des MAC sources à cause du DHCP
- ! **Attention aux performances**

Traitement des équipements non configurables



Équipements non configurables :

- **Équipements ne supportant ni la configuration manuelle en /32 ni le DHCP en /32**
 - **Équipements de l'infrastructure (switchs, ...)**
 - **Visiteurs indésirables**
 - **Pirates**
- ⇒ **Ces équipements se comportent normalement et utilisent l'ARP pour joindre leurs voisins. A ce titre, leurs échanges sont détectables sur l'ensemble du LAN.**

Traitement des équipements non configurables (*suite*)



Cas non traités :

- **Spoofting IP et MAC pour obtenir les droits d'un équipement autorisé**
 - ⇒ Détectable uniquement par les switches
- **Injection en unicast d'entrée ARP dans un poste en vue de spoofer un serveur autorisé pour ce poste**
- ⇒ **Ces cas correspondent à des attaques intelligentes et ciblées qui ne peuvent être couverts sans coupure physique**

BILAN



- ❑ **Besoin d'un serveur DHCP évolué**
- ❑ **Besoin d'un firewall avancé**
- ❑ **Besoin d'un détecteur/analyseur d'ARP**
- ❑ **Besoin d'interfaces de configuration adaptées à un grand nombre de nœuds pour l'ensemble de ces outils**

Les choix retenus



Le serveur DHCP : ISC DHCP

- **Serveur réputé : existe depuis 1996, utilisé chez les opérateurs**
- **Très riche en termes de fonctionnalités**
- **Flexible et robuste : supporte facilement des milliers de noeuds**
- **Licence libre ISC**

- **Manque le critère de test sur les options demandées par le client, nécessaire au traitement des configurations par type de client, et la possibilité d'exécution d'un programme externe sur changement de bail**

Les choix retenus *(suite)*



Le Firewall : Netfilter

- ✓ **Supporte le one-leg routing**
- ✓ **Supporte le filtrage asymétrique**
- ✓ **Supporte le filtrage par adresse MAC**
- ✓ **Performant**
- ✓ **Licence libre GPL**
- **Mises à jour de configuration atomiques avec iptables-restore**
- **Architecture flexible grâce aux branchements laissant le soin de l'optimisation à l'application de configuration**
- **Logging avancé avec ULOGD**
- **Supporte des modules d'extensions (PSD, ipset, ...)**

Les choix retenus *(suite)*



La surveillance ARP : arpalert

- **L'auteur fait partie de l'équipe**
- ✓ **Détection de nouvelles adresses MAC**
- ✓ **Détection de spoofing**
- ✓ **Détection de requêtes ARP non autorisées**
- ✓ **Auto-protection contre les attaques**
- ✓ **Licence libre GPL**
- **Détection des floods**
- **Détection des scans**
- **Exécution d'une commande externe sur événement**

Synthèse des choix retenus



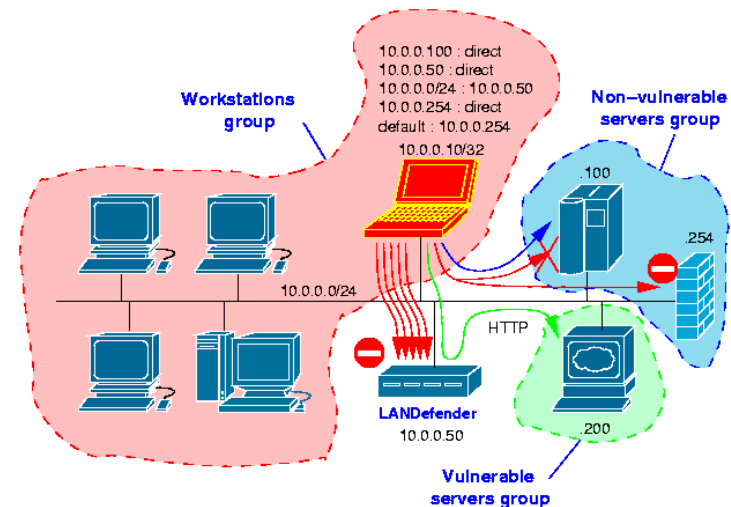
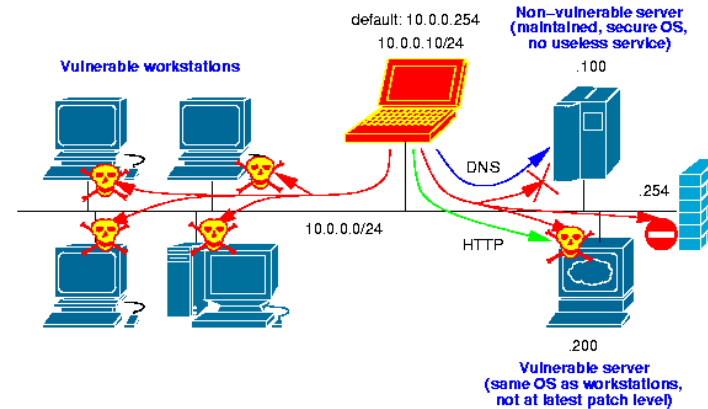
- ❑ La combinaison de Netfilter, ISC DHCP et arpalert permet d'obtenir un bon niveau de contrôle du réseau local
 - ❑ Certains composants ont subi des modifications
 - ❑ Reste à résoudre le problème d'écriture des configurations
 - ❑ Traiter l'information riche rapportée par ces 3 composants
- ⇒ **Cette intégration délicate justifie la création d'une appliance dédiée à la protection du réseau local : le LANDefender**

Intégration au sein du réseau



- ❑ Le LANDefender s'intègre sur le réseau local comme un firewall entre les postes de travail
- ❑ Aucune modification d'architecture n'est nécessaire garantissant une intégration sans risque

Avant
Après



Le LANDefender actuel (version 1.7)



- ❑ **Les composants**
 - **Plates-formes sélectionnées**
 - **Logiciels libres et contributions**
 - **Logiciels propriétaires**
- ❑ **Fonctionnement**

Les composants



La plate-forme

- **Base x86 au format "network appliance"**
- **Développements et tests possibles sous VMWare**
- **Systeme compact : Formilux**
- **Packagé façon firmware (~12 Mo)**
- **2 images sur CompactFlash en read-only**
- **Boot-loader avancé commun à toutes nos appliances**

Les composants *(suite)*



Formilux

- ❑ Distribution Linux « maison » robuste orientée systèmes embarqués (always-on)
- ❑ Système de fichiers en lecture-seule
- ❑ Fichier de configuration unique
- ❑ Gestion avancée du réseau (bonding, VRRP, VLAN)
- ❑ Monitoring intégré des services
- ❑ Installation du strict nécessaire : pas de fichiers inutiles

Les composants *(suite)*



Logiciels libres

- **Linux, Netfilter, isc-dhcp, arpalert, ulogd, psd, arpoison, sqlite3, ...**
- **Licences : GPL, BSD, ISC, ...**

Nos contributions

- **DHCP : critère de test**
- **ULOGD : corrélation**
- **ipset : correctifs, ...**
- **arpalert et formilux : du temps (beaucoup :-)**
- **Keepalived : correctifs, tracking par script**

Les composants *(suite)*



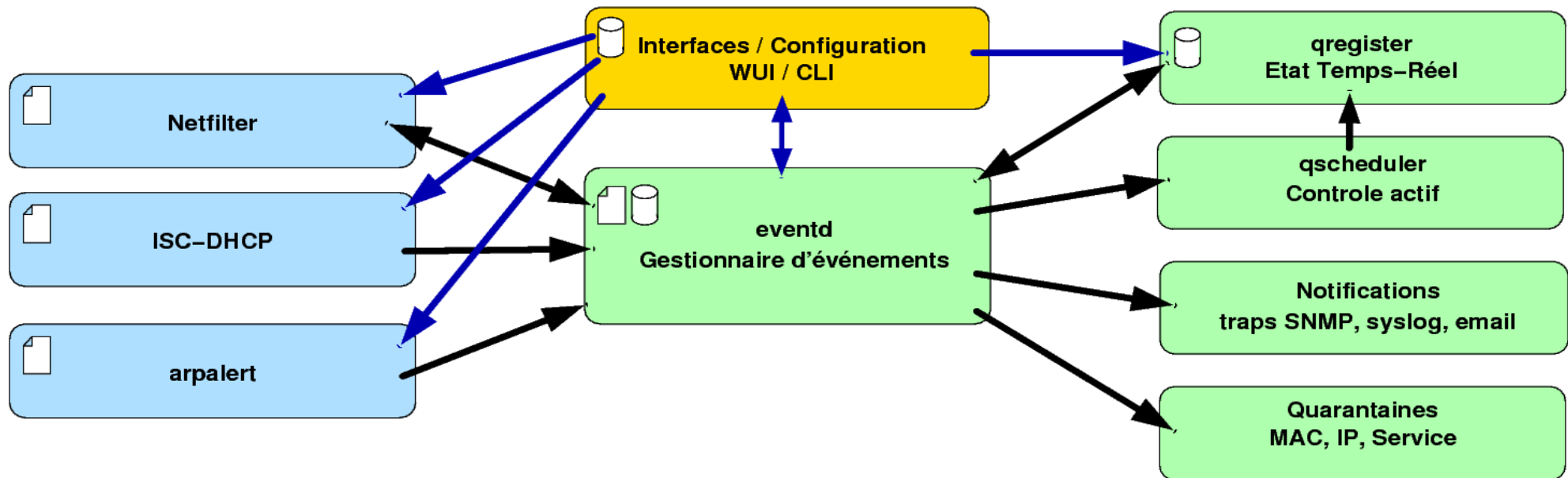
Logiciels propriétaires

- **Gestionnaire d'événements : eventd**
- **Qualification des noeuds : qsched, qregister**
- **Générateurs de configuration : dhcp, netfilter, arpalert**
- **Interface de configuration et reporting**

Fonctionnement



□ schéma d'agencement des composants



Configuration du DHCP



- ❑ Définition du routage par poste
- ❑ Gestion des modes de protection (filtré ou non)
- ❑ Optimisation par factorisation des règles communes
- ❑ Prise en compte des options spécifiques à chaque client (ex: options 249 et 121)
- ❑ Prémption du type de client sur les options supportées (ex: Windows 98 supporte l'option 33 sans la demander)

Configuration du firewall

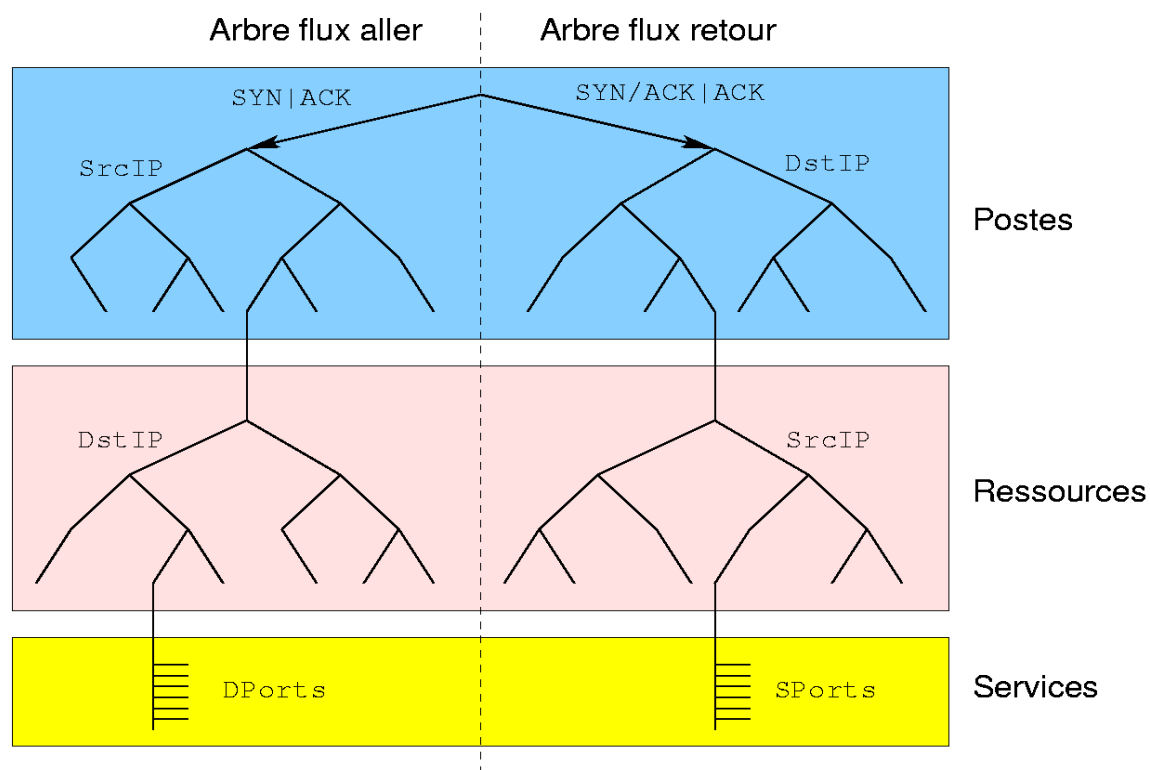


- ❑ Validation bidirectionnelle de chaque flux
- ❑ Anti-spoofing par vérification IP/MAC (synchronisation avec le DHCP)
- ❑ Utilisation des chaînes pour traiter le grand nombre de nœuds
- ❑ Génération d'un arbre de chaînes pour optimiser la recherche d'un nœud
- ❑ Génération d'un arbre de chaînes pour optimiser les autorisations
- ❑ Règles par défaut

Configuration du firewall (*suite*)



□ Schéma de l'arbre IP



Gestion des autorisations



- ❑ Liste d'autorisations explicites
- ❑ Aucune relation d'ordre entre les règles
- ❑ La source et la destination sont les identifiants d'objets connus et non de simples adresses IP
- ❑ Les autorisations peuvent être de 3 types :
 - **Direct (accès à la ressource par routage local)**
 - **Indirect Full-IP (idem via le LANDefender)**
 - **Indirect après filtrage par service**

Gestion des autorisations (*suite*)



❑ Exemple de matrice d'autorisations

Groupes Ressources	Registered	Guest	Engineering	Finance	HR	IT	Management	Manufacturing	Marketing	Sales
SVN	HTTP									
Wiki	<input type="checkbox"/> DIRECT <input checked="" type="checkbox"/> ALL-TCP <input checked="" type="checkbox"/> ALL-UDP <input checked="" type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP
azote	ALL-TCP, ALL...	ALL-TCP, ALL...								
groupware	<input type="checkbox"/> DIRECT <input checked="" type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input checked="" type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP	<input type="checkbox"/> DIRECT <input type="checkbox"/> HTTP
silicium	<input checked="" type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP	<input type="checkbox"/> DIRECT <input type="checkbox"/> ALL-TCP <input type="checkbox"/> ALL-UDP <input type="checkbox"/> ALL-ICMP

Notifications et quarantaine



Notifications :

Chaque événement peut donner lieu à une notification et/ou une mise en quarantaine.

- **Événements :** `new_mac`, `scan_host`, `blacklisted_host`, `unauthorized_access`, `error_proto`, `unknown_host`, `scan_service`, `scan_host`, `scan_net`, `mac_error`, `flood`, `ip_change`
- **Notifications :** traps SNMP, syslog, email
- **Quarantaines**
 - **ARP :** arpoison
 - **MAC :** Netfilter
 - **IP :** Netfilter
 - **Service :** Netfilter (contre les vers)

Reporting



- ❑ **Des informations sont collectées à intervalles réguliers sur les postes pour obtenir une représentation temps-réel du réseau :**
 - **Disponibilité, adresse IP, OS,**
 - **Nom et utilisateur NetBIOS,**
 - ⇒ **Historique de présence des nœuds sur le réseau à l'heure près**
- ❑ **Stockage et restitution des événements**
- ❑ **Historisation d'indicateurs élémentaires : nombre de nœuds, trafic, baux DHCP, comptabilisation d'événements**

Contrôle d'activité



- ❑ L'expérience montre que les clients se contentent seulement d'une partie des fonctions de sécurité (ex: DHCP, ARP).
 - ❑ Le firewall leur sert plus souvent à détecter des accès à certains services qu'à appliquer une politique de sécurité, même s'ils sont conscients qu'ils y viendront.
- ⇒ **Ils cherchent avant tout à exploiter la simplicité de mise en œuvre du LANDefender pour mieux connaître l'activité du réseau.**

Contrôle d'activité *(suite)*



Fonctions recherchées

- **Identification et localisation des postes,**
 - **Présence des utilisateurs sur le réseau,**
 - **Disponibilité des équipements,**
 - **Notification/reporting sur les accès interdits,**
 - **Journalisation des événements.**
- ⇒ **Savoir** qui **fait** quoi, quand, où.

Les évolutions en cours



- ❑ **Monitoring étendu : détection et qualification plus fine basée sur l'analyse du trafic (NetBIOS, CDP, ...),**
- ❑ **Support du multi-LAN : déployer le LANDefender sur plusieurs VLAN sans influencer le routage entre les VLANs**
- ❑ **Détection et localisation des nœuds à partir des FDB des switches**
- ❑ **Quarantaine niveau 2 en agissant sur les switches**
- ❑ **Framework commun avec Aloha, SightFlow, ...**

Merci de votre attention

