Grid of security: a new approach of the network security

Olivier Flauzac, Florent Nolot, Cyril Rabat, Luiz Angelo Steffenel

Grid of security: a new approach of the network security

Olivier FLAUZAC, Florent NOLOT, Cyril RABAT, Luiz-Angelo STEFFENEL
CReSTIC - SysCom Team
University of Reims Champagne-Ardenne
BP 1039, 51687 Reims Cedex 2, FRANCE
{olivier.flauzac, florent.nolot, cyril.rabat, luiz-angelo.steffenel}@univ-reims.fr

***Abstract*—Network security is in a daily evolving domain. Every day, new attacks, virus or intrusion techniques are released. Hence, network devices, enterprise servers or personal computers are potential targets of these attacks. Current security solutions like firewalls, intrusion detection systems (IDS) and virtual private networks (VPN) are centralized solutions which rely mostly on the analyze of inbound network connections. This approach notably forgets the effects of a rogue station, whose communications cannot be easily controlled unless the administrators establish a global authentication policy using methods like 802.1x to control all network communications among each device. To the best of our knowledge, a distributed and easily manageable solution for the global security of an enterprise network does not exist. In this paper, we present a new approach to deploy a distributed security solution where communication between each device can be control in a collaborative manner. Indeed, each device has its own security rules, who can be shared and improved through exchanges with others devices. With this new approach, called *grid of security*, a community of devices ensures that a device is trustworthy and that communications between devices progress in respect of the control of the system policies. To support this approach, we present a new communication model that helps structuring the distribution of security services among the devices. Like this, we can secure both ad-hoc, local-area or enterprise networks in a decentralized manner, preventing the risk of a security breach in the case of a failure.**

***Keywords*-security architecture, grid design, distributed communication**

I. Introduction

The definition and deployment of security policies is a domain which is widely studied in the last years. Most solutions, like firewalls, intrusion detection systems (IDS), intrusion prevention systems and virtual private networks (VPN) are all centralized, being more adapted for traditional cabled networks than for wireless networks. Today, wireless devices are important elements on the access-layer network, and solutions to secure communications between devices require the deployment of complex solutions like wireless controllers, 802.1x authentication or virtual private network tunnels. While these solutions ensure that communications cannot be intercepted or modified, nothing prevents a virus, Trojan or malicious user to launch an attack on the network, from the inside.

In this paper, we first study existing solutions, proposing a new approach to ensure a fast and decentralized enforcement of the network security: *the grid of security*. This new approach can be described as the addition of each device security policies, creating a global security behavior. We define a community like a set of devices which share the same global policy. With this collaborative approach, devices in the community exchanges their local policy rules among each other, even if the final decision to accept or deny a new rule depends on the device's user. With this new approach, a user who wants to open a network service such as a file transfer service (FTP) will create a new local policy rule. This new rule will be exchange with other device on the community and other users must approve or refuse this new service. With this approach, we can quickly create a secure network without any centralized solution. While each device is independent of any centralized solution, a device may benefit from the mutual security enforcement from a community. In the same principle, different communities may arise as a result of different security levels authorized by the users.

Which differs our approach from other trustiness and recommendation-based approaches is that we structure our mechanisms around a middleware especially tailored for grid computing and peer to peer communication model. A grid-like approach offers the advantage to rationalize every resources of each device, like storage, computing resource or data analysis. With a peer to peer communication model, devices communicate without relying on a central server, improving therefore the system fault tolerance.

In this paper, we first present in Section II actual used solution to ensure security of a network. From this study, we observe that each solution need a complex centralized administration device or service to manage global security. But now, with the mobility of each user, this solution is not appropriate. From these observations, we propose a new approach of information system based on grid in Section III and our concept of grid of security in Section IV to offer a new distributed security services. Finally, in Section V, we conclude this paper and give some open tracks from this work.

II. The Security Problem

Today, the Internet is far from being a secure environment. The continuous growth of security risks (intrusions, virus,

spywares, information stealing) forces enterprises and network administrators to expend a considerable amount of time and money to improve security aspects from their networks, usually through the association of multiple techniques and tools. Despite the fact that defining and deploying security policies if a study field that rapidly advanced in the last years, most of the proposed solutions are still based on centralized servers.

In our approach, we try to better represent the constraints from the real world by starting our models with a typical enterprise network, connected to the Internet. In this model, all network devices connected to the enterprise network constitute what we call a "confidence zone". By default, the confidence zone is delimited by the equipments directly connected to the Internet, i.e. those devices with a public IPv4 interface. Formally, a confidence zone includes all communicating devices in a network where the global security is under mutual control. Therefore, a confidence zone can be extended across a WAN link or reduced to a few devices if the devices find a common agreement on the security policies.

A. *Security: study cases on today networks*

In this section, we present three scenarios that represent typical situations where secure communications are required: (*i*) protection against intrusions, (*ii*) connection to the confidence zone from abroad and (*iii*) communication security inside the confidence zone. In all these cases we observe that current networks rely on centralized services. Indeed, inbound and outbound communications are usually filtered through firewalls, intrusion detection systems and VPN concentrators. Some companies like Cisco Systems and CheckPoint reinforce this centralized organization by integrating all security services in a single box. We believe however that reinforcing the central role of a security box only increases the risks in the case of failures or attacks.

1) Intrusion Detection Systems: This scenario is typically represented by networks hidden behind a firewall. Here, only authorized data flows may reach the internal network. Authorization policies include source and destination addresses, ports and even the protocol types. Usually at the enterprise network entry point (cf. Figure 1), firewalls are now found also installed in each user's computer.

According to their specifications and strategic location in the enterprise network, firewalls (personal or not) are good tools to block direct attacks coming from the outside of the confidence zone. At the other hand, data flows originated from the inside network are seldom analyzed by the firewalls. Indeed, while a network administrator is able to control the connections that traverse the enterprise entry points, it has no control over alternative access points opened by an user, as for example a laptop computer connected to the Internet through the user's cellular phone. To ensure that all devices in the internal zone share the same security

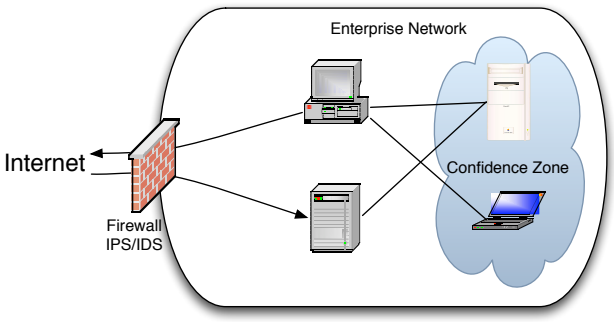

Figure 1. A typical Firewalled network

policies, it is important to implement an additional control over the internal exchanges. Due to the complexity of this task, the security policies coordination must be implemented through mechanisms that are transparent to the user.

2) Connection to a secured zone: A data flow authorized by a firewall allows a distant machine to exchange data with the secured zone but doesn't guarantee the confidentiality of the data that cross the Internet. Therefore, some additional properties must be ensured when connecting to a confidence zone: encryption, authentication and data integrity. These properties are provided, for example, by VPN "tunnels" connected to the enterprise network (Figure 2).

Indeed, some protocols individually provide some of these properties (SSL, SSH) but the Virtual Private Networks - VPN - have the advantage to integrate these properties while securing the totality of the data flows that are tunneled. Furthermore, VPNs create a virtual extension of the local area network, preserving the internal security appliances defined on the confidence zone and given access to internal services like printer and mail servers. The problem, however, is that nothing prevents harming codes such as virus to flow through the VPN, compromising the internal security.

Also, accessing a VPN requires a centralized server (usually called a VPN server or VPN concentrator). As all the traffic must be relayed by this central server, the available bandwidth is limited. Some companies integrate all functionalities from firewalls, IPS and VPNs in a single network devices, which has the side-effect of centralizing even more the network and limit the bandwidth. For instance, a Cisco ASA 5550 firewall can handle only 425 Mbps if both VPN and firewall are active, against 1.2 Gbps in a firewall mode only[1].

3) Establishing a confidence zone: To allow a machine to access a confidence zone is always a risky decision as this machine may be infected by virus or malwares. Similarly, some applications may not be adapted to the established security policies (instant messaging or P2P, for example).

[1]http://www.cisco.com/en/US/products/ps6120/prod_models_comparison.html

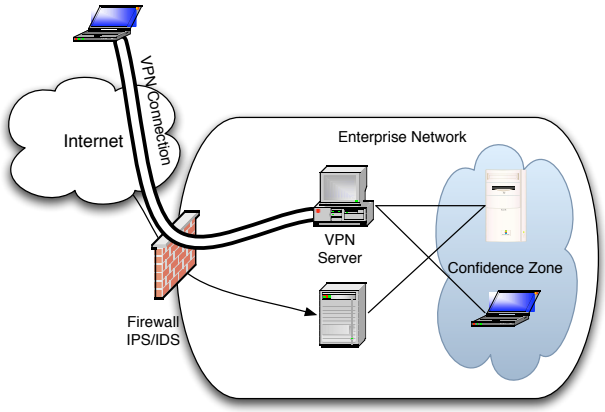

Figure 2. VPN usage in current networks

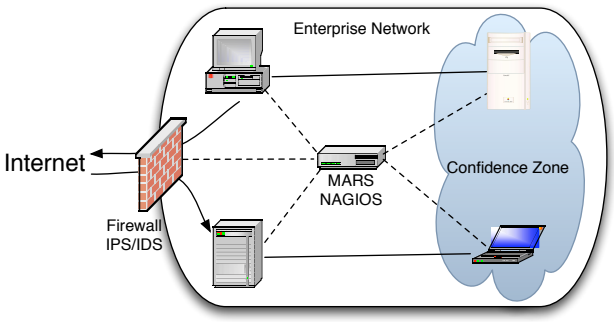

Figure 3. Monitoring a confidence zone

To reduce the risk and verify if a device complies with the security policies, some companies like Cisco Systems, Microsoft or Nortel Networks propose the use of *Network Access Control* - NAC - mechanisms. Basically, a NAC associates user authentication and verification of the user's machine before allowing it to connect to the network. Among the elements a NAC may verify (or impose) there are:

- anti-virus status (activation, last update);
- OS security updates;
- public key certificates;
- firewall status and current rules;
- authorized applications;
- permission to activate WiFi or Bluetooth connections;
- etc.

Hence, Cisco Systems proposes a Network Admission Control Appliance (NAC Appliance)[2]. In addition to the previous controls, the NAC Appliance analyzes the behavior of the network devices, looking for abnormal patterns. For example, if the NAC Appliance detects an IP phone establishing a *telnet* connection with a computer instead of exchanging informations with the call manager, an alert will be thrown. Among the possible reactions, the NAC Appliance can alert the network administrator, the final user or even automatically isolate the incident zone, placing it in quarantine. The inconvenient of this approach relies on the fact that all connections (data, voice and video) must pass through the NAC Appliance, with a potential performance bottleneck.

In the same philosophy we found the network supervising systems (Figure 3). With functionalities going from the simple display of network statistics to a proactive network management (such as the Intrusion Detection Systems), these services are useful tools to identify the weaknesses in a network. As before, Cisco Systems proposes a solution called MARS[3] where informations are exchanged among MARS agents, improving the behavioral analysis of the network.

All these approach are centralized solution. We always have a centralized service who analyze all other devices of the network. In our solution, NAC functionalities can be distributed in many device of the network in order to avoid overload of only one device and to be fault tolerant.

B. A path to IPv6 secure network

The gradual deployment of IPv6 represents a milestone on the security community. Indeed, IPv6 has a much larger address space (2^{128} for IPv6 against 2^{32} for IPv4) that allows every communicating device to hold a public IP address. While IPv4 still resists in many networks, some estimations point that the entire IPv4 address space will be depleted around 2011[4]. For the matter of example, IPv6 allows roughly $3,4 \times 10^{38}$ addresses (the rest of the address space is reserved for now), which represents more than 6×10^{19} IP address per cm^2 on planet Earth. With this abundance of public IPv6 addresses, the use of private addresses inside a network will disappear.

However, once each network device (PC, cellular telephone, sensor and so on) uses a public IP address, it becomes more vulnerable to attacks. This is especially true with Mobile IPv6 [1], [2], as a mobile device will be able to roam from network to network keeping the connections previously opened. Different routers will exchange connection informations in order to migrate transparently the user's connections. This new kind of service may be explored to allow an attacker to enter the enterprise network by piggybacking on the previously opened connections from the mobile device. Some works [3], [4] exist to secure Mobile IPv6 with IPSec but a specific security functionality needs to be deployed.

C. Secure ad-hoc networks

An ad-hoc network is a network without fixed infrastructure in which each device can communicate with its

[2]http://www.cisco.com/go/nac

[3]http://www.cisco.com/go/mars

[4]http://penrose.uk6x.com/

neighbors. It differs from current enterprise solutions which were developed for networks with fixed infrastructure, even in a wireless environment. The security is done with secure communication link between the wireless client and the access point. For instance, the access to the access point is a major control point that cannot be neglected. Actual researches on security and ad-hoc networks are based on cryptographic solutions [5], [6], [7]. These solutions are enough to ensure confidentiality and data integrity but are not design to deploy the same security policies on the network. Other works [8] focus on data exchange to secure ad-hoc network but these solutions are similar to fixed infrastructure solutions.

In our approach, secure communication between two devices can be implemented together with the deployment of security policies on each device of the network. With our solution, each device has a security agent who is able to communicate with all other agents on the network, sharing security policies.

III. The grids - General presentation

The grids are one of the solutions to manage and share available resources on a network. Two types of grids are distinguished: grid computing and data grids. In grid computing solutions (like SETI@home [9], BOINC [10], XtremWEB [11], Diet [12], Globus[13], and CONFIIT [14], [15], [16]), resources are associated to computing (processor, memory, ...). In data grid (OceanStore [17], Freenet [18]), resources are associated to data storage. Whatever the grid type, it is necessary to develop a middleware for management of the different resources: connectivity, resources monitoring, tasks scheduling in computing grid and data replication (or distribution) management in data grids. Today, most of grids are based on either centralized or hierarchical architecture. In both cases, they require several management tasks and each device must be specialize.

In parallel to this grid concept, peer-to-peer model have been developed. A P2P communication model uses fully decentralized architectures and is easily scalable. Moreover, it can tolerate dynamic networks like wireless or ad-hoc networks. At the end, the main objective of peer-to-peer systems is allow communication between each device without any additional requirement (location server, proxy, etc.).

However, when we design a middleware or grid application, we must use a theoretical model. Like in a grid, each device have a specific function and we can have many device in the network (switch, firewall, personal computer, server, ...), the model must describe each function and each device in order to correctly study and evaluate our grid application. From this theoretical model and study, we can try to find solution to each problem.

To be most effective, a model must take into account the whole system. The grid model can be applied in an environment which is not necessarily dedicated. In this case, applications or mechanisms outside the grid can affect the overall effectiveness of the middleware or grid application. The model must also take into account the physical hardware if we want to make appropriate management mechanisms. However, the models proposed in the literature take only into account a sub-part of the overall system. That is why we proposed a new theoretical model.

In [19], authors proposed a method focusing on the description of network components. Their model allows to describe both protocols used and the network hardware such as routers or switches. Thus, the physical network of the grid is represented as a graph where each node represents a network device or a particular type of network (*(*Ethernet), *(*Myrinet) ...). The interest of a such model, close to the physical network, is to highlight the problems of network congestion or delay in transferring data.

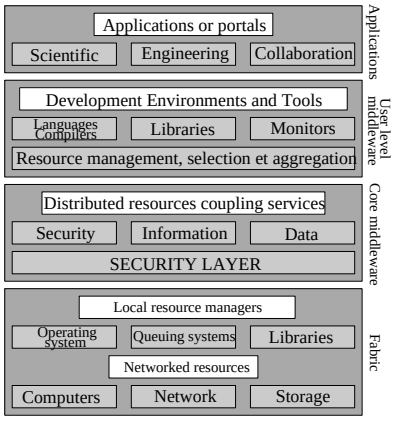

Figure 4. Grid model proposed in [20].

In [20], a new approach is proposed, based on the concept of a factory. Components and architecture of the grid are organized into layers as shown in Figure 4. The lowest layer is close to the physical network and represents the physical resources of the grid. These resources are accessible via the local resource managers. The second layer represents the security and how to access the resources, aiming to ensure the security of connections. The third layer is the middleware that serves as an interface between the application and the access to resources. The last layer represents the application itself, in which operates the middleware. Contrary to the previous model, it does not highlight issues close to the physical network, but focuses on the problems of access to resources in terms of middleware and its services.

Another commonly used model is based on *Globus* from [21]. It focuses on the material forming the grid as shown in Figure 5. Such model is composed by 4 layers. The first layer represents the physical network, i.e. physical connection and routing equipment. Over this layer, we find the resources of the grid: the computing resources, storage or applications shared. The third layer relates to components and middle-

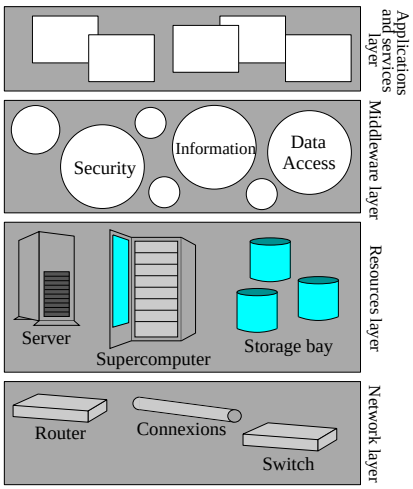

Figure 5. Grid model proposed in [21].

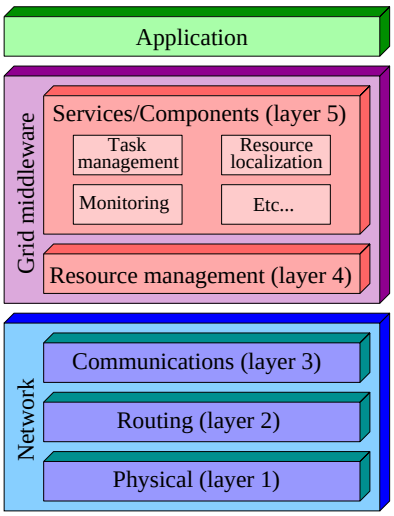

Figure 6. Theoretical model for grid applications designing

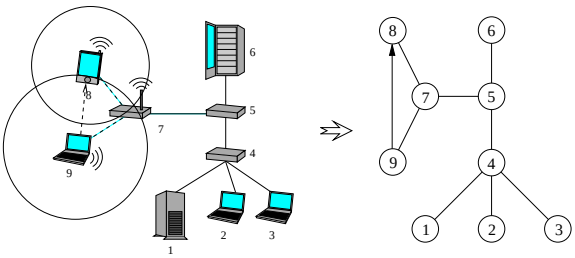

Figure 7. Example of a network representation in Layer 1.

ware services that communicate with the resources. And the last layer is the application that uses the services provided by the middleware.

As all of these previous grid models do not consider all the resources of a network and a grid application, another model was proposed in [22]. In this new theoretical model, physical devices, communication link and each resource of the application are represented. This model is the most adapted to design the grid of security in which physical devices, communication links and their policies have a main role. It is structured in five independent layers: physical layer, routing layer, communication layer, resource manager and finally all the components and middleware grid services.

A. Grid design

In [22], we have proposed a 5 layers model for grid or peer-to-peer applications design. This model is represented in Figure 6. It is used to model the network of a grid that interacts independently of the grid middleware. It also models the components of the grid middleware and interactions between them.

Layer 1 - Physical network layer. The first layer concerns the physical network. The network is represented by a graph $G_1 = (V_1, E_1)$. V_1 is the network nodes set. A node can be an *active* component (like desktop computers, servers, ...), or a *passive* component (like routers, switches, ...). E_1 is the set of links that interconnect network nodes. We distinguish two kinds of links: wired and wireless connection. The wired connections are naturally undirected. But with the wireless connections, we have to take care of the different emission ranges of the network nodes. If a node has a higher range than another one, this induces a directed link in E_1.

Figure 7 shows an example of a network (left figure) represented in the first layer of the model (right figure). The nodes (1 to 7) are connected with wired connections: the links in the corresponding graph are undirected. For the two wireless nodes, we can remark that Node 9 has a higher range that Node 8 (ranges are represented by a circle on the figure). We obtain a directed link in E_1.

Layer 2 - Routing layer. Over the physical network, a routing protocol builds and maintains paths between the nodes of the network. Two entities can communicate even if they are not directly physically connected. The paths construction takes into account the several security policies deployed over subnetworks (firewalls). In the same way, some protocols (like *NAT*) can limit the access to nodes. For these reasons, directed communication links are considered. In Layer 2, the network is represented by the graph $G_2 = (V_2, E_2)$, where $V_2 = V_1$ and E_2 is the set of paths between nodes of V_2.

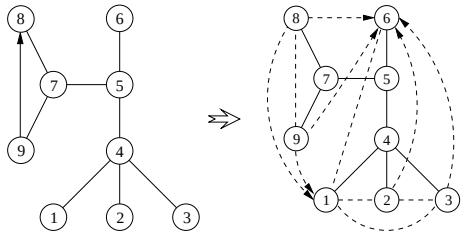

Figure 8. Example of a network representation in Layer 2.

Figure 8 is based on the example of Figure 7 and shows the representation of the network in Layer 2. To simplify, the paths that start or end from passive components (Nodes 4, 5, and 7) are not displayed. We remark new links that represent the paths computed by the routing protocol. For the wireless entities (Nodes 8 and 9), we remark that the directed link $(9, 8)$ has been deleted: Node 8 can contact Node 9 through Node 7.

Layer 3 - Communication Layer. Over the paths built from the lower layer, it is possible to send data between two distant nodes that are not physically connected. The network is represented as a graph $G_3 = G_2$. In this layer, we can have the message send and receive capabilities thanks to a given protocol or a protocol stack. Several mechanisms can be proposed to manage communication problems (loss or duplication of messages, data corruption). An acknowledgment mechanism can ensure that a sent message has been received. If a message is lost, it is sent again. Another mechanism can ensure the message integrity.

Layer 4 - Resource management. The two higher layers focus on the grid middleware. Layer 4 is the resources management layer that can be viewed as an interface between the components and the services of the grid and the lower layers. In this layer, we distinguish two kinds of nodes. The first ones, called the *active nodes*, are within the grid. These nodes share their own resources or use the grid resources. The others ones, the *passive nodes* are outside the grid such as routers or switches.

In this layer, the grid is represented as a graph $G_4 = (V_4, E_4)$ where V_4 is the set of active nodes and E_4 is the set of communication links between active nodes. Passive nodes are not represented in the graph (*cf* Figure 9) but they can influence the efficiency of the grid application (due to network overloads).

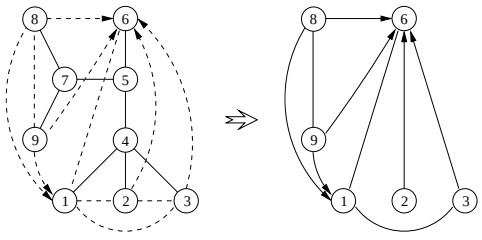

Figure 9. Example of grid representation in Layer 4.

Layer 5 - Grid components and services layer. The last layer concerns the grid components and services including the tasks management and the resources monitoring service. The deployed components depend on the middleware: if it concerns the file sharing, it must have a component to transfer the files and maybe a component to manage access rights and queues for users.

The grid is represented by the graph $G_5 = (V_5, E_5)$ where $V_5 = V_4$ and E_5 is the set of communication links proposed by the topology layer. E_5 is not equal to E_4: it depends on the protocol that manages the grid topology or the peer-to-peer overlay network.

IV. From grid to network security architecture

From the previous observations, we proposed a new architecture and a new security middleware in which each device or user is an actor of the global security of the network. Thus, each user can manage its local security but also, through exchanges with its neighbor in his community, manage the global security policies. To prevent malicious users to attack the network, each exchange must be secure, controlled and validated by authorized users or authorized devices. An authorized user is a user who was already in the community and has exchanged some policy rules with another authorized neighbor. An authorized device is either a computer, a server or a network device who is considered to be secure and authenticated.

To form a "confidence zone", exchanges inside the network must be secured to prevent unauthorized actions that can compromise the security of the community. Our work, however, goes beyond the proposal of a simple security mechanism, as we can have with a wireless LAN controller or network access controller. Our solution considers all the aspects in order to design a new security architecture and a new middleware to secure the network. A computer or a device, with our security middleware, can be specialized to control some particular functionalities. For instance, a computer can administrate the anti-virus database, another can administrate authentication and another some firewall rules. From the specification of the computer, we can choose which security function the computer must offer. In an ad-hoc environment, communication can be secured using cryptographic methods but this approach is not enough for a complex enterprise network where only a part of the traffic flows through a VPN or cryptographic tunnel. Similarly, an extensive control on the access points of the network through firewalls only works on structured networks, not ad-hoc. In a ad-hoc network, nothing prevents an user to to share its Internet access or to open a web or FTP service.

In our security architecture, devices will be mutually monitored. If a device become "dangerous" because a virus or a trojan is detected, it will be blocked and removed from the community (or confidence zone), as illustrated in Figure 10. Furthermore, a new user in a mobile environment must be authorized to enter the community. Nowadays, similar procedures can be implemented through the use of 802.1x authentication or VPNs but the configuration complexity and the technical knowledge required is high. In our solution, a new device can be added without any human manipulation, making the security of our network self-managed.

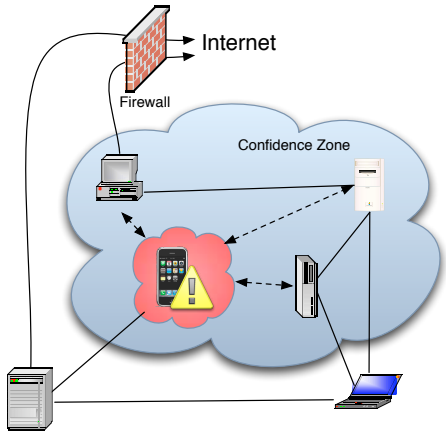

Figure 10. Grid of security example

A. Problems to solve

To achieve our objectives, we need to answer several questions: how to distribute the security functions on peers, how to exchange data, which communication protocols will be used between peer, how to distinguish different types of traffic. Also, we must define how to secure voice traffic, how to block communications from a peer, ... We will try to answer some of these questions in the next parts.

1) Distribute security resource on peers: From our middleware (in Layer 4), all data exchanged among peers in the same community are consider to be safe, so we don't need to verify each exchanged data. However, if an user wants to create a new community, he needs to control the traffic between this new community and his own community, which implies that new services must be installed on this peer. For instance, a similar approach is used on wireless environment with a wireless LAN controller, where the protocols LWAPP or CAPWAP are used. Data exchanges between wireless client and access point can be controlled either by the access point or the controller. With our middleware, the procedure is similar. A peer A can exchange informations with another peer B in order to use a security service that A does not have but B has. From the technical specification of a peer, a user can define which service he wants and he can deploy it on his peer.

2) Controls of data exchanged in a community: Inside a community, if a peer receives too many messages during a small amount of time from one of its neighbor, it can decide to start an analysis on this neighbor. Using our security middleware, a peer can therefore launch a security task in a distant node from the same community to check if there's no anomaly. One example is when a peer decide to run an anti-virus on one of its neighbor.

3) When a peer wants to join an existing community: From the access network resource in layer 4 of our middleware, we can implement a network access service to control new peers. In this layer, we manage authentication exchange with the 802.1x protocol and in layer 5, a Radius service. When authentication is successful, exchanges can be made with other resource manager in order to control all services that must be present on the peers.

4) Exclude a peer of the community: To exclude a peer from the community because this peer became untrusted, each of its neighbor can decide to change their firewall rules to block communication from this untrusted peer.

B. A deployment example of a logical secure architecture on a physical existing network

In many cases, users need to exchange data via secure communication link. But current solutions are not so easy to deploy. The right communication port must be open and we need to ask to the administrator to change the rules of the firewall only for this connection, perhaps for only a small amount of time. The approach "grid of security" can solve these problems. For instance, if a user in a community wants to create a VPN from his computer A to a server S, the middleware asks if an existing VPN from on computer of the community to this server exists. If a computer B has already establish this connection, a simple connection between A and B can be establish and all data from A to B will be redirect to S. If no VPN connection to S exist in the community, the connection resource manager (in layer 4 of our model) will inform the firewall service (in layer 5) to open a given port to allow a VPN connection between A and S.

In the same principle, several security services can benefit from this distributed management: firewall services, anti-virus, intrusion detection, system updating, network access control, virtual private network, etc.

For each of these services, rules are defined for inbound and outbound connexion. The resource manager (in Layer 4) exchange information between each service of each peer. For instance, if a user wants to open one communication port for an existing service on his computer A, the resource manager will contact all other peers in the community and look for a similar rule on each peers. If this rule already exists in the community, the resource manager of computer A informs the firewall service (in Layer 5) of computer A that it can open this port.

V. Conclusions

The new approach developed in this paper permit to easily create a confidence community in which each user communications are safe and secured. Each peer is self-managed and exchanges informations with other peers to mutually develop a security policy management. This process is transparent, and each peer does not need to have the knowledge of the global policy. Moreover from this new architecture, a peer

can be easily exclude of the network or build a secure ad-hoc network without any centralized control. In the advent of IPv6, this distributed solution may help to establish secure networks when all devices have public IP and can be reached from Internet. The proposed new security architecture and middleware can be a solution to construct secure solutions over Internet between any computer.

REFERENCES

[1] A. Ebalard and G. Valadon, "La sécurité dans mobile ipv6," in *SSTIC06*, 2006.

[2] G. Valadon, "Mobile ipv6 : architectures et protocoles," Thèse de doctorat, Université Pierre et Marie Curie, Juin 2008.

[3] K. HyunGon and O. ByeongKyun, "Secure and low latency handoff scheme for proxy mobile ipv6," in *Mobility '08: Proceedings of the International Conference on Mobile Technology, Applications, and Systems*. New York, NY, USA: ACM, 2008, pp. 1–9.

[4] K. Elgoarany and M. Eltoweissy, "Security in mobile ipv6: A survey," *Information Security Technical Report*, vol. 12, no. 1, pp. 32–43, 2007.

[5] Z. Lidong and J. H. Zygmunt, "Securing ad hoc networks," in *IEEE Network*, vol. 13, no. 6. IEEE, 1999, pp. 24–30.

[6] C. Castelluccia and A. Spognardi, "Rok : A robust key pre-distribution protocol for multi-stage wireless sensor networks," in *IEEE Securecomm*, September 2007.

[7] C. Castellucia and A. Francillon, "Protéger les réseaux de capteurs sans fil," in *SSTIC08*, 2008.

[8] Y. Ping, Y. Yan, H. Yafei, Z. Yiping, and Z. Shiyong, "Securing ad hoc networks through mobile agent," in *InfoSecu '04; Proceedings of the 3rd internatianal conference on Information security*. ACM, 2004.

[9] D. P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, and D. Werthimer, "SETI@home: an experiment in public-resource computing," *Communications of the ACM*, vol. 45, no. 11, pp. 56–61, November 2002.

[10] D. P. Anderson, "BOINC: A System for Public-Resource Computing and Storage," in *GRID '04: Proceedings of the Fifth IEEE/ACM International Workshop on Grid Computing (GRID'04)*. Washington, DC, USA: IEEE Computer Society, 2004, pp. 4–10.

[11] F. Cappello, S. Djilali, G. Fedak, T. Herault, F. Magniette, V. Néri, and O. Lodygensky, "Computing on Large Scale Distributed Systems: XtremWeb Architecture, Programming Models, Security, Tests and Convergence with Grid," in *FGCS Future Generation Computer Science*, vol. 21, March 2004, pp. 417–437.

[12] E. Caron and F. Desprez, "Diet: A scalable toolbox to build network enabled servers on the grid," *International Journal of High Performance Computing Applications*, vol. 20, no. 3, pp. 335–352, 2006.

[13] W. Allcock, A. Chervenak, I. Foster, L. Pearlman, V. Welch, and M. Wilde, "Globus toolkit support for distributed data-intensive science," in *in International Conference on Computing in High Energy and Nuclear Physics (CHEP'01)*. IEEE Press, September 2001.

[14] O. Flauzac, M. Krajecki, and J. Fugère, "CONFIIT : a middleware for peer to peer computing," in *The 2003 International Conference on Computational Science and its Applications (ICCSA 2003)*, C. T. M. Gravilova and P. L'Ecuyer, Eds., vol. 2669 (III) of Lecture Notes in Computer Science. Montréal, Québec: Springer-Verlag, June 2003, pp. 69–78.

[15] M. Krajecki, O. Flauzac, and P.-P. Mérel, "Focus on the communication scheme in the middleware CONFIIT using XML-RPC," in *International Workshop on Java for Parallel Distributed Computing (IW-JPDC'04)*, vol. 6. Santa Fe, New Mexico, USA: IEEE Computer Society, April 2004, p. 160b.

[16] M. Krajecki and O. Flauzac, "Brevet numéro 0308501 - système de gestion distribuée de ressources informatiques et de données."

[17] J. Kubiatowicz, D. Bindel, Y. Chen, P. Eaton, D. Geels, R. Gummadi, S. Rhea, H. Weatherspoon, W. Weimer, C. Wells, and B. Zhao, "Oceanstore : An architecture for global-scale persistent storage," in *Proceedings of ACM ASPLOS*. ACM Press, November 2000.

[18] Freenet, "http://www.freenet.sourceforge.net."

[19] S. Lacour, C. Perez, and T. Priol, "A Network Topology Description Model for Grid Application Deployment," in *GRID '04: Proceedings of the Fifth IEEE/ACM International Workshop on Grid Computing (GRID'04)*. Washington, DC, USA: IEEE Computer Society, 2004, pp. 61–68.

[20] M. Baker, R. Buyya, and D. Laforenza, "Grids and grid technologies for wide-area distributed computing," *Softw. Pract. Exper.*, vol. 32, no. 15, pp. 1437–1466, Dec. 2002.

[21] I. Foster and C. Kesselman, "Globus : a metacomputing infrastructure toolkit," in *Supercomputer Applications*, I. Press, Ed., vol. 11 (2), 1997, pp. 115–128.

[22] C. Rabat, A. Bui, and O. Flauzac, "A random walk topology management solution for grid," in *I2CS*, ser. Lecture Notes in Computer Science, vol. 3908. Springer, 2006, pp. 91–104.