Internet Engineering Task Force
Internet-Draft
Expires: January 12, 2006

A. Vives
J. Palet
Consulintel
P. Savola
CSC/FUNET

July 11, 2005

Distributed Security Framework
draft-vives-v6ops-distributed-security-framework-00.txt

Status of this Memo

Copyright Notice

Abstract

Current Internet trends in several fields have brought some security concerns with regards to what will happen with the current security paradigms and mechanisms.

This document analyzes two security paradigms, the network-based and the host-based. The former refers to what is being used nowadays out

there and the latter is based on the distributed firewall concept [2].

From the point of view of these security concerns it is stated that there is a problem that must be addressed.

Some insights are given with respect to the host-based security paradigm.

Table of Contents

1. Introduction

There are a lot of emerging technologies that lead to scenarios where the current security paradigms, mechanisms and practices are not capable to protect against current threats, which have increased in type and number. These have raised some security concerns with regard to what will happen in a medium/short term.

Nowadays we are seeing how IP-enabled devices are more common each day, so we don&#65533;t just see laptops but also PDAs and mobile phones walking around and connecting/roaming to/between different networks. This comes together with the use of P2P and GRID applications which are based on the end-to-end paradigm.

In line with the end-to-end paradigm is the new Internet Protocol version (IPv6) [3] because of the provision of enough globally routable addresses as required. For example Mobile IP needs several addresses for each moving host [4].

IPv6 also adds the availability of IPsec [5] [7] in the stack, what could be used for end-to-end encrypted communications, with all the problems that this imply to the security infrastructures currently deployed.

Another kind of IP devices that are appearing are home automation devices which have its own IP stack and applications but few computing resources. These devices are susceptible of being compromised and used for malicious things but have almost no resources to be used for being self-protected.

From this perspective, this document analyzes the most (currently) used security paradigm, which from now will be referred as network-based security scheme. The objective is to identify its drawbacks and advantages against the new foreseen scenarios.

Based on the distributed firewall concept [2] we introduce the host-based security scheme, which extends the security mechanisms used from only firewalling to a number of them (IDS, firewalling, anti-virus, version control, etc.). Not only its drawbacks and advantages against the new foreseen scenarios are identified but also it is presented as a possible direction to follow to solve the above-mentioned security concerns.

Once these two security models are described we state that a security problem will arise if no new techniques are used to address the coming technologies.

In order to provide some insights about the distributed security

model some definitions and scenarios are given along with some concrete issues analysis.

2. Security Models

2.1 Network-based

To secure a network one or more Firewalls (FW) are used depending on the network topology and size. The FW can perform security tasks over the traffic that goes through/to its interfaces. The security administrator will be in charge of putting the firewalls where it considers and to configure them to accomplish the organization&#65533;s network security policy.

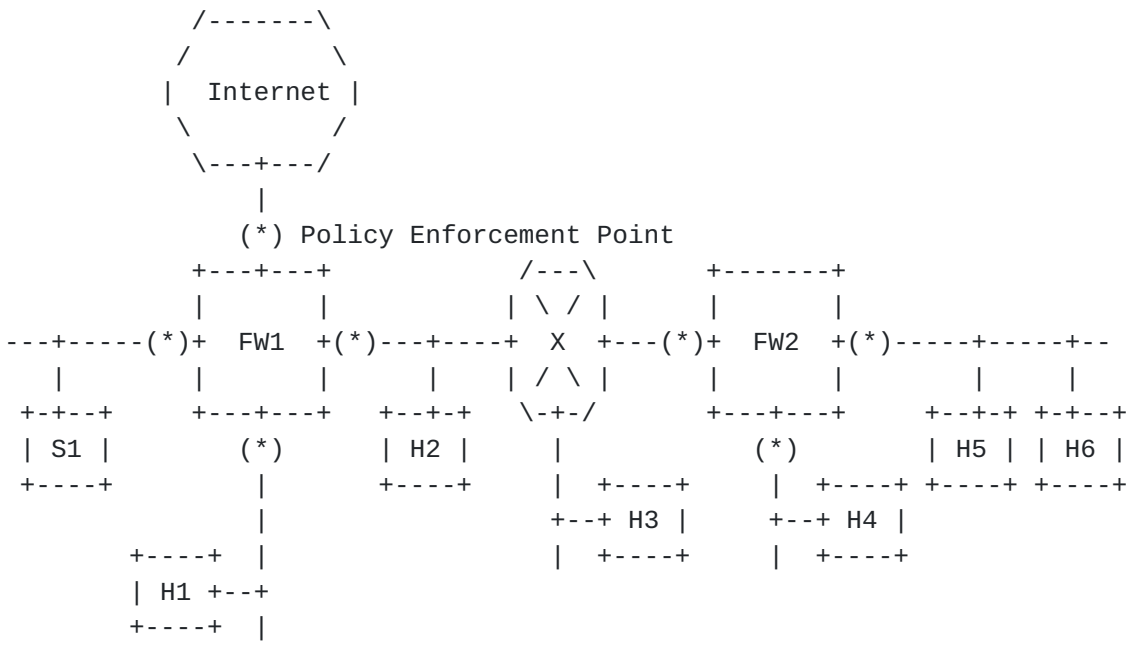

Figure 1: Network-based Security

As an example we can see in Figure 1 a network with one connection to Internet and several LANs. With this configuration the FW1 could inspect all the traffic coming in/out from/to Internet. This means that FW1 will be the first node that an outside attack will see. As can be seen the security policy in enforced in all FWs interfaces. Note that, for example, traffic between H2 and H3 or between H5 and H6 is not noticed by any FW.

This is the most used scheme, where the security of a host depends on the point of the network it is connected to, i.e., depends on the topology of the network.

The complexity of the security infrastructure will be proportional to the size of the network and the decisions taken by the security administrator who will decide the number and type of FWs. There are mechanisms to propagate the configuration among different firewalls, from the same manufacturer and for big appliances, in order to simplify the administration in case of large networks.

This model is based on the following assumptions to work properly:

- The threats come from "outside" the protected network, basically the Internet.
- Everybody from the same LAN segment is trusted.
- The protected nodes won't go "outside" the protected network where the security infrastructure won't be able to protect them.
- There are no backdoors on the network (modem, WLAN, other connections).
- The hosts will not need to be accessed directly from outside (at least in a general manner, i.e., potentially all ports on all hosts).
- The security policy could be applied in one or more of the following levels: network, transport and application.

The advantages of this model are:

- It is a mature technology which have been used for a long time.
- Its simplicity and easiness as the elements and points of configuration are reduced to the minimum.

The drawbacks of this model are:

- This is a firewall-dependant model, i.e., if a FW fails, then all the networks connected to it will loose network connectivity unless specific fail-over techniques are applied.
- A big percentage of the threats come from inside the protected network. To protect all the inter-LAN communications in a large network the number and cost of the needed FWs could be too much. In any case the hosts are not protected within its own LAN segment.
- The most dangerous threats, in the sense that one may not be able to protect from them, come from inside the protected network.

- The FW usually acts as NAT and/or proxy box, interfering or even disallowing end-to-end communications. In complex configurations, even more than one level of NAT/proxy could appear.

- Transport mode secured communications (using IPsec ESP for example) need special solutions ([1]).

- The same security policy may be enforced for all the nodes of each network connected to the FW, but it is also possible to have separate policies for all hosts. In any case, an error in a FW will equally expose all hosts on networks connected to that FW.

- Virtual organizations, for example those using GRID models, don't work with traditional centralized security models.

- The lack of secure end-to-end prevents deployment of innovative applications.

2.2 Host-based

We will call Host-based security model an evolution of the concept of distributed firewall already introduced by [2]. It is based on the idea of enforcing the security policy in each network host from a central control point.

The biggest challenge is trusting that the hosts comply to the rules they've received, for example that the user can't just disable the firewall if (s)he dislike the policy. Of course, this only can happen in the case (s)he has administrative rights for that (often not the case in non-personal systems, those not owned by the end-user, such as corporate PCs or laptops). It seems that one or more network entities would have to keep watch over the hosts in order to detect if they are not following the received policy.

From a security point of view this model somehow eases the work to the "enemies", putting the Policy Enforcement Point in their hands. So, not only mechanisms to prevent direct attacks to the security solution must be developed but mechanisms to minimize the consequences as well.

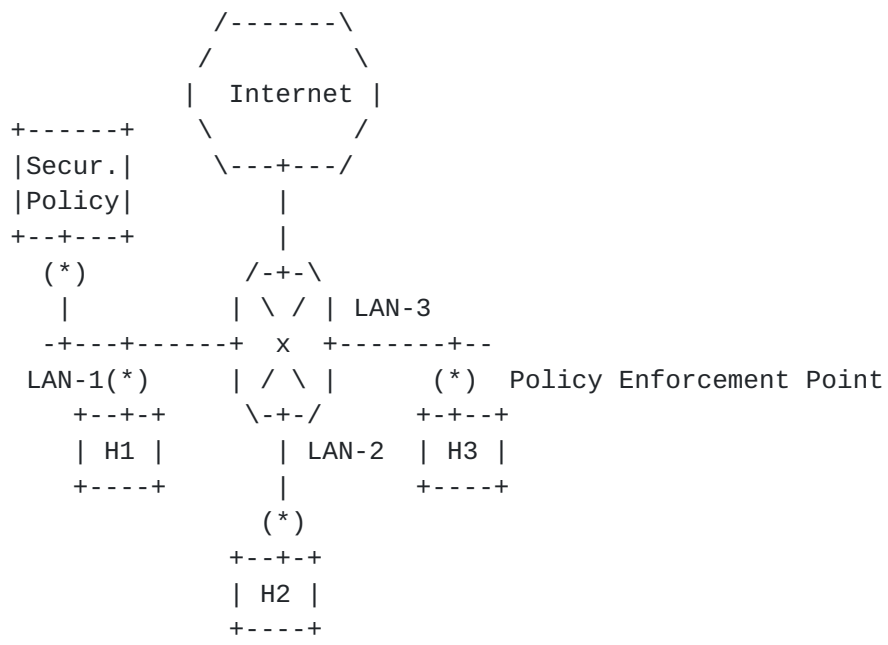

Figure 2: Host-based Security

This model is based on the following assumptions:

- Each host can be uniquely and securely identified.
- The security policy could be applied in one or more of the following levels: network, transport and application.
- Threats come from anywhere in the network.
- "Outside" hosts may be able to access all hosts "Inside", depending on the policies.
- No assumptions are made about where the host can be connected.

The advantages of this model are:

- The flexibility in the definition of security policies, as it is based on the assumption of an available Policy Specification Language which can be used for high-level definitions of all the needed policies.
- A host can take better decisions as it knows what it is doing or trying to do, that means it can better detect strange packets. For example, it could allow mail traffic to only one application on the system.

- Enables the usage of end-to-end applications level security (e.g., web services security standards).

- Enables better protection from attacks by the "internal" users, and possibly even to a degree from those in the local segment. For example address spoofing can be detected and avoided coming from the same LAN segment, without router participation, because a host in a LAN can detect packets from other host with source addresses that are not used in that LAN.

- Can protect a host independent of the topology, i.e., wherever the host is connected.

- Does not need specific devices to secure a host. Consider the case of a single host with a CPE (Customer Premises Equipment), if the CPE has no (user-controllable) firewall functions.

- Can control the outgoing attempts from each host, avoiding local network misbehavior or malicious practices.

- The collection of audit information could be more complete in a distributed model, despite the processing of that information is done in a distributed or centralized fashion.

- It maintains the centralized control of the security policies, from where they are distributed to each host (central decisions, local enforcement), despite the size of the network to protect. In general it scales well.

- It enables new distributed and cooperative solutions to improve the network security.

The drawbacks of this model are:

- It is more complex than the Network-based one as more elements are needed, some of them need to be defined or even designed.

- The uniqueness and secured identification of hosts is not trivial (for example, [2] proposes the use of certificates).

- The hosts must be trusted (or designed appropriately) so that they will operate according to the policy. For example, it must be impossible to disable the firewall functions or if the policy is not followed network communication is not allowed.

- A host that becomes compromised or infected with a worm or virus in any case can't be trusted to operate according to the policies, as the worms/viruses probably first create holes or disable the

protections if they can.

- It may be challenging to design the system so that policy updates are made available to the nodes which may not be network-reachable all the time.

- It may be difficult to distinguish a misbehaving application from a legitimate application (for example, many email worms may be channeled through the MUA which must be authorized to send the mails to operate correctly).

- Because of having a centralized Policy Decision Point (PDP) from where the Security Policies are distributed a weakness is introduced in form of a central point of failure unless more complexity is added, for example with a distributed/replicated system.

- The host security is in some sense 'server-dependant'. It must be able to detect the lost of connectivity with the PDP and act in consequence. It also seems that being disconnected from the PDP for a long period could be dangerous because updated security information raise the security level.

3. Problem Statement

The starting points are the new technologies we mentioned above and the network-based security model. We will demonstrate that things like IPv6 deployment or P2P applications impose a problem to the most common security models.

Finally we will outline how the host-based security model is able to address a number of those problems.

Not only new technologies but also new threats have appeared that use security holes in the software. Viruses, spyware, adware, spam, worms and (D)DoS attacks have made necessary to use several security tools to fight these threats. This is the reason of the appearance of different software pieces that are installed on both the servers (anti-spam and anti-virus) and the user hosts (software version control, anti-virus and anti-spyware). The trend seems to be to direct the attacks against user hosts, the attacks directed to servers are decreasing.

We can summarize the consequences of the appearance of new technologies (IPv6, P2P, GRID, mobile IP, etc.), new behaviors and new threats as:

1. The need/use of end-to-end communications.

2. The availability/use of IPsec on all IP devices. For example, all IPv6 stacks have IPsec capability that can be used if required.

3. Nomadic IP devices that will move between different networks under different security administration.

4. A number of different security mechanisms are needed in order to protect a network/host.

The network-based security model has problems addressing the above points. This can be summarized in:

1. It difficults/avoids end-to-end communications because of the FWs acting as NAT and/or proxy.

2. Transport mode secured communications (using IPsec ESP for example) need special solutions ([1]). The basic idea is that the encrypted payload can&#65533;'t be inspected.

3. It is not able to protect nomadic nodes that move out of the protected network. In foreign network the nodes are exposed to threats and can be infected when they come back to their "home" network.

In the other hand the host-based security model could address the following points from the above-mentioned:

1. It assumes end-to-end connectivity of all nodes, so the end-to-end communications are the natural way of doing things.

2. As the security rules could be applied before encrypting the payload, the encrypting does not affect the security mechanism which could work in a straightforward way.

3. Nodes will be protected wherever they are as always will have security mechanisms on the hosts. It should be taken into account that the security policy update must be done as frequently as possible.

In any case it should be clearly stated that the network-based security model is a mature technology which have been used for a long time. The host-based security model is basically just this, a model, and several issues must be solved before it takes place.

Security improvements in both the network-based and the host-based

security models are required, for example to be able to cope with all the actual security threats. The idea is to try to integrate in a unique solution as much mechanisms as possible, and tune them to follow the security policy within a protected network and its hosts, in case they move to a foreign network.

Following this idea a hybrid model could be used where both the network-based and host-based models are used. The tasks could be distributed among both or be activated depending of where the host is connected to, if there is a security alert situation, etc.

Insights over the problems that host-based security model must resolve before being deployed in real life are outlined in following sections.

4. Framework for Distributed Security

4.1 Definitions

To describe the distributed security model several terms will be used. They are defined here as follows:

- SD (Security Domain): Network portion under the administration of the same Security Administrator/Organization.

- SP (Security Policy): We refer to the information that is distributed to each policy enforcement point within a SD in order to achieve the desired level of security. This information will follow the whole protected network security policy defined by the Security Administrator of that network. This information will be converted to specific rules for each platform by the Policy Enforcement Agent.

- SS (Security Status): Information about host different aspects that could be used to measure how secure it is.

- PSL (Policy Specification Language): Language used to define SP and SS.

- PDP (Policy Decision Point): The node where the SPs for a SD are defined. From the PDP the SPs are distributed to PEPs.

- PEP (Policy Enforcement Point): The place where a SP is applied.

- PEA (Policy Enforcement Agent): The entity in charge of applying the SP at the PEP.

o PXP (Policy Exchange Protocol): The protocol used for distribution of the SP to the PEA.

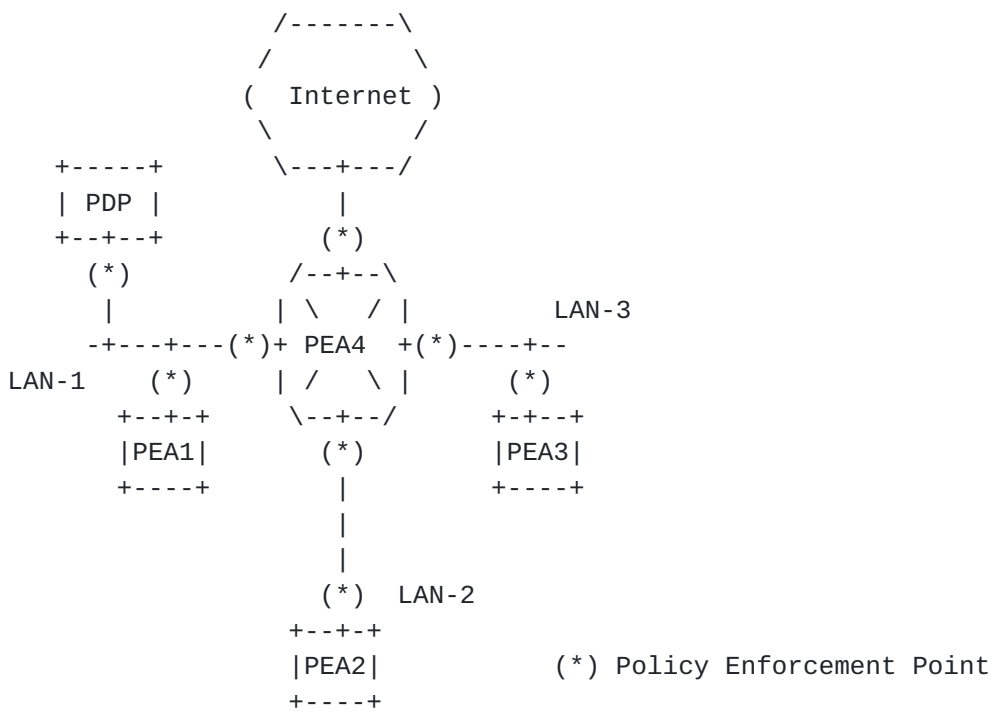

Figure 3: Definitions: Basic Scheme

The basic idea is simple: the Security Policy is centrally defined using the Policy Specification Language and distributed to each Policy Enforcement Agent by means of the Policy Exchange Protocol. The PEA will apply the SP to each Policy Enforcement Point it is responsible for. The network entities need to be authenticated in order to be trusted, for example to allow an incoming connection or to trust on the received Security Policy.

4.2 Scenarios

In order to gain some insights in the distributed security analysis some scenarios are depicted to be considered when drawbacks and advantages are outlined.

The idea is to address some general scenarios which already exist and where new technologies, devices, users and behaviors take place. For example the deployment of the new Internet Protocol, IPv6, the use of P2P and GRID applications and new nomadic IP devices could be seen as some of the issues that bring new security scenarios that should be

analyzed.

One important issue that must be taken into account is the movement of a host between different scenarios/networks. This point will be addressed in section 4.4.5 of this document.

Basically three possible scenarios have to be addressed, all of them interconnected through Internet:

o Enterprise.

o ISP-Client.

o Public.

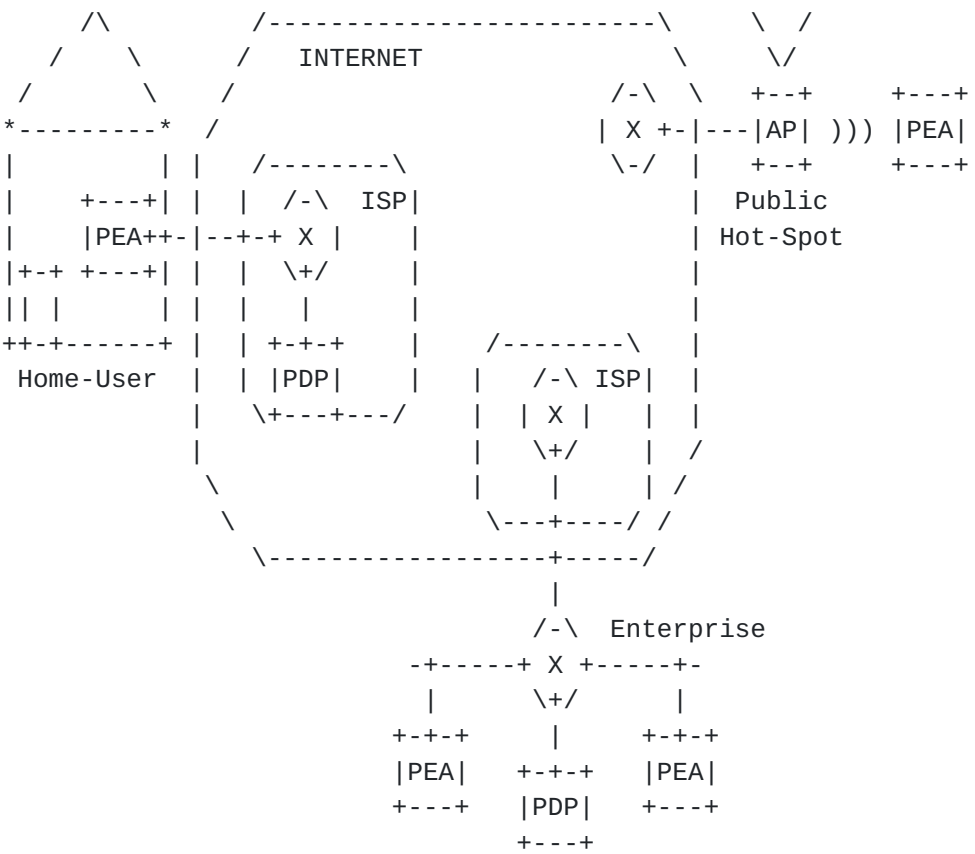

Figure 4: Scenarios

4.2.1 Enterprise

This scenario considers the case of an organization with its own infrastructure containing both PDP(s) and PEP(s). This means that

all the security infrastructure elements will be within the organization premises under the same administration.

All the hosts connected to the protected network will also be administered by the above-mentioned administration. So, it is highly probable that they use some kind of distributed security software that would collaborate to increase the security.

4.2.2 Home-User

This scenario considers the case of an Residential Customer which has its PEP as part of the security solution. The user has several choices as PDP. The user could even not have a PDP and define by himself the Security Policy. Also could use one provided as a paid service from a company located somewhere in Internet. The ISP could also offer a PDP service for its customers.

In case of a user connecting to his/her enterprise VPN the PDP used should be the one from that network. Even in the case of not using a VPN the PDP could be the one from the user company.

Other hosts in the same network will be in charge of the Home-User, so they could use some kind of distributed security software that would collaborate to increase the security.

4.2.3 Public Hot-Spot

This scenario considers the case of the host being connected to a pubic Internet connection (not neccesarily only the case of a Wi-Fi Hot-Spot). In this case the PEP will be located at the host but could not be sure to trust/have connectivity to a foreign PDP.

Other hosts in the same network can not be trusted at all to be using some kind of distributed security software that would collaborate to increase the security.

4.3 Functions of the Elements

4.3.1 Policy Specification Language (PSL)

The host-based model is based on the assumption of the use of a number of security mechanisms, for example firewall, IDS, anti-virus and software version control.

This requirement means that the PSL must be flexible enough to specify the information about different objects and rules to behave depending on the value of that information.

Also the PSL must be able to specify security policies for new mechanism that could be added or appear in the future.

The flexibility in the PSL will allow the coordinated use of the different security mechanisms by the PEA. For example it could be defined that if the version of the mail user agent is not a safe one (version control security mechanism) the mail traffic is not allowed (firewall security mechanism).

The syntax and semantics of the PSL must be clearly defined in a standard way.

4.3.2 Security Policy (SP)

Thanks to the flexibility of the PSL the SP will include all the needed rules to follow the Security Administrator needs.

The security policy should have rules to define configuration for all the security mechanisms used, based on the Security Status of the host.

The SP could be specified with different granularity and using conditional statements.

Granularity refers to the ability of referencing, at each layer, to all the possible elements. For example, TCP/UDP ports or any IP header element&#65533;s value. It is a matter of the implementation to reach a compromise between granularity and complexity.

Conditional statements refers to the ability of taking decisions based on the values of different elements, as detailed as the granularity allows. Even different complete sets of rules could be defined for different situations, like changing to a different SD (see Scenarios section above). For example, in case of the change of a value the PEA could already have a rule on the received SP for the new value, avoiding the need of communicating it to the PDP, which would have to define a new SP and send it to the PEA.

The SP also will be used to manage the update of elements in the host in order to increase the security, for example, a new anti-virus signature file or a new patched version of a piece of software with a known security breach.

4.3.3 Security Status (SS)

Security Status is the list of the defined properties of the system, to be used for checking the conformance to the Security Policy. For example: "firefox", "1.0.2"; where the security policy might mandate

that version 1.0.3 would be required.

4.3.4 Security Domain (SD)

The concept of Security Domain is of capital importance in order to clarify where a SP must be applied. Also the concept of changing from one SD to another one is important and will be addressed leter in this document in detail.

A host that connects to a SD must accept the SP it receives and apply it. In case of not following this rule the host could not be sure to have network connectivity. It is matter of the security solution how to manage the hosts that don't apply the received policy.

4.3.5 Policy Enforcement Agent (PEA)

The PEA will have a key role in the whole system as it will be the one in charge of assuring that the received SP is applied. To accomplish this task several issues must be addressed:

- Verification of Authenticity and integrity of the received SP.
- Verification of the Security Status (SS) of the PEP.
- Comparison between the SS and the received SP and application of the specified rules depending on the comparison results.
- Running the different security mechanisms.
- Being able to communicate with other PEAs in order to allow distributed security mechanisms.
- Being proactive in order to detect and respond to any security event.

4.4 Issues

4.4.1 Node Addition/Deletion

We refer to addition to both:

- The process of configuring a totally new node, installing the PEA and its first message exchange with the PDP or other PEAs.
- The addition of a node to the process launched when a node that has been off-line get reconnected again and tries to communicate with one PDP to get the last available SP.

This dual approach applies also for the deletion process.

During the process of a node addition the host must be able to find the correct PDP which should authenticate itself as must do the host as well.

The solution must support the addition and deletion of hosts from the SD dynamically with no degradation of the functionality and performance.

When a new node is connected to the SD network it should follow the required steps in order to be authenticated and configured following the appropriated SP.

It will be a matter of the solution to assure that the hosts are following the received SP during the time they are connected to the SD network.

4.4.2 Authentication

It is required that new hosts connected to the network demonstrate their identity for both receiving a useful SP and to communicate with other hosts within the same SD.

This way, a host needs to authenticate itself first. After that, the host may or may not be authorized to have connectivity with other networks through a switch/router or to be able to communicate with other hosts.

As a guideline, cryptographic certificates could be used for this purpose, in order to guarantee the identity of the sender of a message. As the identity will be used within the SD a SD-wide PKI could be used.

4.4.3 Policy Exchange Protocol

The PXP is in charge of the distribution of the corresponding SP(s) to the PEAs. This protocol should assure the delivery and update of the SP even in the case of possible problems, like the chance of a PDP failure or some kind of unreachability, for example in case of network segmentation.

Also either the PEA or the PDP could launch an event that results in a SP update or change. The PDP will update the SP in case of new security information is received for one or more of the used security mechanisms. The PEA could also inform the PDP of a new Security Status because of some change in the PEP configuration. Based in this new status the PDP could update the SP.

There could be some active mechanisms, like IDS, that could lead to some SP change.

4.4.4 Data Integrity and Authenticity

There are several pieces of information that will be passed among entities within the security solution that would be a good target for an attack. This information should be protected both while stored in a host and while transmitted from one host to another.

As a guideline, cryptographic certificates could be used for this purpose, in order to guarantee the integrity and origin of the information. As the identity will be used within the SD a SD-wide PKI could be used.

4.4.5 Moving between security domains

As have been seen above a host, with its PEA, could move between different SD or between different scenarios, some of them with no security guarantees at all and no PDP available.

If all network devices are globally reachable there will be no problem on reaching other hosts belonging to the same security solution cluster, including the PDP, which could be inside the corporate network.

The solution must be able to manage this situation both being able to detect a network/SD change and responding in consequence, for example establishing a default SP in foreign networks (presumably a restrictive SP).

5. Other Issues

Further elaboration is required (TBD) on:

- Malicious users: We can't protect the network from malicious users that have physical access to network hosts in the protected network. The objective is to minimize the danger they can cause.

- In the host-based security, the host that stores and distributes the security policies seems to be the best option to be the one that acts as IDS information collector.

6. Conclusions

New technologies (IPv6, P2P, GRID, Mobile IP, etc.), behaviors (use of small devices like PDAs and moving to different networks) and

threats (Virus, spam, spyware, adware, etc.) require improving the security mechanisms actually being used. By one side the integration of different mechanisms and by other side the movement of the security policy enforcement point towards the hosts interfaces are recommended in order to improve the security of the hosts and in consequence of the network.

Also a centralized control over the policy definition and enforcement is of importance in order to have a scalable solution.

The network-based security model has problems addressing the new technologies and threats. The host-based model has been described as a reference for a possible solution. The latter model is presented as complementary to the former one.

7. Security Considerations

This document is concerned entirely with security.

8. Acknowledgements

The authors would like to acknowledge the inputs of Brian Carpenter, Satoshi Kondo, Shinsuke Suzuki, Peter Bieringer and the European Commission support in the co-funding of the Euro6IX project, where this work is being developed.

9. References

9.1 Normative References

9.2 Informative References

[1] "IETF midcom WG", <http://www.ietf.org/html.charters/midcom-charter.html>.

[2] Bellovin, S., "Distributed Firewalls", November 1999, <http://www.research.att.com/~smb/papers/distfw.pdf>.

[3] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[4] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[5] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[6] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402,

November 1998.

[7] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.

Authors' Addresses

Alvaro Vives Martinez
Consulintel
San Jose Artesano, 1
Alcobendas - Madrid
E-28108 - Spain

Phone: +34 91 151 81 99
Fax: +34 91 151 81 98
Email: alvaro.vives@consulintel.es

Jordi Palet Martinez
Consulintel
San Jose Artesano, 1
Alcobendas - Madrid
E-28108 - Spain

Phone: +34 91 151 81 99
Fax: +34 91 151 81 98
Email: jordi.palet@consulintel.es

Pekka Savola
CSC/FUNET
Espoo
Finland

Email: psavola@funet.fi

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.