Internet Engineering Task Force
Internet-Draft
Expires: August 24, 2005

J. Palet
A. Vives
Consulintel
G. Martinez
A. Gomez
University of Murcia (UMU)

February 20, 2005

IPv6 Distributed Security Requirements
draft-palet-v6ops-ipv6security-02.txt

Status of this Memo

Copyright Notice

Abstract

The security policies currently applied in Internet with IPv4, doesn't longer apply for end-to-end security models which IPv6 will enable.

Today, each network is often secured by one or several devices (i.e. security gateway or border firewall in the simplest configuration), which become a bottleneck for the end-to-end security model with IPv6.

In addition, users and devices start to be nomadic, moving between different networks that could have different security policies.

A distributed and dynamic approach is consequently required, as already described by [1].

All these points and others are discussed in [2] as a reason of concern for the security administrator when operating IPv6 networks. In this document the problem is accepted and a step forward is done defining the requirements for a possible solution.

How these requirements are satisfied by a possible solution is out of the scope of the present document.

Table of Contents

1. Introduction

Today's Internet paradigms for security need a revision with the deployment of IPv6, as suggested in [2], offering end-to-end security capabilities.

Current security policies based on a centric approach with unique border devices don't longer apply, the so-called network-based security. Often they are based in a firewall or security gateway and statically configured rules, which don't work in all the situations, for example, they don't consider the internal threats.

Additionally, the network-based security model is deeply incompatible with the model of virtual organizations that is fundamental to Grid computing, where virtual organizations cross all traditional security boundaries.

Users and devices start to be nomadic. They often move from one network to another and this needs to be taken in consideration to keep the security of the complete visited network abd the nomadic host.

Keeping today's static security model seems to be the wrong approach, which interferes with the end-to-end features and advantages of IPv6.

Enforcing the nomadic users and devices to connect to Internet by means of the security gateway, in tunnel mode, is often equivalent to disable the IPsec protocol on each node, not allowing the use of transport mode and consequently invalidating one of the key IPv6 advantages.

The lack of end-to-end secure communication and in general the current network-based security model, specially in enterprise networks, prevents innovation.

On the other hand, it is also true and perfectly understandable that there is a need to enforce security in the networks, in such way that the security administrator has always the control over it.

2. Security Definition

As this document tries to stablish the security requirements for an IPv6 network, the definition of what is understood as security is of capital importance.

We use security in the "big scope" of the word, trying to include as much as possible. In other words, a host, a network or some information, will be secure when no attacks could succeed against

them. A success will mean compromise of availability, integrity, confidentiality or authenticity. The realistic objective is to be as much secure as possible in a precise moment.

So the security solution should include a number of mechanisms to provide security to network devices. Current mechanisms could be integrated in the solution and defined in the security policy. For example there could be active firewalling together with Intrusion detection, antivirus software and system update mechanisms.

Security mechanisms should also include techniques to mitigate the danger in case of a compromised host and/or network.

3. Distributed Security Model

As described in [2], a possible security scheme is the distributed one [1], as an alternative to the network-based model.

The aim is to keep, or even more, be able to increase the security in the network as a whole and simultaneously keep the control of it under the security administrator hands, while the individual nodes can take advantage of end-to-end and secure end-to-end communications.

The basic idea is simple: the Security Policy is centrally defined using the Policy Specification Language and distributed to each host by means of a Policy Exchange Protocol. The Network Entities need to be authenticated in order to be trusted. See [2] for more details.

These hosts must respect the security policy of the network where they are attached. In case of a conflict which is not automatically resoluble, a resolution arbitration mechanism should be established.

The effect is simple to understand: instead of a one or a few firewalls, each one being a point of failure for the complete network(s), that could be attacked or fail, creating a bottleneck for all the communications, there will be a number of firewalls (at every host) configured according to a central policy, which increase the scalability, reliability, efficiency and performance of the complete network.

This is often becoming possible in most of the nodes because even if IPsec and encryption are enforced for most of the communications, nodes often have powerful CPUs with unused cycles that will easily accommodate the extra required workload. In case of small devices, they may not have those resources, and still need to rely on other devices for performing security functions on their behalf.

On the other hand, the central firewalls will be able to dedicate CPU cycles to new functions, or be able to protect bigger networks.

4. The Host

With IPv6 and the distributed security model the host play a crucial role in the network security, in other words, the security mechanisms are moved to each host.

As said above the entities, in this case the hosts, should authenticate themselves in order to be trusted. This will be a requirement of a possible solution.

4.1 Interior Security

With this approach, the security of each host is not only towards communications with Internet or other networks, but also with the rest of the nodes in the same network.

This means an increase in the overall security and the possibility to isolate individual nodes if required.

4.2 The Visiting Node

This distributed security model is valid not only for fixed nodes, i.e. desktop computers, but specially interesting and important for those nodes like laptops and PDAs, which keep moving among different networks. Vice versa, this model is of key importance for those networks that receive visits from nodes that are not under the control of the network/security administrator.

Different visited networks have different security requirements. Consequently is required that those nomadic nodes dynamically accommodate their own security policy to the one defined in the visited network and arbitrate the conflict resolution between different policies.

Nodes attaching to a network via VPNs, RAS, dial-up modems or other similar means can also be considered as visiting nodes, as they can also create a path between the visited network and any other network where they are actually connected. They must also be able to dynamically configure their own security to match the one existing in the visited network.

When a node is attached to a visited network and receives the visited Network's security policy, basically there are two possible situations:

1. The network security policy is equivalent or less restrictive than the node configuration. In this case, the node could not change its security policy configuration or relax its restrictions if needed for some applications, always following the received security policy. For this some degree of granularity in the security policy specification and enforcement should be given.

2. The network security policy is more restrictive than the actual node configuration. In this case, the node will adapt its security configuration to at least match the one indicated by the security policy.

A possible solution should take into account the case of a device attaching to the network and not following the security policy, either because it does not want to or because is not able to.

The alternative often used today to accomplish this, is by means of manual changes in the configuration of the visiting node, but they are always prone to errors and dangerous to be considered useful and secure enough, specially considering that the visiting node can be already infected from previous connections to other non-protected networks (home network, hot-spot, ...).

4.3 Default Security

The nodes can be attached to a network which doesn't offer any protection means, not only against external attacks, but also those coming from the same network, for example, in hot-spots, public networks, ad-hoc networks or even networks temporarily setup for conferences.

The distributed security model addresses this case because the host will have all the necessary means to protect itself. A Possible solution must take this into account and have an appropriated mechanism to detect the connection to a foreign network and apply the correspondent security policy, previously defined by the host security administrator.

This security Policy applied in foreign networks and/or in case of not having connectivity with the Policy Enforcement Point will be called the Default Security Policy.

4.4 Other Considerations

A requirement will be to offer Policy Change Facilities allowing the user or the host security administrator to change security settings. Also the switching between two or more allowed security policies

could be implemented.

5. Security Policy Server and Protocol

In order to achieve the benefits of the distributed security model, and at the same time provide the mean for the adequate and dynamic control of the overall network security by the network/security administrator, a security policy server is required.

The policy server(s) function could replace the main functionality of the central firewall and complement it. The security administrator will define the security rules required by all the networks and/or individual nodes.

A requirement will be to have a reliable Security Policy distribution mechanism. For example, the different nodes could query to the policy server to learn about the network security policy and adapt themselves in order to match it. The policy server could also request information and security status to the nodes.

Until the node performs and acknowledge the required security policy configuration update, it must not be allowed to transfer/receive data to/from other nodes either in the network or other connected networks.

The security policy server can also dynamically update the security policy for the complete network or specific nodes. This can be done in response to a security administrator decision, or other situations, like information received from an external or internal attack, detected by an intrusion detection system, firewall or even by nodes inside the network.

The security policy should be administered at a network level or individually for every node, upon decision of the network/security administrator.

A single standard Policy definicion Language and a Policy Exchange protocol are required for the signaling between the nodes, security policy servers, firewalls (including node or host firewalls), intrusion detections systems, honey pots, routers, and any other elements implicated in the overall network and nodes security.

Following this approach, the security administrator will use a PMT (Policy Management Tool), to edit the policies and distribute them via PXP (Policy Exchange Protocols) to the PEP (Policy Enforcement Points), in this case the end nodes.

For the interaction with IPsec policies, it seems appropriate the

existing IPsecCPIM [5].

To guarantee the self-security of this model, the security policy being communicated to the nodes should be digitally signed, in order to provide integrity, origin authentication and non-repudiate authenticity of the source.

6. Non-security-capable Nodes and Security Workload Distribution

Increase in security often means increase in processing power. Some nodes could not have the required CPU cycles to afford the complete required security policy.

Another requirement will be to take into account this, what we will call non-security-capable nodes.

The possible solution could fragment the security enforcement in different levels establishing a ligh set of security requirements for those kind of nodes. Another alternative is that the noces could be partitioned from the network and treated as non-security-capable nodes. Alternatively, the firewalls or even other security-capable nodes with free resources, could act as trusted security gateways for the non-security-capable nodes.

How to address this requirement is out of the scope of this document.

Despite the adopted solution, it seems only possible if minimum security verification can be done by those nodes, i.e. digital signature verification.

It could be even considered a system to provide a kind of security workload-balancing.

7. Location of the Security Policy Server

Firewalls and security gateways are expensive devices and they are required to sit at the border of the network. They also require qualified personal to manage them.

In the case of the distributed security model, the security policy server isn't required to be collocated as a border device.

This provides the opportunity to have this device not only inside the network, but also at any other point in Internet.

This opens the doors to new services and business models that provide very sophisticated security services, especially for Home, SOHO and SMEs.

Some possible "ideal" locations for the security policy servers could be Internet Exchanges [6] or in general PoPs, ISPs, and other similar central Internet locations.

8. Security Mechanism Modules

As said above, the security mechanism implemented could address several security problems by means of a number of tools.

The basic ones should be firewall, IDS (Intrusion Detection System), Anti-virus and software version checker.

These different tools could be thought as modules for both the policy definition and enforcement and the solution implementation.

9. Conclusions

In this document it was accepted that a problem will arise with the network-based security scheme and the deployment of IPv6. Also the security scheme that was in mind during the requirements definition was the host-based or the distributed one [2].

Possible solutions to addresses the requirements outlined in this document is out of the scope and will be defined elsewhere.

The Distributed Security Scheme has been described as the one that best fits as a solution to the Security Problem Stated [2]. This doesn't mean that the solution must follow this scheme strictly but seems to be useful at least as a guideline.

The purpose of this document is to give some abstract requirements of a possible solution.

As a summary of what has been seen above, we can outline the following requirements:

1. The solution must try to address as much as possible, in the sense of being able to protect against different threats using a number of mechanisms. The recommended ones are firewall, IDS, Anti-virus and software version control.

2. There must be a control mechanism to detect if a node is not following the appropriate security policy. This allows the solution to be prepared to receive foreign hosts.

3. The solution must allow the hosts to move to other networks under the same security policy, under a different one or under no security at all.

4. The security policy and its enforcement must be given with a certain degree of granularity in order to ease the different policies comparison and use.

5. A Security Policy Specification tool must be provided. This tool should use a single standard Security Policy Specification Language.

6. A reliable Security Policy Distribution mechanism must be provided. This mechanism should use a single standard Policy Exchange Protocol.

7. A reliable Security Policy Enforcement mechanism must be provided.

8. A reliable entity identity's authentication mechanism must be provided.

9. The solution must be dynamic in the sense of being able to respond to security events and adapt the policies accordingly.

10. Related to the previous one, a mechanism of "alarm distribution" is recommended, allowing the hosts to report security events to other hosts even in the case of, for example, problems in the Security Policy Server. The idea is that a distributed system could be more robust than a client-server one.

11. The solution must ease the security administrator's work allowing, for example, the centralized Security Policy management, i.e., definition, distribution and updating.

10. Security Considerations

This document is concerned entirely with security. TBD.

11. Acknowledgements

The authors would like to acknowledge the inputs from Cesar Olvera, Brian Carpenter, Satoshi Kondo, Pekka Savola and the European Commission support in the co-funding of the Euro6IX project, where this work is being developed.

12. References

12.1 Normative References

12.2 Informative References

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

[2] Vives, A. and J. Palet, "IPv6 Security Problem Statement", Internet-Draft draft-vives-v6ops-ipv6-security-ps-02, October 2004.

[3] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R. and A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC 2748, January 2000.

[4] Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R. and A. Smith, "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, March 2001.

[5] Jason, J., Rafalow, L. and E. Vyncke, "IPsec Configuration Policy Information Model", RFC 3585, August 2003.

[6] Morelli, M., "Advanced IPv6 Internet Exchange model", Internet-Draft draft-morelli-v6ops-ipv6-ix-00, July 2004.

[7] Arkko, J., Kempf, J., Sommerfeld, B., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", Internet-Draft draft-ietf-send-ndopt-06, July 2004.

Authors' Addresses

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

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

Gregorio Martinez
University of Murcia (UMU)
Campus de Espinardo s/n
Murcia
E-30071 - Spain

Phone: +34 968 364 607
Fax: +34 968 364 151
Email: gregorio@um.es

Antonio F. Gomez Skarmeta
University of Murcia (UMU)
Campus de Espinardo s/n
Murcia
E-30071 - Spain

Phone: +34 968 364 607
Fax: +34 968 364 151
Email: skarmeta@um.es

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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