



Permissions-Based Network Security

Most networks today use TCP/IP. With TCP/IP, networks are “default-open” - any device that is connected to the network can connect to any other device on the network, and two (or more) networks can easily be connected with each other. There is little need for management or control.

The virtue of TCP/IP networks is that they give users access to the information they need, when they need it, and where they need it. But these features also make it easy for hackers, worms and viruses to invade the network.

The rise of abuse has shown that default-open, while ideal, is simply not practical. In response, vendors have developed a variety of network security solutions. For the most part, these solutions address discrete points of network vulnerability.

For example:

- Usernames and passwords control access to servers
- Spam appliances stem the flow of unwanted email
- Firewalls, access lists, and intrusion protection keep traffic from entering the network in the first place
- Anti-virus software protects computers from worms, viruses, spyware and adware

This approach to network security is known as point-product because it applies a product to a point of vulnerability on the network. Point-product solutions have significant disadvantages in that they:

- Address classes of problems with general rules or algorithms. As a result, they paint with a broad brush, as anyone who has missed a legitimate email because it was incorrectly identified as spam knows;
- Assume user participation. For example, users must keep operating system patches and anti-virus definitions up to date, and must keep usernames and passwords secure. A visit to any office in which usernames and passwords are posted on computer screens shows one of the shortcomings of this approach;
- Can be quite costly. Firewalls and spam appliances can cost thousands of dollars to purchase and maintain. As a result, they are beyond the budgets of smaller companies and organizations, and the owners of even larger networks cannot afford redundancy, so point-product solutions can be single points of network failure.

It is also difficult for network owners to know which solutions are the “best of breed” and it takes considerable time to evaluate the various solutions available.

Finally, because of the proliferation of point-product solutions and the conflicting demands of network users, even small networks require either an in-house or third party security administrator to make the solutions effective.

It is understandable that the point-product approach has driven the network security market. Networks have grown as quickly as network abusers have discovered new ways to undermine them. It made sense to stamp out the fires.

But the age of the point-product approach is coming to an end. Network owners are increasingly concerned about its complexity and “stovepipe” design, and that it requires ever-increasing investments for staff education, system integration, and operation.

At the same time, businesses are making demands on their security teams to contribute to initiatives like regulatory compliance or service level management. Product-point solutions are islands unto themselves, and are increasingly technically ineffective and too complex and expensive to own and operate.

Cisco Systems summarizes the problem this way: “The point-product solution model has become inadequate for managing today’s network security risk, compliance and audit requirements.”

Permissions-Based Network Security

Networks are made up devices – routers, switches, computers, etc. This is the underlying perspective of the point-product approach.

A permissions-based approach to network security takes a different view. It sees that networks are also made up of users – users who download programs they should not download, open email that contains worms and viruses, or hack servers to which they should not have access.

Under a permissions-based approach, it does not matter who the user is. It also does not matter what the user’s motivations are. Permissions-based network security assumes that any user or device (desktop, laptop, PDA, etc.) is a potential abuser, whether by intent, accident, or oversight.

Permissions are, of course, based on the organization’s policies regarding network access, both in general and as those policies apply to individual users. Permissions-based network security addresses such questions as the following:

- Network Admission: Does the user have access to the network and is the user’s device healthy? Is the operating system up to date? Is anti-virus software installed and running? Are anti-virus definitions up to date? Is the user operating software that is not allowed on the network?

- Network Access: Determine the identity of the user and set permissions accordingly. If a user's identity cannot be established, the user is denied access to the network. If a user's identity can be established, set parameters regarding what the user can and cannot do on the network.
- Network Operation: Can network abuse be traced back to individual users? Can the solution report on network intrusion attempts? Can users circumvent permissions during a session by adjusting computer settings, installing new software, using another password, etc.? Is the solution easy to administer and affordable?

Under the permissions-based approach, permissions are stored as secure digital certificates in the AppiaSecure gateway, which administers those permissions on a real-time basis.

Permissions are set for both devices and user activities. AppiaSecure can be used to set permissions for such activities as:

- Web access
- Email
- Chat
- FTP
- Remote access
- Document and executable downloads
- Use of removable storage devices
- Web conferencing

What are the advantages of the permissions-based approach over the familiar point-product-approach?

- The permissions-based model is simpler and less complicated to manage, because it involves one device as opposed to several. It is therefore also less costly.
- Policies can be set to meet the individual needs of users. This contrasts with the broad brush approach of point-product solutions.
- A permissions-based approach addresses both device and user access. This ensures that the network is protected from both inside and outside threats.
- A permissions-based solution enables the network owner to decide how open or closed the network is, with a degree of precision that is simply not possible with point-product solutions.
- Permissions-based network security is fully auditable because network activity can be traced directly back to users.

It will, of course, take time for the permissions-based approach to replace the traditional point-product solutions. However, its lower cost, ease of administration, and flexibility are powerful arguments for adoption.