Class-based defense solution for VoIP networks

Because VoIP works on IP infrastructure, it is vulnerable to attack. The theory that Juniper launched began with the most effective methods in network security and similar to any other IP network.

Because VoIP works on IP infrastructure, it is vulnerable to attack. The theory that Juniper launched began with the most effective methods in network security and similar to any other IP network.

The first is to know all the relevant components including servers, IP protocols, processes, users and use a risk analysis pattern to determine where the risks are. Then select the appropriate technology or process to minimize the risks.

The network center of the business or service provider is located in the VoIP application server or UNIX server or PC running Linux operating system. The core network also has servers running the user and cost data management program to support VoIP applications.

At the periphery are gateway servers, servers that communicate with other VoIP network servers or transfer calls between switched and VoIP voice networks. The client is the IP phone that converts the digital signal into audio.

Source: ***checkpoint*** Juniper defense strategy lies in network layers, helping to protect each core device, edge area and client device, based on three main factors: Identifying the identity of network users, processes Control and technology are applied to protect the above content.

The first two goals can be accomplished with normal security checks, which identify those involved in the operation and specify security rights to enforce certain tasks. The protection of the application server's network core and devices similar to the protection of LANs against known IP attack risks such as operating system hack

(OS vulnerabily), attack denial of service dispersal / denial of service (DOS / DDOS), or other forms of unauthorized intrusion.

For any operating system, it is necessary to use the latest version with all installed patches and remove unknown services as well as user accounts for remote access control.

US security firm recommends that businesses consider using unauthorized intrusion detection and prevention systems (IDP / IPS) to control traffic. Such a system can be bundled to layer 7 to identify potential threats. For example, the preferred goal of a computer worm attack is a VoIP application with a web interface for administrators and web servers. An IDP device can use multiple methods to detect provocation and prevent harmful traffic by reducing packets from the network.

Numerous gateway implementations can also be seen in the boundary layer. Typically, the server provides user registration, determines the incoming VoIP traffic and transfers calls to the destination. The two main protocols for VoIP traffic are H.323 and SIP. Both use the Real-time Transport Protocol (RTP) for communications. The VoIP application will start a session using a static port to transmit information and then start transferring information using a random port. However, allowing connections to any port is a security risk for deliberate attacks. In such a case, there should be a gateway located behind a VoIP protection firewall application (such as the NetScreen integrated firewall product line). High-throughput firewall devices should also be considered, as network latency will affect call quality.

The firewall should provide an application level gateway to block VoIP traffic, classify the protocol and check which dynamic ports need to be opened by the application. This feature opens a path that allows the information to be transmitted in a specific conversation and closes after the call is completed.

When the user ends the call via IP, the conversation content is still sensitive data, which must not be exposed to the public network. Therefore, IP telephone equipment should support an effective authentication mechanism for registration of VoIP servers. Additional encryption with the use of a virtual private network (VPN) channel should also be applied to both call setup and communication.

In short, VoIP technology provides businesses with new ways to save costs and improve operational efficiency. In order to maximize the effectiveness of this technology, administrators should use a layer-based defense approach to understand network threats and ensure that they can resist attacks.

Xuan Kim