

RE: Protecting the enterprise wireless network

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2008-05/msg00173.html>

- *From:* "Sergio Castro" <sergio.castro@xxxxxxxxxx>
 - *Date:* Fri, 16 May 2008 12:04:39 -0500
-

Hi Zeffy,

They way we set a similar wifi network is using 2Wire wifi access points connected to a Foundry switch, using a VLAN. Access to the Internet is controlled through a Juniper firewall. The switch is configured in such a way that each port connected to an access point knows the mac address of the access point, and will not transmit packets if it detects a different mac address. Thus, if someone hooks up a laptop to the access point's ethernet connection, the switch will not transmit. (Of course a dedicated hacker inside your building could spoof the mac address).

With pretty much any decent firewall you can control the protocols you want to permit AND add business rules such as limiting by time of day, by user, by access point, etc.

As to load balancing, unless you have a 14.4K modem I wouldn't worry about it :)

You probably have several Mbs in Internet access, and your users will only use a fraction of it. Don't spend your budget on traffic shapers unless you're an ISP providing services to corporate customers.

As to wifi security, I strongly recommend using WPA; WEP can be cracked in minutes. As an extra layer of security you may want to limit the power of the access points to cover only the office or meeting room, so packets won't leak outside your physical perimeter. And remember, don't put your company's name in the SSID! :)

As to limiting an attacker, bear in mind that if a laptop is compromised, the hacker will have the same privileges as the user. But maybe I don't understand your last question? Care to elaborate?

Regards,

Sergio

-----Mensaje original-----

De: listbounce@xxxxxxxxxxxxxxxxxx [<mailto:listbounce@xxxxxxxxxxxxxxxxxx>] En nombre de zefferno@xxxxxxxxxx

Enviado el: Viernes, 16 de Mayo de 2008 12:51 a.m.

RE: Protecting the enterprise wireless network

Para: security-basics@xxxxxxxxxxxxxxxxxxxx

Asunto: Protecting the enterprise wireless network

Hey all.

We want to implement a separated secure Internet Wireless network which will be used by guests or users from our company in our building.

We will use Access Points, managed switch and Gateway device that you might offer. The Gateway can be also a Linux (open-source) based solution – it is much better for us :)

We are looking for the following features:

1. Only HTTP, HTTPS, SMTP will be permitted, and it will be great if it is also analyzes the protocol, not just blocking a port.
2. QOS – Some kind of traffic shaping to balance the Internet between all users.
3. We want to limit the access from specific time range.
4. Since there is a chance that a User from our company will accidentally connect the LAN cable without disconnecting the Wireless network. Is there any way to block all access between all connected Wireless users? So that an attacker won't be able to access any of the Wireless clients?

Best Regards,
Zeffy.

_____ NOD32 3104 (20080516) Information _____

This message was checked by NOD32 antivirus system.

<http://www.eset.com>