Firewall-based authentication with Edenwall

WATCHMAN

Instead of granting access by address, the NuFW Netfilter module provides identity-based authentication. The Edenwall firewall appliance comes with built-in NuFW technology. **BY JÖRG FRITSCH AND PATRICK NEST**

Today's firewalls typically reside in Layers 3 and 4 of the OSI model, where they filter traffic on the basis of IP addresses and TCP/UDP ports. To take Layer 7 information into consideration, administrators either deploy proxies or use fairly simplistic patterns. Things get even worse if you need a rule base that gives you filtering on the basis of user IDs. Most models are throwbacks to the 90s and assume that each machine will have a single user only. Of course, this assumption is fatal if you are dealing with terminal servers or Linux.

The open source community has improved the situation recently with two add-on modules for Netfilter [1]. The NuFW module [2] lets you base firewall rules on users and groups rather than on source IP addresses, and the L7 module [3] lets you filter Layer 7 traffic.

France's INL [4] integrates both of these modules in its Edenwall [5] firewall appliance (see the "Hardware" box). The NuFW module is by the founders of INL, and user authentication is the firewall's strongest selling point. We investigated the capabilities of the Edenwall appliances in a simulated production environment in our lab. Edenwall comes with three admin modules that share a web interface: NuConf, NuFace (open source), and NuLog (also open source). The latter is a PHP-based front-end for Ulogd.

In Layer 3, the Edenwall's rule set supports Network Address Translation (NAT), source and target IP addresses, and protocol and port numbers. We had no trouble setting up support for more

Figure 1: The Edenwall device is by Portwell. The CompactFlash module (bottom center) is used for installation and resetting.

complex environments in our lab, such as NAT for ISAKMP (Internet Security Association and Key Management Protocol) or UDP-encapsulated traffic from VPN clients (IPsec with AH and ESP: Authentication Header and Encapsulated Security Payload).

Firewall admins often want to avoid using source IP addresses and would prefer to assign privileges to the user currently working on the machine. This will mean a workaround with any legacy firewall. One common approach is to set the DHCP server up to assign static IPs to machines used by privileged users or groups. The DHCP service identifies the machine by its MAC address. The firewall rule base just has to rely on the MAC/IP assignments being bona fide.

Usually firewalls that authenticate their users do this through manual authentication via http or Telnet. Most commercial products implement this feature by redirecting initial web access by an internal machine to a login page, or requiring users to log on to the firewall via Telnet. The rule set blocks all requests from a machine until the authentication is complete. Only then is its traffic allowed through. This approach is complex for the user and insecure if you have multi-user clients because the setup is based on a single-source IP address. Admins tend to avoid this kind of setup, unless they have no other choice.

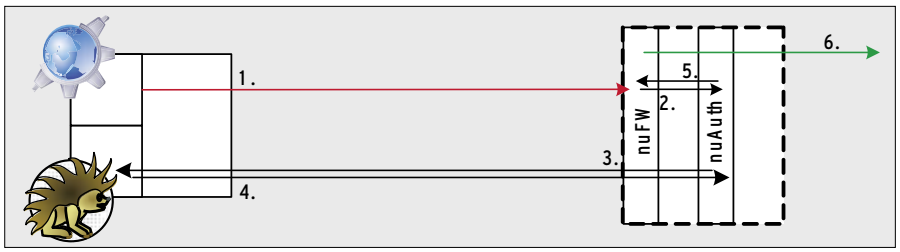

Figure 2: To allow the firewall to identify an internal user and filter connections on the basis of the user's identity, NuFW relies on NuAuth, which in turn communicates with the program installed on the client machine.

Fortunately, this approach is not chiseled in stone by an RFC, and there are more sensible ways of handling things: NuFW uses a program installed on the client computer to identify the user account that originated the connection. NuFW clients are available for Linux and Windows right now, with Mac OS X just around the corner. This means you can set up rules on the Edenwall firewall that reference users or user groups rather than source IP addresses. This combination is completely different, and far more secure and flexible than the legacy implementation that uses Telnet or http/https authentication.

Nicely Integrated

INL has gone to a great deal of trouble to integrate Edenwall into Windows environments. The product will bind with an Active Directory domain (Figure 3); a Windows client is available in addition to the Linux version. In combination with the client, NuFW can determine which user sent which TCP packet (we tested NuWINc for Windows). The overhead is negligible. NuFW's identity-based rules are persistent and follow the user from computer to computer in a mobile world. It is also possible to identify individual users on multi-user machines, mainframes, or terminal servers, and to assign individual rights to those users, even if the packets all originate with the same source IP address.

Edenwall and the clients cooperate to identify a connection:

- A firewall with NuFW and an authentication server (NuAuth) run on the Edenwall appliance; the two services communicate.
- NuWINc is installed on the client; when launched, it connects to the authentication server on TCP port 4130. Edenwall later authenticates the *SYN* packets sent to it via this TCP connection. If multiple users are working on the same host at the same time, each user launches a client.

If an application sends a *SYN* packet to establish a new connection, the packet is first queued by the NuFW firewall software (step 1 in Figure 2). The firewall

Edenwall

Product: Edenwall 2.1 [5] with NuFW 2.0.22 [2]
Function: Firewall appliance with Layer 7 filter and innovative user authentication
Vendor: INL [4]
Hardware: 1 HU rack-mounted by Portwell [6]
Linux: Kernel 2.6.19.4 with Grsecurity patch
License: Edenwall's core components are open source; L7 Filter, NuFW, and the Linux client are GPL'd. The Windows client is proprietary and released under a commercial license, as are parts of the admin front-end (NuConf). NuFace and NuLog are also GPL'd.
Price: The cost of the Edenwall appliance depends on the number of protected users. The Edenwall 50 (for 50 protected users) starts at 4700 Euros, Edenwall 500 (for 500 protected users) weighs in at around 22,000 Euros including hardware by Portwell. The price with IBM P5-505 RISC hardware is about 60 percent higher. Support for one year costs about a quarter of the purchase price, depending on the options.

Hardware

The hardware platform we tested is based on the Portwell NAR-5060 Communication Appliance [6] and, according to the vendor, it is designed for small to mid-sized corporations.

The device includes an Intel Pentium 4 CPU running at 2.8GHz (512KB of L2 cache, FSB 533), 512MB RAM (DDR 400, Timing 3-3-3), and a 1GB CF (CompactFlash) card. Unfortunately, the CF card is not locked in place in its socket, and we were worried about it working itself loose during transport or in extended periods of use.

The chassis is designed to accommodate a laptop hard disk (bottom right in Figure 1). This saves power (and also heat); additionally, laptop hard disks are more resilient against knocks and vibrations. Instead, INL opted for an IDE PATA desktop-sized hard disk (a 40GB Seagate ST340015A).

The unit has a single 250-Watt power supply and a free IDE port and a COM port, neither of which are available to the end user. The COM port on the front of the appliance is disabled.

INL puts the LCD display on the front of the appliance to good use. In combination with the four buttons, it offers useful functions such as shutdown and reboot and another very clever function: An administrator who is inadvertently closed out when a rule set goes wrong can re-enable https administration at the press of a button.

Figure 3: Instead of managing each account, Edenwall references a directory service: The options are LDAP and Active Directory.

NuFW module contacts the NuAuth authentication service to authenticate the packet (step 2). NuAuth uses the existing connection, which was established by the client that sent the *SYN* packet. NuAuth asks the client to produce valid credentials (steps 3 and 4). If multiple users are working on the same machine, the service asks each client in sequence. This gives NuAuth the ability to validate the credentials passed and, if they are okay, to tell the NuFW firewall software which user it is dealing with (step 5).

Depending on the rule base, NuFW decides whether the packet is permitted for the user (step 6). Netfilter then steps in to handle the remaining packets for this connection without additional overhead. This approach is reminiscent of the Ident daemon, but Ident does without authentication; it is designed as an information service and assumes that the client admin is trustworthy. Ident credentials are easy to spoof; NuAuth is harder.

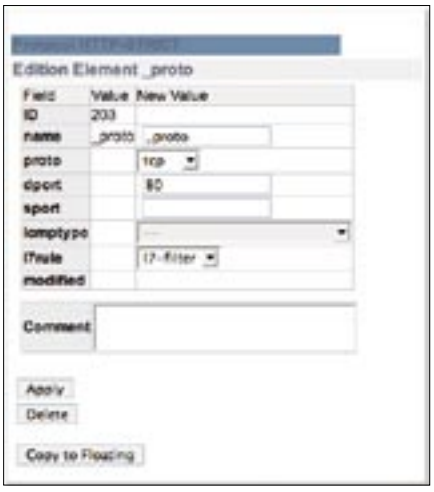

Figure 4: Thanks to an L7 filter, Edenwall can identify not only protocols by their port numbers, but also the data the protocol car-

The Edenwall appliance has two other features that enhance security. With every packet, the NuFW client transmits the path of the application that created the packet. A rule might stipulate that user 1 on TCP port 80 is allowed to access the Internet with Firefox, but not with Internet Explorer. This rule could help avoid the problem of applications (viruses, etc.) phoning home without the user noticing.

This approach is like Checkpoint Integrity [7], except that it does not use a personal firewall on the client PC to block suspicious applications at the client's NIC, and is how it prevents one PC on a network from infecting others with viruses or the like. The path sent by the NuFW client is no guarantee that the application behind the path is not a rogue, but any protection that raises the bar for attackers is worthwhile.

Edenwall also has L7 Filter [3], version 2.9. Its patterns, which you can extend, detect far more protocols than most conventional firewalls. This gives administrators the ability to stipulate that, say, only http is allowed to use TCP port 80 without deploying a proxy (Figure 4). You can also use patterns to disable peer-to-peer software or even VPNs.

Installation

The Edenwall appliance is designed for rack deployment and is just one height unit tall (see the "Hardware" box). After powering up, the appliance is configured to port *GbE1* with an IP address of 192.168.1.1, and it is reachable by https in your browser (Figure 5). The Edenwall web GUI includes three components: Nuconf gives the appliance IP addresses, routes, and other parameters. Nuface is the front-end for NuFW and is where the admin sets up a rule base. Nulog is a front-end for the Netfilter Ulogd. The Edenwall GUI also uses these cryptic terms.

You need Nuconf for the first few settings. The firewall needs at least one IP address on its external interface (always *GbE0*), an internal port, and a directory service with the user database. Edenwall supports Active Directory and LDAP (see the "Edenwall with LDAP" box).

NAT Obstacles

The NuFW security model will not accept modification of the source IP

Edenwall with LDAP

Edenwall's vendor assumes that its appliance will be deployed mainly in Active Directory environments. However, it is possible to run the user database on an OpenLDAP server, although your mileage will vary. The developers have outlined the major steps. The simplest approach is to use the Smbldap-tools [8] and Samba.

1. Install Smbldap-tools, Samba, and Slapd.
2. Unpack *samba.schema* and copy it to */etc/ldap/schema*.
3. Work your way through the HOWTO (typically *smbldap-tools.pdf.gz*) for Smbldap-tools, that is:
4. add a line with *include /etc/ldap/schema/samba.schema* to the */etc/ldap/slapd.conf* file,
5. modify the *sambaDomain* entry in the */etc/smbldap-tools/smbldap.conf* file, and
6. run *smbldap-populate*.

Then add users and set passwords:

```
smbldap-useradd -u 1501 user1
smbldap-usermod -G 'Domain Users' user1
smbldap-useradd -u 1502 user1
smbldap-usermod -G 'Domain Guests' user2
smbldap-passwd user1
```

Finally, the administrator has to ensure that each user belongs to at least one group.

Figure 5: On initial installation, the administrator uses the Nuface GUI to enter critical parameters for the appliance. The external network is always connected to interface GbEO – an unnecessarily inflexible approach.

Figure 6: Nuface is not intuitive when managing your setup. Here, you can see the admin creating a subject that will be used as the source for connections in the ACLs. The authenticated.users subject is a catch-all for any user who has authenticated successfully.

address and port number by NAT en route to the Edenwall appliance. With most source NAT configurations on routers, multiple-source IP addresses hide behind a single NAT IP address. A typical NAT implementation will modify the source port of the the TCP/UDP packets, making it impossible for NuFW to identify the users.

Once your directory service is running, you must do some fine tuning; for example, you have to specify whether you want the integrated Squid proxy to use a virus scanner or whether Edenwall will be your DHCP server. After configuring these settings, the next step is to distribute client software to the PCs. NuWINc is used on Windows; for Linux, there is the Nutcpc command-line client, the Nuapplet Gnome applet, and the Gnome application Nuapp.

Configuration with Nuface

In the configuration phase, Nuface compiles access lists (ACLs) from subjects, resources, protocols, applications, and L7 filters. All of these elements in turn compose what are known as working elements. What Edenwall refers to as a *Subject* is in fact the source of a packet (a user or an IP address; Figure 6); resources are packet targets (always an IP address, never a user). The idea of an L7 filter is that it will not just open TCP or UDP ports after a fixed pattern but will actually discover which protocol is using the port.

The Nuface GUI is recalcitrant in many cases. It seems to be fairly difficult to tame Edenwall's many functions to an extent that the procedures are intelligible to admins. Two things really bugged us in our lab: a Cleanup ACL is only possible in Layer 3 (any – any – any – deny – log, to deny and log any illegitimate access attempts). And it is very difficult to put this ACL at the end of the rule base in the course of setting up other rules. You can only change the ACL order in specific GUI views by dragging and dropping, and it is hard to say what the different views are intended for.

Web Interface

The web interface is mainly to blame for the huge amount of time that we spent learning the ropes and troubleshooting the setup.

The configuration process is very plain and does not use intuitive icons. In many cases, we were unable to modify ACLs that we had set up: Our only escape route was to delete and start again, and it took a lengthy excursion to the manual before we discovered that user identities are accessed as working elements *nufw_*. These superficial weaknesses are a pity because the idea behind Edenwall is far superior to that of a conventional firewall.

Very much to our surprise, the vendor states that Edenwall can handle certificate and smartcard-based user authentication. INL has developed a new module dubbed NuPKI for this purpose; the module will be included with the next Edenwall release, along with site-to-site VPN support. Right now, the French Ministry of Education is currently pilot-testing NuPKI. INL is even taking on IPv6 in its NuFW 2.2 release, thus future-proofing the product.

Inner Values

Edenwall's weaknesses are mainly in the GUI, which is cluttered and hard to use. The appliance hardware is also unconvincing. Despite the issues and weaknesses, and the two bugs that made it difficult to get started, NuFW and the Edenwall appliance are on the right track. For years, vendors have been trying to establish more understanding and acceptance for identity-based systems and privilege management. Edenwall offers a promising alternative. ■

INFO

[1] Netfilter: *http://www.netfilter.org*

[2] NuFW: *http://www.nufw.org*

[3] "Beyond the Port: Blocking Protocols at Layer 7 with the L7 Patch" by Jörg Harmuth, *Linux Magazine*, March 2006, pg. 62

[4] INL: *http://www.inl.fr*

[5] Edenwall: *http://www.edenwall.com*

[6] Portwell: *http://www.portwell.com/products/detail.asp?CUSTCHAR1=NAR-5060*

[7] Checkpoint: *http://www.checkpoint.com/products/integrity/*

[8] Smbldap-tools: *https://gna.org/projects/smbldap-tools/*