Proxy Server Implementations

Table of Contents

Proxy Servers................................................................................................................................... 2
Proxy Service Firewalls.................................................................................................................... 4
Proxy Servers................................................................................................................................... 5
Proxy Service Firewalls.................................................................................................................... 6
Proxy Servers -1 .............................................................................................................................. 7
Proxy Servers -2 .............................................................................................................................. 8
Reverse Proxy................................................................................................................................. 10
Notices .......................................................................................................................................... 12
**082 When we look at proxy servers—we're doing things on behalf of the user. That's really what we're doing here.

So when you look at the diagram here what you'll see is is that we have this internal group right here. What is this internal group? Well we don't know. But when they want to get out to the internet and they want to go to the internet, what we say is: Go through the firewall and go to this proxy server and let it examine all of your communications and your traffic.
But a proxy server does nothing but on behalf of. Most proxy servers that when we come from the internet and communicate-- most proxy servers are designed to protect our web server itself. And they say: Okay that proxy server, when you want to go to that server, I'm going to make certain conditions true and I'm going to look for inspect certain things before I pass it on to the web server.

It's possible to come from the inside and actually go to this web server and have a different set of rules communicating for you.

When we use the proxy servers to go to the web, what we might do is we might say: Hum those people over there, well they can't go to any shopping sites and they're not allowed to go to any fantasy football sites; we're not allowing any of that activity or this inappropriate activity; because our policy states that we don't allow people to do shopping online or whatever that is.

Today with the proliferation of end-user handheld devices, BYOD, this is less and less necessary. And I find it so; especially with- also where they're setting up wireless. But we still have to look at the old way that this was set up.
Proxy Service Firewalls

Act as proxies for internal hosts when connecting to the Internet

Circuit level gateways
  • Operate at level 5 of the OSI model
  • Stores flow information for TCP connections

Application level gateways
  • Checks layer 7 of the OSI model for services and filters based on packet contents
  • Slower because of deep packet inspection

**083 Remember that proxy service firewalls come in two flavors: circuit level and application level. But these two things have been collapsed together in most cases.

Circuit level definitely operates at Layer 5. It looks for those connections, those sessions, and says: These are appropriate types of things to do.

Other things at Layer 5 might be-- Layer 5 and Layer 6-- might be Presentation type protocols where we say the circuit-level proxy will not allow you to do streaming video; something like that.
That happens very often on the planes today where the circuit-level gateways on the airplanes when you’re trying to surf the internet will go: Oh he’s trying to load up the codec for blah-blah-blah-blah-blah to do streaming video; we’re going to eliminate that.

Now we could do that at the Application layer if we wanted to. Circuit level, you have to go through it.

So if you look at our previous diagram here.

**Proxy Servers**

Prevent users from directly accessing web servers, deterring malicious activities

**082 You’ll see that in this case**
there is no other way to get to the internet. You have to go through the proxy server. So this would be definitely a circuit-level proxy server.

Proxy Service Firewalls

Proxy Service Firewalls

Act as proxies for internal hosts when connecting to the Internet

Circuit level gateways
  • Operate at level 5 of the OSI model
  • Stores flow information for TCP connections

Application level gateways
  • Checks layer 7 of the OSI model for services and filters based on packet contents
  • Slower because of deep packet inspection

**083 Application level proxy server does things a little bit differently. It says: Let’s look at the application that you’re trying to get to; let’s do a little- a little deeper inspection.

Now the problem is is when we do a little deeper inspection, as we get up layers, this is going to be cost prohibitive because it’s slower.
Proxy Servers -1

Establishes connection on behalf of a client
Shields a client from direct communication with a server
Isolate internal networks from external networks
  • Masks internal hosts from being viewed externally
Saves bandwidth by caching web content
Enforces security policy by restricting sites a client can visit

**084 Remember, a proxy server does one thing very well. It does things on behalf of the client.

And what this does is this isolates the external host from the internal host in a way that won't allow the viewers to see them, abstracting all that communication. That's really elegant.

It also can-- not always-- will do web caching content. So where we'll say: Oh that host has already been to that location; here, here's that webpage already.
With the dynamic nature of webpages today, the likelihood of caching that information is a little bit lower, unless you've got a really big audience.

Now what's really nice about this tool, this proxy server, is it can look at the site that you're going to, and it can limit that communication. It can say: I don't want you to go to these sites or those sites.

**Proxy Servers**

**Proxy Servers**

Web and Email Proxies are most common

Web Proxy Server

- Can filter on URL, inspect content, and detect malware
- Can cache pages for improved bandwidth utilization

SMTP / Email Proxy

- Can filter SPAM, Viruses, etc.
- Can control allowed recipients and senders

**085** Now we could do web proxies-- and that's what we've been talking about so far. But we could also do email proxies.
So when we talk about email proxies, that would stand in front of our mail server and it would scan for things like spam and viruses.

Think about it like this. That SMTP email proxy could say: I’m going to take all the mail from the internet. It’s not going to my real mail server. I’m going to take all of it here; and yes I accept mail for that.

And then every attachment that was sent there, it could do all the scanning for all those attachments; and if those attachments were bad, or suspect, it could remove them and add a link to the email that says: Your attachment was suspect; we’re not allowing it through.

More sophisticated email proxies will actually inspect the header information of the file and say: Yes you’ve changed that into a txt file but it’s really a PDF; because I can look at the header information inside the actual data file itself and say: That’s really a zip file and it shouldn’t be allowed through.

So in these cases what happens is is those proxy servers will catch it, quarantine it.

What I like-- it’s really elegant-- in some is they will catch it, set it over here, create a link to it; and then send it on. And when it sends it on to its destination, it also sends an email to that person’s manager to say: This link is- this is link is here for that particular email; do you approve or disapprove?
Now that's a very sophisticated system. But it happens.

And that's a great use of proxy servers.

**Reverse Proxy**

Reverse Proxy

Accepts requests from clients on the external network on behalf of the servers in the DMZ

Masks the servers (while traditional proxies mask the clients)

Makes it more difficult for attackers to acquire data on server behind the proxy

**086 There is something called a Reverse Proxy; which now what we've done is we've turned this around. In this case with the reverse proxy it masks the actual servers.**

Traditionally we would mask the actual clients themself. And so when we mask the server, what we can do is we can make decisions based upon: Well we really don't want you
from the outside world going to this web server and attacking it in this way.

Oh you’re sending in SQL injection; and the standard signature for SQL injection is where 1 = 1. I’ve got that in my list here. I’m sorry, I’m not going to allow you to do the connection.

Oh you’re doing a standard query where customer number = you. Oh okay I’ll pass that through.

And that’s a reverse proxy. It’s proxying our web server to the rest of the world.
Notices

© 2015 Carnegie Mellon University

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

This material was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.

THE MATERIAL IS PROVIDED ON AN "AS IS" BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT® is a registered mark owned by Carnegie Mellon University.