http://phoneboy.net/ Go JUN JAN FEB
29 captures 02
31 May 2002 - 2 Jan 2014 2005 2014 2015
About this capture

PhoneBoy's Security Theater

Views on Information Security from the guy who brought you ye olde PhoneBoy FireWall-1 FAQ

Dameon Welch-Abernathy

Parent, Writer, Podcaster, Coffee Achiever, VoIP/Telco Curious, C-List Information Security Celebrity, and Mobile Phone Connoisseur residing in Gig Harbor, WA, USA.

You might know him better as PhoneBoy.

Blast from the CHKP Past: Can't Talk to Translated IP from Internal Net

It's pretty obvious from looking through the number of 404s I'm seeing in Google's Webmaster tools that a lot of pages still link to old stuff I wrote about Check Point FireWall-1. I'm actually trying to "fix" these 404s now by resurrecting some of the old content. Not updating it, of course, but at least making the links point to something semi-useful, if historical.

This is one of those articles, obviously not at it's original URL, but the original URLs will point here. What amazes me about this particular article is that it's still relevant today as NAT really hasn't fundamentally changed in the Check Point products for some time. The basic concepts are still the same, too, and other than the implementation details, is probably relevant for other security products, too.

Bottom line: NAT only works if the firewall is in the path of the communication. How do you know? Follow the bouncing packet, otherwise known as Troubleshooting 101.

Hit the break to see this old FAQ in all its ASCII network mapped glory.

Read more »

Subscribe by email »
We'll email you when there are new posts here.

Upvote 0

Tweet

Tags

check point 26
nokia 9
wifi 6
mobile phones 6
iskoot 5
social networking 5
byod 5
skype 4
facebook 4
voip 3
See all 66 tags »

Sites I Like
The PhoneBoy Blog
PhoneBoy's Personal Blog

0 responses // Posted about 1 month ago

The TSA and A Lesson in Data Loss Prevention

From PhoneBoy Speaks Ep 305: Threat? What Threat?

> In sealed court documents accidentally leaked on a US Federal government website, the US government basically admits that there has been no attempted domestic hijackings of any kind in the 12 years since 9/11. Furthermore, at least as of mid-2011, terrorist threat groups present in the Homeland are not known to be actively plotting against civil aviation targets or airports.

It gets better. Jonathan Corbett, the guy who has been challenging the feds on the constitutionality and the effectiveness of the TSA in the courts, was told by the US Justice Department to take down his comments about a sealed document he wasn't allowed to talk about, but the government themselves posted the unredacted version on their site and other sites made it public.

The same is true for Corbett's comments about those documents, the Justice Department asked him to remove from his site, but they apparently forgot to tell Google as it was still in their cache!

This is a clear demonstration of what can happen if confidential data inadvertently leaves your organization. Clearly this unredacted, sealed legal brief should have never been made public. Thankfully, in this case, it was, but surely some folks in the US Government weren't happy with this lapse. Neither would your employer if it's your company's secret plans for world domination that got leaked.

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

Likewise, if you inadvertently leak information on your own website, or someone else does, even if you can manage to get it taken down, Google takes a while to forget it saw it. The rest of the Internet won't necessarily forget, though. Ever.

So what are your plans for Data Loss Prevention in your organization? Are you even employing any DLP technology? Is it actually catching real incidents of data loss or is everyone going around it?

I'm not saying DLP is a panacea or 100% effective, but if you're not doing it, then you don't have any idea where your corporate information might end up.

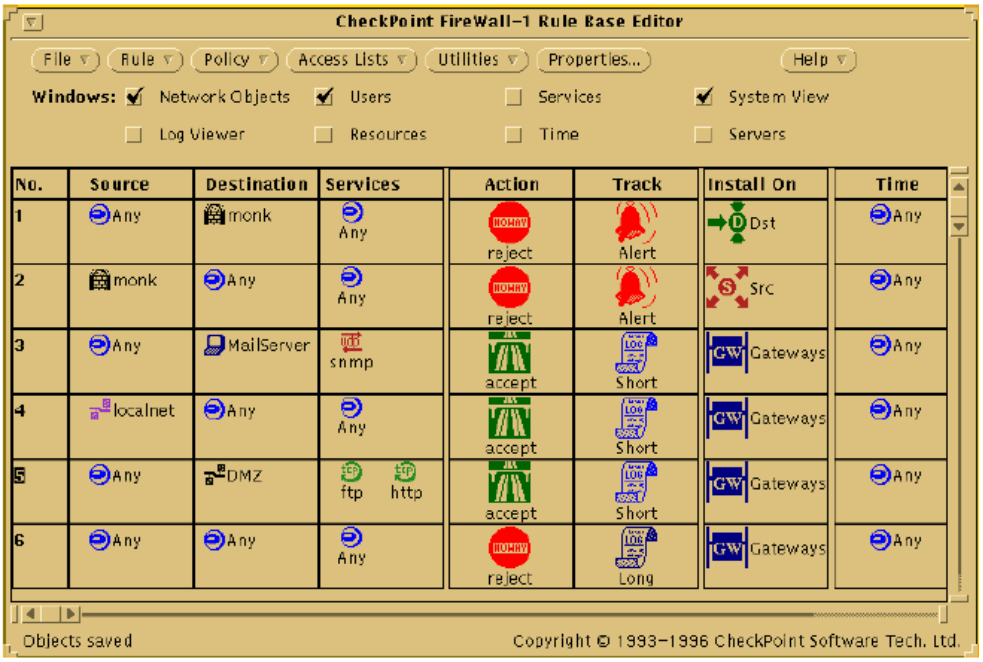
Upvote 0

Tweet

0 responses // Posted 3 months ago

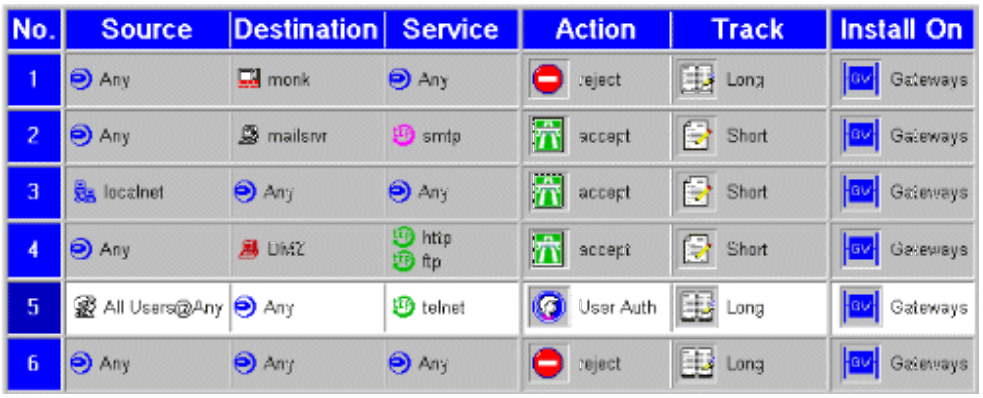
FireWall-1 User Interface from 3.0

If you ran Check Point FireWall-1 on SunOS or Solaris, you probably remember this screen:



This is a screen capture from fwui, the management interface for FireWall-1. Actually FireWall-1 2.0 and 2.1 looked like this too.

Meanwhile if you ran the management interface on Windows, you were presented with something like this:



You could actually run the firewall on Windows NT as of 2.1, though it took until 2.1c until it was reasonably stable.

Actually you could run something that looked like the Windows UI on Solaris with Motif, which Check Point charged extra for. Eventually the Motif and the OpenLook GUI were deprecated and what we now refer to as SmartDashboad only runs on Windows.

And, of course, there are far more GUI clients these days--about a dozen or so if I remember correctly. But then again, the product does so much more today than it did back in the mid 1990s.

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

And yes, I remember those days quiet fondly.

Upvote 0

Tweet

2 responses // Posted 5 months ago

Blast from the CHKP Past: Can't Get Putkeys to Work

For those of you who never had to work with Check Point FireWall-1 4.1 and earlier, you're lucky you likely never EVER had to use putkeys.

The fw putkey was used to establish authentication between the Management and Firewall modules. The problem was: the authentication would frequently break. Especially in larger, distributed environments. Often for reasons that no one outside of a few developers in Tel Aviv never fully understood.

The eventual replacement for fw putkey was SIC, which was added in FireWall-1 NG (5.0). It is based on certificates and is way easier to set up. It's also far less prone to random breakage.

The following classic article is presented for nostalgia purposes only. Hopefully no one in their right mind still needs this article, which was very popular on my FireWall-1 FAQ back in the day. It was the collective wisdom of my peers and my own experience as of around 2000 or so.

Read more »

Upvote 1

Tweet

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

2 responses // Posted 5 months ago

Moving The Security Theater Elsewhere

I decided to move PhoneBoy's Security Theater off of Wordpress onto Posthaven.

On the plus side, it's one less instance of Wordpress to maintain. On the minus side, I had to copy/paste the old articles in since there is no way to import Wordpress as of yet. But it was under 100 articles and it was kind of nice to see my thoughts on security from the last several years again.

The reality is, the threats haven't changed. We've had to evolve the tools in order to address increasingly complex threats. You can look at Check Point's own product evolution to get a sense of that.

Also, the basics haven't changed. A lot of security risks can be sufficiently mitigated by properly segmenting your networks, using sufficiently complex passwords that are unique, proper monitoring of the logs of your security devices, and keeping your software up-to-date with the latest security patches.

Tags administrivia

Upvote 0

Tweet

0 responses // Posted 5 months ago

Fun with Compliance

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

Earlier this week, I hung out with Jeremy Kaye, one of our in-house compliance experts at Check Point:

http://www.youtube.com/embed/uvL6HdlrW08

While I've been doing InfoSec for a while, or at least working in companies that sell InfoSec products, compliance isn't something I've had a ton of direct experience with. Sure, Check Point customers used our products to help meet various compliance regulations, but until Check Point acquired DynaSec in 2011, there wasn't a team inside Check Point dedicated to this topic.

While we had some technical challenges with the Google+ Hangout itself (and it was the first one we did at Check Point), I think the conversation with Jeremy went fairly well. The questions I asked where ones I've always wanted answers to. Like, what good is compliance? Why does it seem like compliance is in the eye of the auditor? Why so many regulations anyway?

The big takeaway for me from this conversation is that security should drive your compliance efforts, not the other way around. Because chances are, if you have a strong information security program in place already, compliance is pretty straightforward, no matter which regulations you have to comply with.

Tags compliance

Upvote 0

Tweet

0 responses // Posted 6 months ago

Check Point 600 Appliance: Big Security for Small Business

Ok, this is a completely shameless plug for my employer. But it's

really big. And really small at the same time. And my take on it, which wasn't cleared with the marketing folks, and thus my, albeit biased, opinion.

The Check Point 600 Appliance, which was announced today at Interop, represents Check Point's refreshed entry into the SMB Security space. It provides the same security functionality you'd find in Check Point's larger appliances in something that fits into an SMB--both in terms of form factor and price. This includes Check Point's award-winning IPS, App Control, URL Filtering, Anti-Virus, Anti-Spam, VPN, oh and don't forget the firewall :)

If you're familiar with the SG80, which Check Point launched a couple years back, the new 600 Appliance looks a bit like that, though the internals are slightly different from the SG80. There are standard USB ports, Express Card and SD-card slots in the 600 as well as optional WiFi and ADSL ports. It also includes a revamped Web Interface that incorporates functionality from the UTM-1 EDGE and Safe@ appliances allowing full management of the security policy across all Software Blades.

Under the hood? It's nearly the same code that runs in the larger Check Point appliances--Check Point R75.20 running Embedded Gaia, to be exact. When you SSH or serial console into the appliance, you are presented with clish, which functions similar to how it does on one of the larger appliances. You can also drop into Expert mode for more advanced debugging, which again, works very similar to how its done on the larger gateways.

The main differences between the 600 and the Check Point 1100 Appliance, which was announced a few weeks ago are:

- Lower price: List price of a 600 is roughly $200 cheaper than the comparable 1100 model.
- Chassis color: Bright orange, like the old Safe@ boxes.
- Central Management: While the 1100 can be centrally managed with standard R75.46 or R76 management (standalone or Provider-1), the 600 can only be centrally managed by Check Point Cloud-Managed Security service.

In any case, I am truly excited about this as finally, SMBs can finally get the same Enterprise-grade security that the Fortune 100 relies on for a fraction of the cost--starting at $399.

Check Point's SMB Portal has information about the new appliances as well as how to acquire them.

Tags check point smb

Upvote 0

Tweet

0 responses // Posted 8 months ago

Check Point 2013 Security Report

When I was in Israel at the end of 2012, I was talking with the folks putting the finishing touches on the Check Point 2013 Security Report. Of course, since then, the report has been formally released and you can now read it for yourself. Here's a video preview of what you'll find in it:

Some of the data gathered for this report was related to the 3D Security Reports Check Point generated for customers during 2012

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

where we took a Security Gateway and either ran it in-line (in bridge mode) or plugged it into a mirror port on a customer's switch. It's worth pointing out that, in many cases, *a competitive security solution was already in place* and the Check Point Security Gateways were seeing stuff the other solutions were missing.

Other data for this report also came from SensorNet, ThreatCloud, and results from our Endpoint Security Best Practices Report, which is a great way to find out if your Windows PC is configured according to our Best Practices.

The most surprising statistics?

- 63% of the organizations surveyed had at least one malicious bot in their network.
- 43% of the organizations surveyed had traffic to/from an anonymizer service.

Of course, if you're knee deep in the security space, 0% of this is news to you.

Tags check point

Upvote 0

Tweet

0 responses // Posted 9 months ago

How to Not Be Like Burger King. Or Jeep.

On today's episode of PhoneBoy Speaks, I discuss how to prevent your Twitter account from being hacked like Burger King's account was. And today (after I recorded this episode), Jeep's Twitter account was also hacked. Of course, I can only do so much in a 5 minute podcast, and the topic itself of choosing strong passwords--and getting users to actually do it--has been covered ad-infinitum

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

elsewhere.

The fact is, passwords are not very secure. To be secure, they must be both long (number of characters) and high-entropy (more random, the better). Humans, as a lot, are not able to remember passwords that meet both of these requirements, so they cheat. They either write the passwords down, they use password management tools like LastPass or 1Password, or they just choose stupid passwords--usually the latter.

The best compromise I've seen is actually the Password Haystacks method that Steve Gibson came up with. All other things being equal, as long as you use all 4 different types of characters in your password, length wins. Because when it comes to guessing passwords, there is no such thing as "close."

Of course, if the password itself can't be guessed, surely you can compromise the password reset process, as was done with Mat Honan's widely publicized pwnage. Hopefully we can strengthen that too, but companies--especially ones that cater to non technical people--rarely err on the side of secure.

Tags social networking passwords

Upvote 0

Tweet

0 responses // Posted 11 months ago

Securing Data in the Cloud

On my podcast PhoneBoy Speaks today, I discussed (very briefly) the idea of doing information security in the cloud. Surely, I could talk and write volumes on the subject. I've even given presentations on the subject.

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]

The reality is, virtualization changes the game in so many ways that it's hard to know where to begin. That said, my view starts with the most basic question: what is it we're ultimately trying to protect?

The good news is that the answer is still the same, regardless of whether physical servers on your premises are involved or some cloud services provider is: it's the data. Your job in information security is to ensure the Confidentiality, Integrity, and Availability of data to prevent Disclosure, Alteration, or Destruction of said data.

The bad news: the cloud makes this job a lot harder. The reality of bring your own device (BYOD) also makes this harder for much the same reason--less opportunities to inject the necessary controls to ensure data doesn't go where it's not supposed to.

Of course, it's not just about protecting the data. That part is actually pretty easy. Protecting in a way that allows it to be used in a convenient way, now that's a lot harder.

Tags cloud byod

Upvote 0

Tweet

0 responses // Posted 11 months ago

1 2 3 4 5 … Next › Last »

https://web.archive.org/web/20140102143305/http://phoneboy.net/[9/17/2018 1:50:49 PM]