Top 10 Considerations for Securing Private Clouds

JUNIPer NETWORKS

Who’s that knocking at my door?

If you know who’s accessing your cloud, you can head off many problems before they turn into disasters.

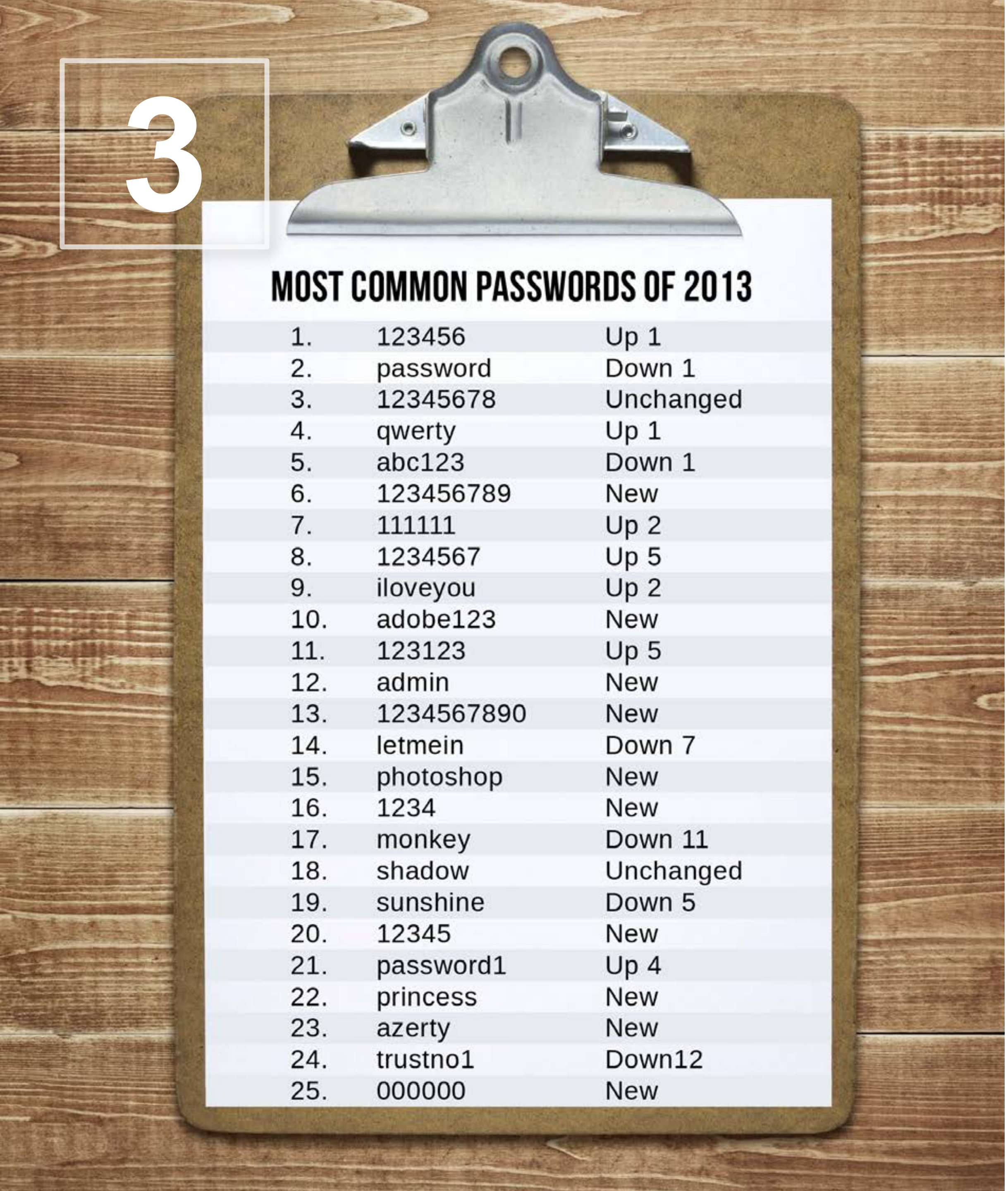
You should ensure easy access for your trusted users — but make it hard for everyone else. The lock on the front door of your home is there for a reason: to let the good guys in, and keep the bad guys out. But you must balance security with convenience (I know, story of your life). Deploy difficult-to-guess usernames, strong password protection (more on that later), two-factor authentication, and authorized devices to strengthen that lock.

2

Help the honest stay honest

Once the good guys are inside your cloud, keep them honest by identifying their roles — and by making it impossible for them to wander into places they don't belong. Engineering has no business getting into financial systems. Finance should have very little to do with dev environments. Enforce this with role-based access control, segment your cloud network appropriately, and encrypt sensitive content. Put temptation out of reach, and you'll prevent a lot of trouble.

3



MOST COMMON PASSWORDS OF 2013

1.	123456	Up 1
2.	password	Down 1
3.	12345678	Unchanged
4.	qwerty	Up 1
5.	abc123	Down 1
6.	123456789	New
7.	111111	Up 2
8.	1234567	Up 5
9.	iloveyou	Up 2
10.	adobe123	New
11.	123123	Up 5
12.	admin	New
13.	1234567890	New
14.	letmein	Down 7
15.	photoshop	New
16.	1234	New
17.	monkey	Down 11
18.	shadow	Unchanged
19.	sunshine	Down 5
20.	12345	New
21.	password1	Up 4
22.	princess	New
23.	azerty	New
24.	trustno1	Down12
25.	000000	New

Passwords are still important. Really.

Now and probably forever, we'll be dealing with passwords. So have a strong password policy. It's really important. Enforcing the policy is paramount. Here are the 25 most common passwords of 2013, along with the change in rank from last year, according to CBS News: http://www.cbsnews.com/news/the-25-most-common-passwords-of-2013/

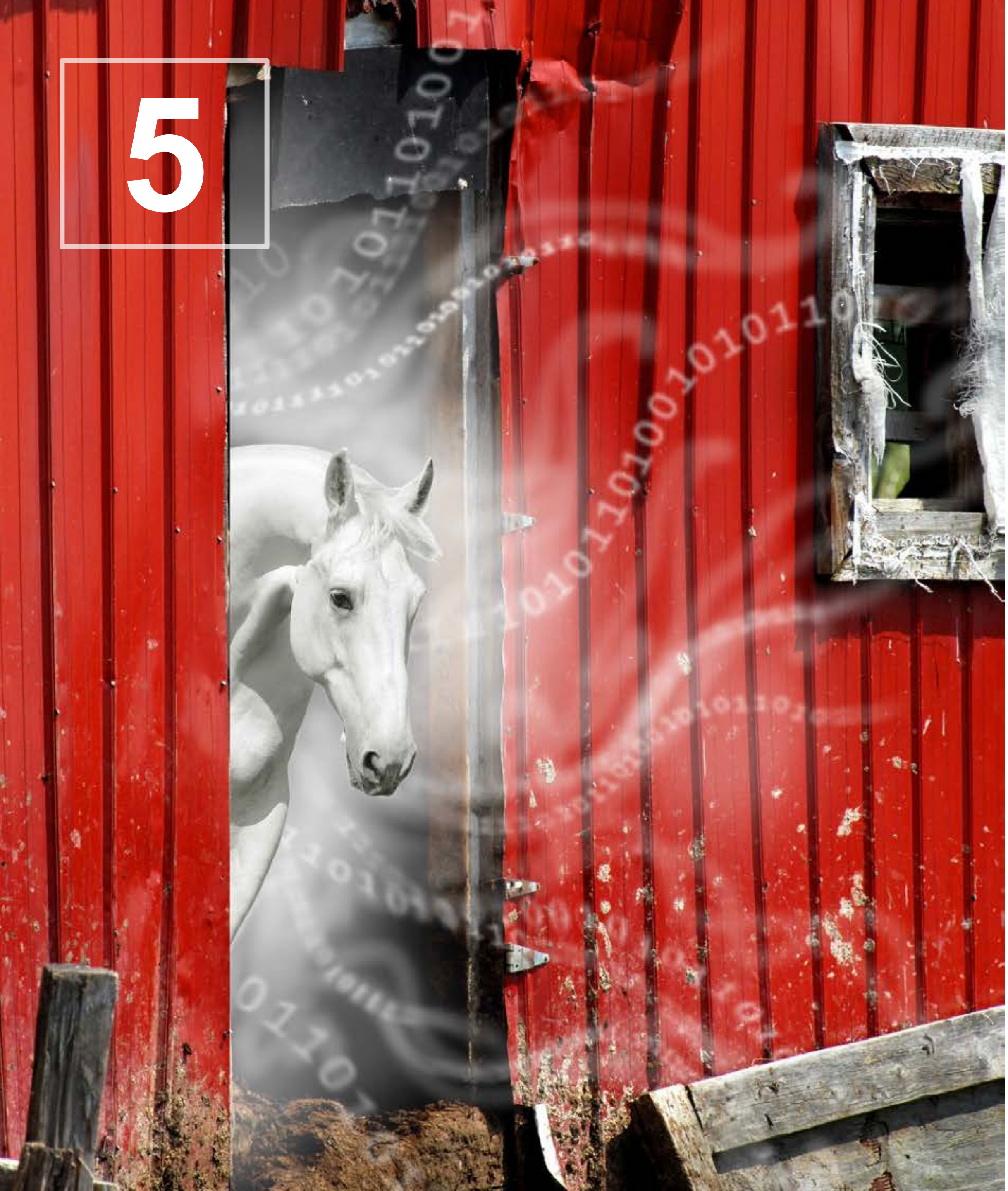
OK, really? 123456? Monkey? Princess? Really? Your users must be more advanced than this. Or are they? A dictionary brute force attack is a very common way for hackers to simply walk into your cloud. Enforce a strong password policy. Really.

Scrub, scrub, scrub

Inspecting traffic that enters your cloud is essential. Use the latest technologies on the market to scrub through packets so you always know what is traveling through it.

Traditional firewalls are a great start. Next-gen firewalls offer user- and application-awareness as well as threat protection and content security. And even think about protecting against unknown malware attacks with sandboxing technologies.

JUNIPER
NETWORKS


5

Shut the barn door *before* the horse leaves

Just as you should inspect traffic coming into your cloud, you should know what’s leaving it.

You may store sensitive information, such as lists of credit cards, social security numbers, or company IP. Consider data-loss prevention and database encryption, especially if you store sensitive information — yours or your customers.’

JUNIPer
NETWORKS

Knowledge is power

Knowing where people are coming from can make protecting your cloud much easier. Think about it…if you know you will never do business with a certain country, you can simply block all IP addresses coming from or going to that country. How easy is that?

However, IP addresses happen to change all the time. To adjust for that, your enforcement points (aka firewalls) must adjust as well with intelligence from a Geolocation (geographic location) IP feed source. Make sure your firewalls support GeoIP to make the best decisions for someone to access your cloud.

Source: AMC

Breaking Bad

Another nightmare is an attack in which your cloud is an involuntary participant of a botnet. Infected servers in your cloud can be remotely controlled by Command and Control or CnC centers (a bad guy's command post) into sending volumes of unwanted data out to unsuspecting victims. These attacks not only cripple the victims' networks, but they damage your company's reputation and increase your bandwidth costs in the process. Now you are "breaking bad," — that is, becoming the bad guy — unknowingly.

Consider Security Intelligence solutions that collect CnC addresses and deliver them to enforcement points. Now you can block evil remote commands from ever getting to the infected servers in your cloud.

JUNIPer® NETWORKS

8

Sleep like a baby

Feeling good about your security posture might just let you sleep at night. Things like version control for hardware, software patches, and event alerts all contribute to ensuring some amount of confidence for you (and for management). A few well-placed IPSs (intrusion prevention systems) integrated into your gateways can buy you critical time between when you discover a vulnerability and when you're able to patch vulnerable systems. It's all about having the right security posture so you can sleep like a baby.

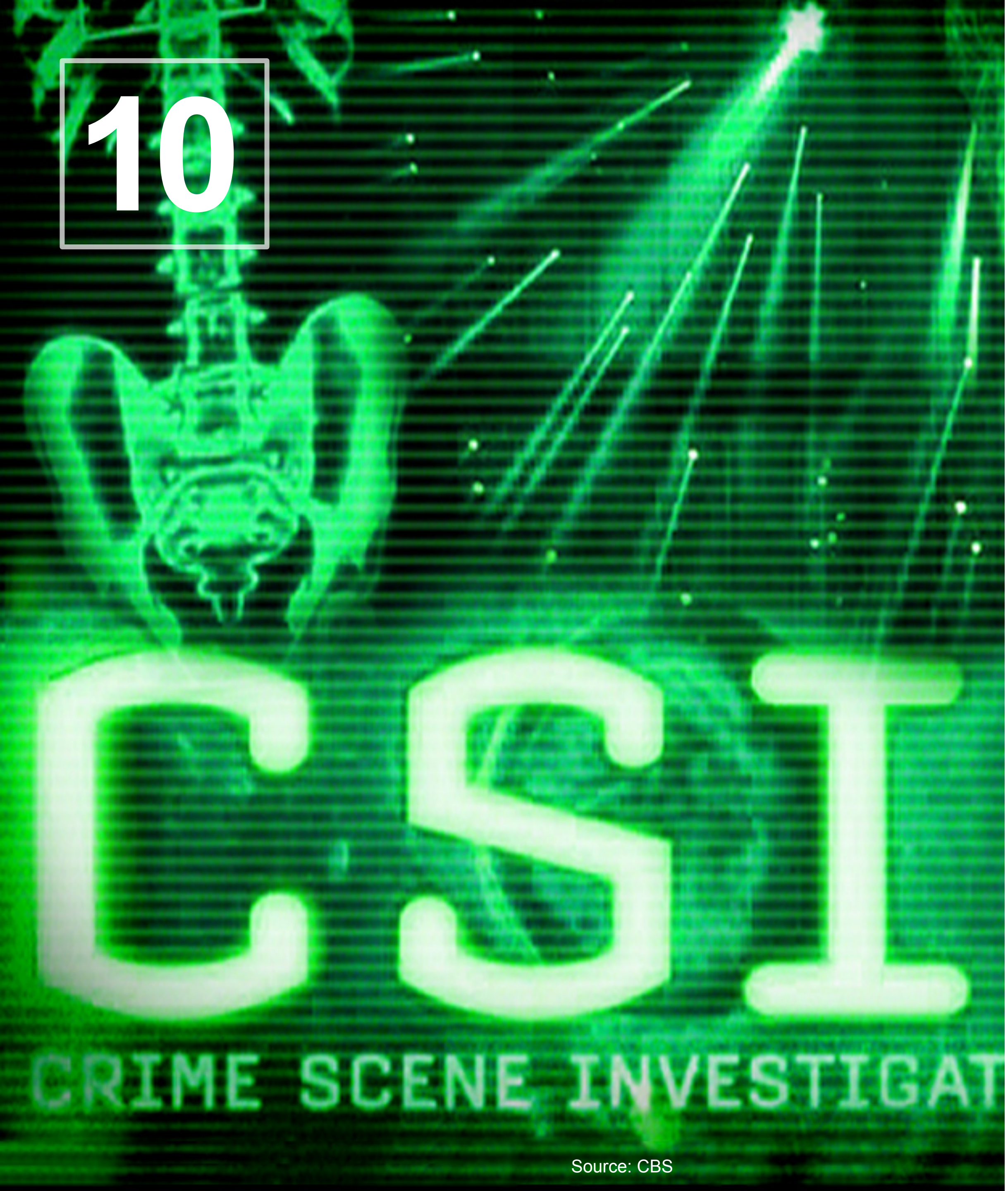
JUNIPER NETWORKS

9

Let’s get physical, physical (and virtual)

Building out good security policy is a long, arduous task. It takes a long time to get policies right. And once policies are solid, changing them is risky in itself. Moreover, the change-control process can be difficult. So once your security policies are in place, make sure you can share those policies between both physical and virtual infrastructures in your cloud. When spinning up a new virtual firewall, the policies should be able to match those of the physical firewalls, and all managed centrally.

10



Source: CBS

Investigate the crime scene

There are two types of companies. Those who have been hacked, and those who have been hacked but don’t know it. Have a plan that assumes you’re always under attack. Have a plan that says if/when you are attacked, who gets the first call. Second call. Have a plan to minimize the damage.

But don’t clean up too fast. Learn how it happened while cleaning the aftermath — after an attack, keep the data, and investigate, CSI style. Learn from the attack. Investigate deeply. And fix what made you vulnerable.

Learn more at www.juniper.net/security