dinCloud

At dinCloud

Cloud Security is Top of Mind

At dinCloud, Cloud Security is Top of Mind

A set of surveys by the international IT services company, the BT group, revealed the major dilemma facing the IT community concerning cloud and cloud deployments. 79 percent of respondents said they're adopting cloud storage and web applications in their businesses, but in another study by Intel, “What’s holding the Cloud Back”, 80% of the respondents of IT executives “identify security and ease of deployment” as the primary obstacles to cloud computer adoption.

This paper will start the discussion on itemizing the steps that dinCloud has implemented for the purpose of cloud security for all customers via a hosted private cloud.

Going to the cloud is the obvious part – but how to do you do it securely?

As the BT survey states, almost 80% of medium and large - sized enterprises are moving to the cloud for storage and web – but, at the same time, the IT community does not feel the industry has resolved the security issues.

dinCloud has heard these requests and have taken the time to address these issues by breaking down the security challenge in three parts:

- Protect from outside threats to dinCloud
- Encrypt and monitor activity once users have entered the dinCloud trusted network
- Provide resiliency and backup capabilities to dinCloud customers

Outside threats will not decrease – they will increase

In 2014, we saw hackers go where the money is - public clouds. Companies running in the cloud, from big names like Apple iCloud and eBay to smaller names like EverNote and SnapChat, saw direct and targeted attacks on their enterprises. Research showed that specialized tools were created for these attacks. Researchers also discovered that the tools hackers used and are still using are readily accessible and being exchanged openly. The RAND Corporation reveals cyber black markets have reached unprecedented levels of economic maturity and growth. Their 2014 report had the following findings:

- The Cyber black market is not that much different than the traditional market – with participants communicating through various channe ls to place their orders and obtain products
- The cyber black market mirrors normal evolution of markets in both innovation and growth
- For many, the cyber black market has become more profitable and thus replaced markets such as illegal drug trading

To this end the need for the cloud will increase, not decrease. There is no way a small or medium sized enterprise, especially in sectors like financial services, education, and medical, can keep up with these attacks.

dinCloud Secures its Customers by first Mitigating the outside attacks

dinCloud realizes that to meet the objective of a secure cloud it needs to understand, inspect and, when necessary, block suspect external traffic. To achieve this mission, dinCloud armed itself and its hosted customers with the latest tools for enterprise grade security.

For starters, dinCloud has IP Reputation installed across all segments. dinCloud utilizes Threatstop to analyze and rank all external traffic that flows in and out of its secure data centers. IP Reputation not only keeps a record of malicious addresses but can also process request from the sites in real time.
These tools input and collate malicious attacks from thousands of entry points across the globe to provide real time analysis of the sources that are entering the network. All of this work is done without slowing down the traffic of dinCloud customers.

By evaluating network requests and dropping sources that come from known malicious sites, dinCloud updates its source IP tables every 20 minutes and blocks more than 70,000 malicious packets a day.

Many new attacks involve DNS poisoning, which is initiated by modifying the legitimate IP address of a domain with a rouge address that the malicious party intends. Usually, the malicious party then loads either a worm, spyware, web browser hijacking software or other malware from this rogue site. The results of these attacks have implications that can affect millions of devices.

In addition, the DNS entry can simply be erased from the DNS caches – thus effectively "firewalling" users from the modified site names. This is one of the mechanisms the "Great Firewall of China" utilizes to block sites like Twitter for ISPs in their control. A missing or erroneous DNS entry effectively blocks the user from accessing the intended site.

dinCloud Utilizes Latest Security Tools

This is why dinCloud utilizes the most advanced DNS system in the world. dinCloud utilizes a core IP Anycast Routing DNS architecture that has provided our clients with a 99.9999% uptime history. The use of IP Anycast Routing ensures our network is of the highest quality as well as fully redundant with no single point of failure. A 99.9999% overall uptime history is something that very few providers worldwide can claim.

dinCloud utilizes IP Anycast Routing because it provides global load balancing, redundancy, decreased latency, and a true distributed response to denial of service (DoS) and distributed denial of service

(DDoS) attacks. Using IP Anycast Routing, each name server IP corresponds to hundreds of systems worldwide that are announced from different geographical locations. DNS queries are then sent to the closest name server to the querying client. With multiple networks dynamically responding to the same IP address, network performance and uptime are drastically increased.

In addition to security against DOS (Denial of Service) and DDOS (Distributed Denial of Service), dinCloud utilizes its ability to recognize botnets, call-homes and other malware packets that tend to come from infected IPs. These attacks are recognized by the IP Reputation facilities that din-Cloud deploys.
Lastly, dinCloud can deploy almost infinite numbers of virtual firewalls. dinCloud has perfected this via the utilization and scaling of virtual dedicated firewalls per VPC (Virtual Private Cloud).

dinCloud Takes Pro-Active Action

Customers can choose to utilize additional security measures and services from dinCloud to provide a more robust security posture.

Once the source has been validated and it has determined it's not a malware, DNS or DDOS attack, dinCloud utilizes a robust AAA (authentication, authorization, and accounting) system for all users at all access points (This addresses the authentication weakness that the target hackers took advantage of. The target hackers breached access via the HVAC system that allowed access to the corporate network).

Different levels of access require (by both security standards and best practices) different levels of 2- factor authentication, but all resources should have some additional access above traditional username/password access.

This remains the premise of dinClouds' ongoing AAA strategy – all access from all customers will be governed by 2-factor authentication because in the multi-tenanted cloud, enterprises are only as secure as the security practices of the adjacent neighbors who are sharing their facilities.

dinCloud understands: A Crunchy Outside, Soft Middle is not Security

Traditional security started from the outside with firewalls and authentication – this is where din-Cloud has stepped up cloud security.

At dinCloud, we started by delineating each hosted private cloud with its own dedicated set of SSL VPNs, firewalls and routers. In this scenario, we can mitigate breach spill-over and insure

confidentiality and security to each enterprise. Much the same way a naval vessel incorporates bulkheads and partitions to ensure that a breach on one segment does not cause damage to other unaffected areas (See Image #1).

This segmentation and partitioning is paramount to a secure cloud design – one that other enterprises and cloud vendors need to deploy.

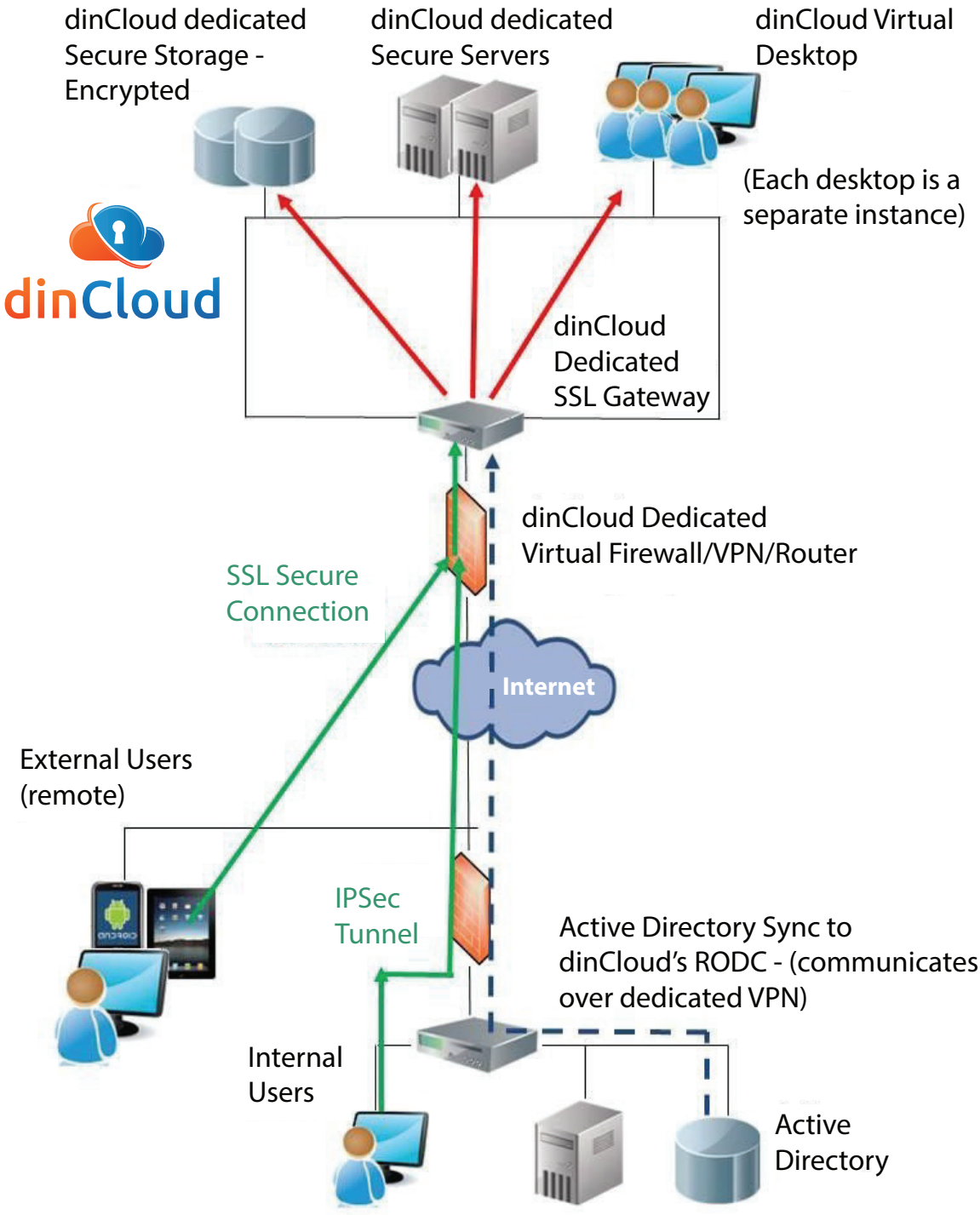

Image #1: dinCloud creates a secure virtual private cloud (VPC) with a dedicated firewall/VPN/router for east customer.

Once inside the segment, dinCloud recognizes that it is imperative to implement security procedures in these trusted zones. Just as dinCloud inspects outside traffic with IP Reputation tools, as described above, it also provides intelligence on the actions and behaviors of traffic inside the VPC network.

dinCloud provides its customers with tools to monitor and access the security of the traffic inside their secure segment. dinCloud starts by providing anti-virus and malware detection on all hosted servers and desktops. As stated, if one server gets infected, the likelihood of other servers and desktops becoming infected is greatly increased. Another advantage of dinCloud's environment is that it has security professionals that can offer, install and monitor the proper security tools.

In addition, dinCloud offers intelligent IDPS (Intrusion Detection and Prevention Systems) on all internal network segments. At dinCloud, all segments can be inspected by a dinCloud hosted and monitored IDPS.

dinCloud Addresses the Issue of Data Storage and Security (Encryption and Backup)

Enterprises simply can no longer afford to leave data-at-rest unencrypted. This is all but too evident in all of the large PII (Personal Identifiable Information) attacks of 2014, such as Home Depot, Neiman Marcus, Michaels, Feedly and P.F. Chang's. All data stored with dinCloud is 100% encrypted with AES256 encryption, mitigating the risk of loss data on event of a breach.

Migrating from a non-encrypted environment to a secure, encrypted environment is behind the scope of most enterprises – and therefore something dinCloud has taken seriously for our clients. Of course, there is more than one way for an attacker to wreak havoc. As stated above, the hacker can steal data, but he can also (or other forces) wipe out the data. Example: in the "Code Spaces" cloud tragedy, an attacker seized the company's Amazon console and held the company hostage over threats of deleting all storage. The company didn't give into demands and the attacker deleted all of Code Spaces IT assets.

dinCloud takes system level snapshots once a day and stores them for 10 days, included with our service for no additional charge.

dinCloud also provides full data center redundancy with dual data centers that are individually controlled, monitored and integrated for full redundancy. For added security, dinCloud went to the Internet Assigned Numbers Authority (IANA) to obtain an ASN (autonomous system number) for the purpose of securing the failover traffic between sites (dinCloud's ASN is 53834). dinCloud uses the ASN for its secure BGP routing between secure dinCloud data centers. BGP ensures that only dinCloud traffic is allowed between the sites.

dinCloud secures its BGP backup with secure servers and secure 2-factor authentication on access to all enterprise services, including the associated BGP and DNS routers. All access to these systems is authenticated, logged and monitored by dinCloud. dinCloud has full control of the traffic to the datacenters and can hide or block all traffic as needed. In this manner, dinCloud has an extra level of security against both DNS poisoning and denial of service (DOS) attacks.

The Future is the Cloud - dinCloud's Secure Cloud

Many articles detail the cost benefits for a cloud move - usually detailing cost saving in material (h/w servers) and administration, but the real benefit for running your hosted private cloud at dinCloud is our unwavering commitment to serving a secure cloud.