



Zscaler Cloud Firewall

A guide for secure cloud migration



Taking advantage of Zscaler Cloud Firewall as you migrate to the cloud

The fact that applications are shifting to the cloud using web protocols is not news. At Zscaler, we anticipated this shift in 2008 as we set out to build our security cloud. Today, our massively scalable cloud gives us the flexibility to inspect traffic and to see what is occurring in the data for HTTP and HTTPS sessions.

As apps shift out of centralized data centers, the model of centralized backhaul becomes problematic – it's not only expensive, but it adds latency to the user experience. For example, if you route DNS through a traditional firewall at a central site, the response will be local to the firewall, not to the user, which affects real-time application performance.

Cloud applications are powerful business enablers, but they introduce challenges of their own. [Office 365](#), for example, opens multiple connections per user and increases bandwidth, exhausting the port and throughput capacity of the traditional firewall. A [recent survey](#) commissioned by Zscaler on the effects of Office 365 deployment found that network issues and latency were common. Many organizations upgraded their firewalls prior to deployment, but 69 percent still reported post-deployment latency. Increasing the bandwidth for backhauled traffic didn't work either. Sixty-nine percent of respondents reported weekly issues and 30 percent reported daily performance problems.

How can Zscaler Cloud Firewall help?

[Zscaler Cloud Firewall](#) resolves these challenges in the same way the cloud proxy helps with web-based traffic. It enables fast and secure local internet breakouts for all ports and protocols, without any appliances to upgrade or deploy, all with centralized management. Zscaler Cloud Firewall, like the rest of the Zscaler platform, scales elastically with your consumption, and your cost is based strictly on the user count.

With Zscaler, policies are not tied to a physical location. Instead, policies follow users to provide identical protection no matter what device they use, or where they connect. This means that your company's executives have the same access and protections whether they are working in the corporate office, visiting branch offices, or traveling to meetings around the world.

Zscaler offers two cloud firewall services: A standard Cloud Firewall that's included with every Zscaler Internet Access subscription and an advanced Cloud Firewall upgrade that is included in the transformation bundle, or can be purchased as a separate upgrade.

What's the difference between "standard" and "advanced" Cloud Firewall?

The standard Zscaler Cloud Firewall is included with your subscription for Zscaler Internet Access services, and the following description includes some of the policy functions that are already available to you. We'll also describe the advanced Zscaler Cloud Firewall, a service included as part of the transformation bundle, which can also be purchased as an individual upgrade.

To begin, let's look at the policies you will find in the two products**STANDARD CLOUD FIREWALL**

Apply allow/block security policy based on source and destination IP address, ports, and protocols. The following is available for all your outbound traffic:

- Unified policy (5-tuple by location)
- Single administrative console
- One set of logs across all your sites and users

ADVANCED CLOUD FIREWALL

Apply granular allow/block security policies based on applications using a Deep Packet Inspection (DPI) engine:

- All the capabilities of standard Zscaler Cloud Firewall
- All the advantages of a Next-Generation Firewall (NGFW) – as well as Zscaler cloud intelligence and management – without the need to buy or maintain expensive appliances
- DNS security and control – Optimizes DNS resolution and provides granular controls to detect and prevent DNS tunneling
- NGFW and context-aware policies – Granular allow/block access and security policies based on applications, user identity, group, and location
- Fully Qualified Domain Name policies – Access policies for applications hosted across multiple IPs
- Comprehensive dashboard – Including real-time visibility into traffic usage, threats, and applications by users, groups, and locations
- Full session-by-session logging and reporting
- Cloud IPS - Deliver always-on IPS threat protection and full visibility, regardless of connection type or location; inspect all user internet traffic (even SSL)
- Auto-proxy forwarding for non-standard ports - Automatically identify and secure applications that use non-standard ports and protocols

To stop a protocol-based attack that uses known protocol numbers, the standard Zscaler Cloud Firewall will likely meet your needs. For example, it enables you to prevent the use of an alternate DNS server by blocking port 53.

But what happens if the application matches the port number but isn't the application you think it is? In much the same way that the proxy has become critical for applications running over HTTP and HTTPS, an advanced Cloud Firewall is required if you want more in-depth information. If you need to know what's running on a port you opened, and what your users are trying to do, you should upgrade to the advanced Zscaler Cloud Firewall.

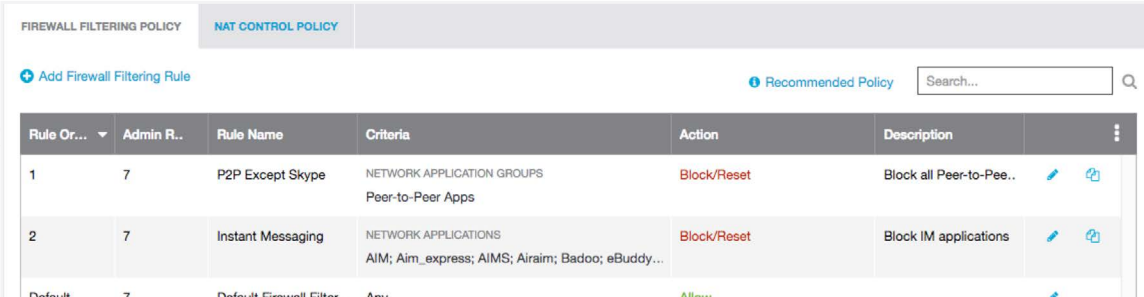
Rethinking the policy

As the industry moved from access control lists (ACLs) to stateful firewalls to NGFWs, the basic operation was the same. We wanted to "punch holes" in the firewall to allow in traffic that we deemed acceptable, and block everything else. The default "deny all" rule exists at the end of almost every firewall rule set in existence.

While still a valid design pattern, when we are talking about traffic leaving the organization instead of entering, it might be time to rethink the pattern. It is worth considering a change to your last rule, and flipping it to "allow all" instead. This pattern approaches stopping that which you don't want, and allowing the rest to continue as normal.

Why change what's worked, and has been recommended by security experts, for decades? Because the nature of our work has completely shifted the way we interact with the internet over the last 20 years.

Today, different organizations have different requirements, either in policy or regulation, that may influence a decision to block or allow all traffic. So how do you decide which is right for you? A look at how your organization operates and what services you provide will often help you choose.



Rule Or...	Admin R..	Rule Name	Criteria	Action	Description
1	7	P2P Except Skype	NETWORK APPLICATION GROUPS Peer-to-Peer Apps	Block/Reset	Block all Peer-to-Pee..
2	7	Instant Messaging	NETWORK APPLICATIONS AIM; Aim_express; AIMS; Airaim; Badoo; eBuddy...	Block/Reset	Block IM applications
Default	7	Default Firewall Filter...	Any	Allow	

Fig 1. Example of an "allow all" default rule

If you are providing a guest network in a public space, you likely will opt for the "allow all" rule after blocking unacceptable content and preventing the potential for malicious or illegal activity by blocking protocols such as P2P. Because the users on a guest network would be accessing the internet and not your data center, the rest of the traffic is likely to be acceptable to your organization.
















Rule Or...	Admin R...	Rule Name	Criteria	Action	Description	
1	7	DNS-Rule	NETWORK SERVICES DNS	Allow	Allow DNS	 
2	7	Allow-Web-Traffic	NETWORK SERVICES HTTP; HTTPS TIME Work-Hours	Allow	Allow the use of HTT...	 
3	7	File-Transfers	DEPARTMENTS IT; IT Networking; IT Security NETWORK APPLICATIONS TFTP; FTPS; FTP-Data; FTP	Allow	Allow IT users to use...	 
4	7	Office-365	DEPARTMENTS Engineering; Engineering QA; Executive; Finance... NETWORK APPLICATION GROUPS Microsoft Office365	Allow	Allow Office 365 for ...	 
5	7	Finance-AWS-Test-S...	DEPARTMENTS Finance DESTINATION ADDRESSES finance-aws.safemarch.com	Allow	Allow finance to use ...	 
6	7	Azure Server Access	DEPARTMENTS IT DESTINATION ADDRESSES mycompanyapp.azure.com	Allow	IT access to Azure s...	 
7	7	Developer-Access	DEPARTMENTS Engineering Development; Research & Developm... DESTINATION ADDRESSES github.com; stackexchange.com	Allow	Allow access to Dev ...	 
Default	7	Default Firewall Filte...	Any	Block/Reset		

Fig 2. Example of a “deny all” default rule

However, if your organization is in a highly regulated industry, such as healthcare or banking, you might want to allow only approved applications. In this case, the most appropriate approach is to let the right stuff out and keep everything else local. Only allowing those applications that need internet access to operate should be allowed, and the “deny all” rule would be the best way to wrap up your policy.

For more details on Zscaler Cloud Firewall and how to configure it, start with our documentation here: <https://help.zscaler.com/zia/about-firewall-control>

Conclusion

The workplace is rapidly shifting. The future includes data centers being replaced by infrastructure and services in the cloud. Expensive backhaul is being replaced by local breakouts. And users are increasingly off the network and away from the office. To secure this future, you need a security platform with integrated services and policies that follow users wherever they go and in whatever way they like to work. Zscaler Cloud Firewall enables fast and secure local internet breakouts for all ports and protocols, without appliances. The Zscaler Cloud Security Platform with standard Cloud Firewall and advanced Cloud Firewall brings the entire security stack closer to the user to ensure identical protection no matter where they connect, and scales elastically to handle all your cloud application traffic.

