

TrustedSource in McAfee UTM Firewall: Providing Small and Mid-Sized Businesses with Big-Business Security



What is TrustedSource?

The TrustedSource™ reputation system is a cornerstone of McAfee's enterprise security portfolio. The most precise and comprehensive Internet host reputation system in the world, TrustedSource collects data worldwide, scoring Internet entities based on global messaging and communications behavior, including reputation, volume, and trends for email, web traffic, and malware. These reputation scores provide the visibility to respond to threats in real time.

Previously available only in our McAfee® Email Gateway (Ironmail) appliances, TrustedSource's unique view into enterprise Internet traffic is now a part of every McAfee UTM Firewall model. That means you can now benefit from the same actionable security information that the largest enterprises depend on. Equally important, you can choose appliances designed for the security needs, network scale, and budget constraints of your small- to medium-sized business (SMB).

Rather than depending solely on localized protection using algorithms that are quickly obsolete, TrustedSource uses a global reputation approach to proactively identify and block traffic from illegitimate sources. For example, TrustedSource detects machines that have been taken over by zombies or botnets for the purpose of generating spam.

The TrustedSource servers accumulate information about spam and malware from tens of thousands of sensors in 82 countries worldwide, enabling:

- The examination of hundreds of billions of messages per month
- The recent detection of more than 4.5 million new zombies per month
- The ability to identify and block better than 80 percent of unwelcome traffic before it ever reaches the enterprise network

TrustedSource uses the global information it gathers to watch for deviations in expected behavior, creating "reputation scores" that can be used to identify and stop spammers, cyber-criminals, targeted attacks, and fraud.

Solution Brief TrustedSource in McAfee UTM Firewall: Providing Small and Mid-Sized Businesses with Big-Business Security

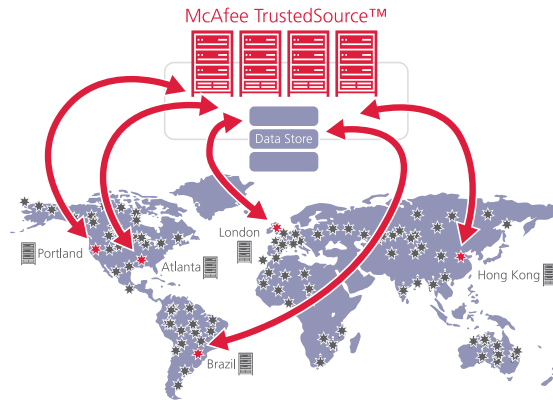


Figure 1: Sensors from around the world gather network behavior analysis data to generate reputation scores for internet entities.

Managing all this information directly on an SMB-scale device such as a McAfee UTM Firewall appliance simply isn't feasible. After all, consider the size and continuous growth of the database and the processing power that would be required to ensure the highest levels of performance. So you may be wondering, how can McAfee UTM Firewall appliances take advantage of TrustedSource's enterprise-scale security information?

To answer that question, let's assume you have a mail server on your premises and you're using a McAfee UTM Firewall appliance connected to the Internet to serve as your firewall and mail filtering device. Every time an incoming SMTP (email) connection request is received, McAfee UTM Firewall asks the TrustedSource data center for a reputation score for the source of the connection request. McAfee UTM Firewall then either accepts or rejects the connection based on the score—before the connection reaches your email server. This process alleviates approximately 80 percent of any spam processing your email servers may have otherwise needed to do. It also improves performance and extends the life of your existing systems—while preventing a huge amount of spam getting through your network to reach your employees.

Figure 2, below, outlines the process of an email coming from a source with a good reputation score. Figure 3 shows what happens when an email comes from a source with a bad reputation. It's important to note that, because different SMBs have different messaging requirements and risk tolerance, McAfee UTM Firewall appliances allow every organization to tailor their own thresholds in terms of what they deem to be a good or bad reputation score.

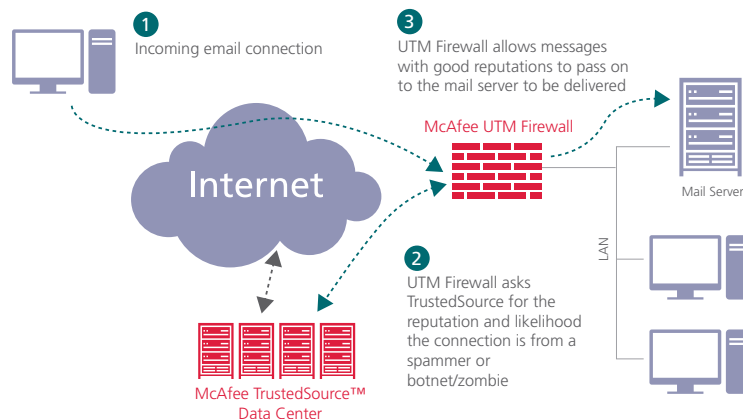


Figure 2: Email with good reputation

Solution Brief TrustedSource in McAfee UTM Firewall: Providing Small and Mid-Sized Businesses with Big-Business Security

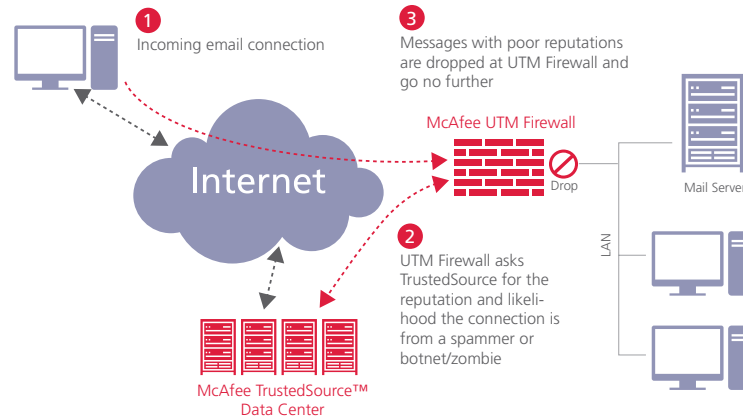


Figure 3: Email with poor reputation

How Does TrustedSource Help the SMB?

Today, SMBs that host their own email systems are facing several growing concerns, including:

- Ever-increasing spam in users' inboxes, incurring significant costs in the form of lost time and productivity
- The need to continually process mail that's more than 90 percent spam, causing undue stress on email systems and filters
- Decreasing effectiveness of anti-spam systems that are based on signatures and blacklists, due to the increasing sophistication and constantly changing tactics of spammers
- Flooding of legacy anti-spam systems, requiring significant investments in upgraded hardware and software while placing an increasing burden on administrators
- Waste of Internet bandwidth and data center resources due to the constant downloading of unfiltered spam

What Does TrustedSource on McAfee UTM Firewall Do for You?

McAfee UTM Firewall appliances, with integrated TrustedSource technology, address all these concerns by:

- Blocking approximately 80 percent of all incoming connections based on sender reputation
- Providing your business with access to technology that had previously been available only to Fortune 2000 companies and other enterprises with large IT budgets and staffs
- Saving you money by blocking unwelcome connections 24/7 to preserve bandwidth and maximize employee productivity
- Freeing your administrator from the need to continually set up new spam filters
- Extending the life of your email servers
- Future-proofing your existing anti-spam systems as TrustedSource becomes even more effective with each new spammer technique identified
- Putting your organization on the leading edge of mail filtering technology without the need to update signature databases
- Providing strong security in a true appliance with no moving parts to wear out or fail, ensuring much higher reliability than other solutions

Solution Brief TrustedSource in McAfee UTM Firewall: Providing Small and Mid-Sized Businesses with Big-Business Security

Why choose McAfee UTM Firewall to deploy such a reputation system? Because the TrustedSource reputation system is the most robust in the world, and McAfee is the only company to offer such a system on SMB-level security appliances. McAfee UTM Firewall is the one multifunction security appliance every SMB needs.

To see detailed information about the dynamic structure of mail volume around the world, where new zombies are being born, and how much of the world's messaging is spam by visiting the TrustedSource website at <http://www.trustedsource.org>. It's free, and it will give you real insight into the threats that are out there and how you can take control over them with McAfee UTM Firewall and TrustedSource.

