

Protecting Your ISA Server from Malicious Attacks

Network firewalls are constantly under attack from malicious software and intrusion attempts, such as:

- Flood or denial of service attacks
- Internal worm propagation
- DHCP poisoning
- DNS exploitation
- IP address spoofing

These attacks can significantly reduce network and server performance, affecting employees, partners, and customers. Damaged applications and data, meanwhile, must be re-installed or recovered from backups, resulting in costly delays and downtime.

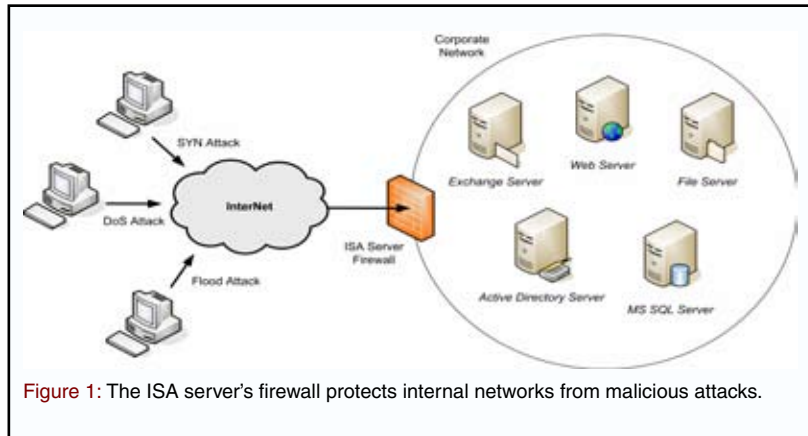


Figure 1: The ISA server's firewall protects internal networks from malicious attacks.

Although Microsoft's Internet Security and Acceleration (ISA) Server has a number of built-in features to prevent and mitigate attacks, some attacks may still go undetected for hours or even days. By baselining ISA Server performance and monitoring key performance counters and alerts, you can improve your ability to recognize and respond to an undetected attack.

Baselining Normal Performance

If you haven't done so already, consider baselining your ISA Server so you know what's normal or typical for your environment. This gives you a basis for recognizing any abnormal resource usage, which may indicate the server is experiencing some type of attack.

When baselining the server, use the following guidelines and performance counters to evaluate resource usage levels:

CPU utilization should average 75%, with short spikes over several minutes in the 80-90% range (\Processor%\Processor Time).

Memory page faults per second should be close to zero and no greater than 10 during peak loads (\Memory\pages/sec).

Disk transfers should not exceed 100 physical disk accesses per second (\Physical Disk\Disk Transfers/sec).

Network interface utilization should average 75% of its maximum bandwidth (Network Interface\Bytes Total/sec).

Try monitoring these resources for a week or so and recording the average usage for both peak and non-peak times in your organization. If resource consumption consistently exceeds the guidelines above, you may need to upgrade one or more resources or otherwise reduce the resource loads on the server.

For more information on how to size and monitor an ISA Server, see the Microsoft article ["Best Practices for Performance in ISA Server 2006."](#)

Managing ISA Service Performance Counters

In addition to monitoring the CPU, memory, disk, and network resources discussed earlier, monitoring the following performance counters for the ISA Server firewall can warn you of an undetected attack.

Total number of active connections. A consistent increase in active connections may indicate a Denial of Service attack where TCP connections are never closed with RST or FIN (\ISA Server Firewall Packet Engine\Active Connections).

Number of denied packets per second. Normally, the number of denied packets should be less than 100. Values greater than 100 may indicate an attack (\ISA Server Firewall Packet Engine\Dropped Packets/sec).

Number of TCP established connections per second. This is the number of connections that successfully completed the 3-way SYN handshake. If the number of TCP established connections/sec is less than 75% of Connections/sec, an attack may be underway (\ISA Server Firewall Packet Engine\TCP Established Connections/sec & \ISA Server Firewall Packet Engine\Connections/sec).

Number of connection objects waiting for a TCP connection. Values greater than 10 may indicate an attack from Firewall clients (\ISA Server Firewall Service\Accepting TCP Connections).

Number of firewall service worker threads. More than 400 worker threads waiting in the completion port queue means that something is wrong with external services (DNS or Active Directory) or an attack is occurring (\ISA Server Firewall Service\Worker Threads).

DNS cache hit rate. Normally, the hit rate should be 70-90%. If hit rate is less than 30%, it may indicate an attack where destination IP addresses are selected randomly (\ISA Server Firewall Service\DNS Cache Hits %).

For more information on monitoring ISA Server performance, see the Microsoft article ["ISA Server 2004: Monitoring and Troubleshooting Performance."](#)

Managing ISA Server Alerts

An ISA Server has over 60 pre-configured alerts. For example, the following alerts warn you of a possible attack:

Connection limit exceeded. A specific IP address tries to flood the ISA Server by maintaining numerous concurrent TCP connections.

DNS intrusion. A host name overflow, length overflow, or zone transfer attack occurred while resolving DNS requests.

Invalid DHCP offer. The IP address in a DHCP request message is not valid.

IP spoofing. The IP packet contains an invalid source address.

Oversized UDP packet. A UDP packet surpassed maximum size limit and was dropped.

POP intrusion. A POP3 buffer overflow detected, indicating a buffer overflow attack.

SYN attack. An attacker is attempting to flood the ISA Server with numerous half-open TCP connections.

By default, these alerts write event log messages to the Windows Event Viewer (you can also configure alerts to send email notifications). Viewing ISA Server alerts/events can help you identify the type of attack and its possible sources.

Detecting and Responding to an Attack

A sudden increase in CPU utilization, memory page faults, or disk transfers is often your first warning of an attack. To identify and mitigate an attack:

1. Check the ISA Server firewall counters to further confirm the ISA Server is experiencing an attack.
2. Check the Windows event log for relevant ISA Server alerts that may confirm an attack has occurred.
3. Inspect the ISA Server logs and verify that all traffic is expected and allowed. Check for clients that:
 - Produce a high volume of connections or requests per second.
 - Extensively consume network bandwidth (bytes per second).
 - Produce connection failures to different destination addresses at a high rate.
 - Attempt to bypass ISA firewall policies.
4. Mitigate the attack. If the source IP address is within the internal network, immediately turn off the switch port for the device. If the source IP address originates from an external network, create a rule denying access.

For more information on how to protect your ISA Server, see the Microsoft article [“ISA Server Network Protection: Protecting against Floods and Attacks.”](#)

Also, www.isaserver.org is a great resource for ISA Server administrators, offering articles, blogs, and FAQs on a variety of ISA Server topics.

Taking an Integrated Approach to Monitoring Servers

Monitoring multiple servers across your network can be a daunting task. Integrating server management into an overall, top-down view of your network can make your life a lot easier.

Using WMI performance counters, you can track resource utilization on all servers and trigger alarms on a central console whenever a particular resource (CPU, memory, disk, or network interface) exceeds a predetermined threshold. Similarly, you can use WMI to monitor applications such as ISA Server, MS Exchange, and Active Directory.

Automatically monitoring the Windows event logs on your servers and triggering alarms for critical events, such as ISA Server alerts, is another way you can simplify server management.

You can centralize server management—and more—with dopplerVUE, a comprehensive yet easy to use network management solution. dopplerVUE enables you to monitor routers, switches, and servers across your network from a single application with consolidated alarms and top-down visualization.

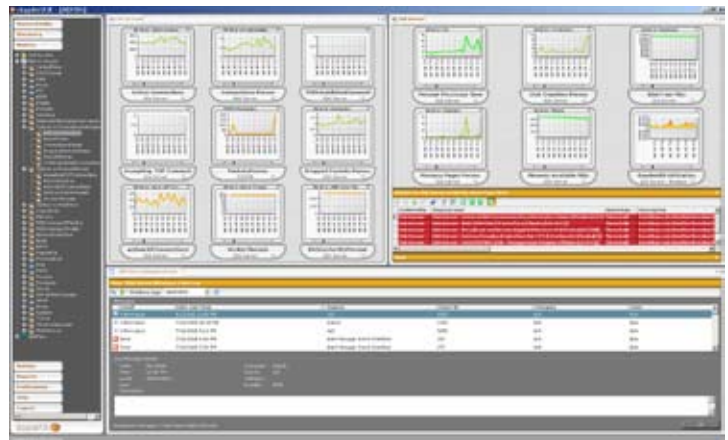


Figure 2: dopplerVUE allows you to monitor all critical aspects of an ISA Server from a single, integrated view. There's no need to start a separate tool or remote in to a server because dopplerVUE puts everything at your fingertips.

About dopplerVUE

dopplerVUE is a powerful yet easy to use network management solution for managing up to 5000 network elements. To see how dopplerVUE can solve your network management needs, visit to www.dopplerVUE.com. For more information call 888-dvue-now (888-388-3669).