



Steelcape Product Overview and Functional Description



TABLE OF CONTENTS

1. General Overview
2. Applications/Uses
3. Key Features
4. Steelcape Components
5. Operations Overview: Typical Communications Session
6. Installation Requirements
7. About Steelcape

1. General Overview:



Steelcape has developed unique technology to *overcome inherent security weaknesses and operational inefficiencies in network communications*. Utilizing patent-pending technology, Steelcape's network communications technology operates within the standard OSI network model at Levels 3 and 4. Steelcape creates a direct IP tunnel between Steelcape components, without the redundancies and inefficiencies that are intrinsic to TCP managed traffic.

Steelcape allows users/applications to establish secure network connections with the following characteristics:

1. No open ports.
2. Fully authenticated users with continuous re-authentication.
3. Optimized routing and message structure to improve performance.
4. Encryption.

The resultant network communications environment is more secure, faster and invulnerable to virtually all current and future TCP/IP threats and exploits. *Since Steelcape does not open ports, it removes the primary attack vector of outside hackers.* Further, Steelcape's unique approach does not require modifications to applications or security software or hardware and installs in minutes.

2. Applications/Uses:

From a technology perspective, Steelcape can be utilized anywhere but has had initial appeal for VPN and VLAN environments. Steelcape allows current VPN and VLAN environments to function without modification and enhances their operations by yielding:

1. Operation of the VPN or VLAN with no open ports.
2. Continuous authentication of source and destination clients (programmable to the millisecond level).
3. Improved performance up to 80%, with typical results of 30 to 40%.

In addition to VPN and VLAN environments, Steelcape can enhance or supplement any point to point communications. Other applications for Steelcape include:

1. FTP
2. SSL
3. Telnet
4. MIME



In addition, Application developers can use Steelcape's library to bypass traditional security products and use Steelcape to conduct point-to-point application communications. This has particular value for applications that send and receive customer or proprietary information:

1. ERP/CRM applications handling customer and financial data.
2. Financial services/banking applications
3. Applications that transfer video or audio programs for the entertainment market.
4. Applications that transfer eDiscovery or litigation information.

3. Key Features:

Steelcape has several key features that enable the enhanced security and performance of network communications. The following are the key features of Steelcape:

1. **Patent Pending Tunneling Methodology:** Steelcape has pioneered a new way of tunneling to establish point-to-point communications. This allows Steelcape clients to communicate without opening ports on Firewalls and without using an intermediate server to proxy data communications.
2. **Patent Pending Steelcape Communications Protocol:** This TCP/IP compatible protocol removes the overhead of typical TCP/IP traffic and uses enhanced routing. Steelcape creates a direct tunnel between its components. The protocol accelerates traffic by:
 - a. Removing redundant TCP processing.
 - b. Maximizing bandwidth utilization.
 - c. Packet compression.This yields greater throughput of up to 80%, and obfuscates the Steelcape traffic from hackers who eavesdrop with packet sniffers. The Steelcape Protocol also provides 100% packet validation to prevent data loss.
3. **Strong and Continuous Authentication:** Steelcape utilizes a layered authentication scheme to ensure that only authorized clients communicate using Steelcape. The Steelcape Server first authenticates the client pair at the start of a session and then the client pair continually authenticates each other. Steelcape keys:
 - i. 48 bit Digital Signature: Digital signature is randomized every few milliseconds.
 - ii. Digital Certificates are encrypted at 2048 bit.
 - iii. PKI signed at 2048 bit with 2 private keys using RSA encryption.
4. **Client Segmentation:** Steelcape allows users to segment their Steelcape clients to enhance security and manage users and applications.



4. Steelcape Components:

Steelcape has developed a range of software and hardware solutions so that customer can configure the Steelcape solutions to their environment and application requirements.

These are the Steelcape hardware and software solutions:

1. **Steelcape Enterprise Server:** The Steelcape Enterprise Server™ administers the protected network. It provides the control and monitoring interface to all other components of Steelcape, including Steelcape Agents.
2. **Steelcape Agents:** Steelcape Agents can be installed on all systems that may access your network, or that may access LANS across different subnets within your network. Agents are also installed on internal systems, such as desktop systems/servers, application servers, and database servers. Steelcape Agents provide end-to-end security across all networked nodes and executed digital certificate and encryption mechanisms to secure our transactional data. Since a fundamental feature of Steelcape supports the closing of ports on your firewalls,

Agents enable secure network communications between systems on opposite sides of the firewalls. Steelcape Agents operate independently, so the Steelcape Enterprise Server™ is not required at all times for secure data flow. Steelcape Agents can be installed on all systems that may access your network, or that may access LANS across different subnets within your network. Agents are also installed on internal systems, such as desktop systems/servers, application servers, and database servers.

Agents provide end-to-end security across all networked nodes and executed digital certificate and encryption mechanisms to secure our transactional data. Since a fundamental feature of Steelcape supports the closing of ports on your firewalls, Agents enable secure network communications between systems on opposite sides of the firewalls. Steelcape Agents operate independently, so the Steelcape Enterprise Server™ is not required at all times for secure data flow.

3. **Steelcape Gateway:** The Steelcape Gateway™ is a hardware device that serves the same purpose as an Agent, as described above. Some environments may have specific needs or unique systems that are better suited for hardware vs. software approach.
4. **Steelcape Applets:** The Steelcape Applets are Agents that Internet users can quickly download to run on their computers, protecting secure data transactions between these users and your network.
5. **Steelcape Library:** The Steelcape libraries are a fully documented set of APIs, methods, and classes that can be licensed for software applications.



These libraries can enhance the security value of applications on many levels. In particular, the application community can securely communicate without requiring an open port on the network.

5. Operations Overview:

Steelcape Agents, Gateways or Applets may initiate network communications. The Steelcape Enterprise Server initiates the session by authenticating the Steelcape components and the components initiate data transfer and integrity checking.

Please note that prior to the first communication session, Steelcape Enterprise Server is configured for what Agents reside in its domain and allowable connections between agents, and then polls these connections for status and best routing. The following is the autonomy of a typical Steelcape communications session.

1. A Steelcape Agent detects a Steelcape enabled communication request. The Agent connects and authenticates to the Steelcape Enterprise Server to request communications from it to the destination Steelcape Agent.
2. The Steelcape Server validates that the source and destination Agents are configured to communicate, and then requests authentication from the destination Agent.
3. After the destination Agent is authenticated, the server then issues routing information to both the destination and source Agents.
4. The source and destination Agents then establish unique session tunnels to each other; both Agents authenticate each other based on a session signature provided by the Steelcape Server.
5. The original source Agent request is now processed by the source Agent and communications begin between the source and destination.

6. Installation Requirements:

All installation and configuration is accomplished through a Web-based interface connected to the Enterprise server. Steelcape has a compact footprint and has broad platform support. Steelcape has the following system requirements per platform:

- Windows 2000/XP/2003/Vista: 16MB of free memory, 25MB of free disk storage
- Windows 9x: 32MB of free memory, 30MB of free disk storage
- Linux 2.6 KernelOSs: 4MB of free memory, 5MB of free disk storage
- Linux 2.4 KernelOSs: 4MB of free memory, 8MB of free disk storage
- AIX: 8MB of free memory, 15MB of free disk storage



- HPUX: 8MB of free memory, 12MB of free disk storage
- Solaris: 8MB of free memory, 10MB of free disk storage
- AS/400: 32MB of free memory, 50MB of free disk storage
- Steelcape Enterprise Server requirements: 64MB of free memory, 200MB of free disk storage and at least 5GB of free disk storage for full reporting (if enabled).

7. About Steelcape:

Steelcape is an emerging leader in the development of next generation network security solutions. Founded in 2004, Steelcape launched its security software and appliances in 2006 and is poised to change the network security landscape by eliminating current and future security vulnerabilities of network communications. Based in Los Angeles California, Steelcape has deployed its solutions in the financial services, entertainment and banking markets.