Protecting sensitive data in Secure Domains.
Mikael Trosell
Aug 17, 2001

Abstract

The basic idea of Secure Domains is to move parts of the network into secure zones, either based on the classification of the data or their being part of a project that can be centralized in a specific zone and are considered as sensitive. Only the application and the data are moved, the users remain on the company network and are able to access the application through protocols like ICA or X11, which only provides the user with a virtual workspace or a display output from the started applications. If we move sensitive data from our corporate network to secure domains, we can achieve an increased security at several levels against both External and Internal threats.

Introduction

In large network and computer environments, it can be difficult to know where the weak points are; there probably is a firewall as the boundary defence against the Internet. Large national and international organisations may not even have contact with each other, but they have network connections between them and the application users could be anywhere in the network.

Basic Condition

Secure Domains demand technical solutions that fulfil some basic requirements:

- A strong encryption between workstations and the Firewall/Access server of the Secure Domain. Encryption key length should be greater than 90 bits (research says this is safe to 2016). *) Avoid using 56-bit DES that is not longer considered to be safe. Performance is also an issue, 128 bits ARCFOUR or 128 bits Blowfish are three times faster in software implementation than Triple DES.
- A strong authentication. It should be two-factor authentication services: something only the user would know (A personal PIN code) and something that establishes the user's identity. This could be an access token or a Smart Card.
- Offered services may depend on the account, method of authentication, time and location.
- Secure Print jobs, computer printouts are logged, and can be permitted or denied in the rule base based on the account.
- Secure Data exchange between different Secure Domains. Data cannot leave or enter the domain without passing a gateway with a logging function, or by procedures that include manual actions. Examples of manual actions are scanning for viruses, verifying software and installation of the software. Import or Export data to tape, cdrom or ftp gateways.
- Capable of detailed logging.
- The application is run in the Secure Domain, only screen output is showed on the user's workstation.
- Workstations in the company network should have a basic virus protection to prevent an attacker to monitor the screen (with Trojan like NetBus or Back Orifice)

*) From: Bruce Schneier, Secrets & Lies. Digital Security in a Networked World

Implementation/Solution

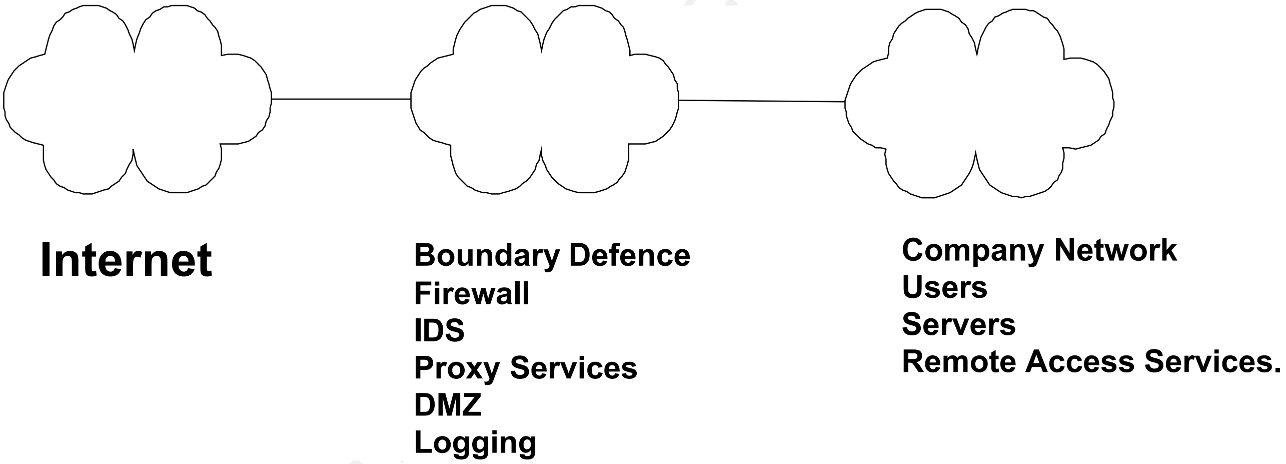
The Secure Domains should be included in the Company Security Policy and, therein, be defined as to what it is. The solution could be configured from being a “Screening” router to the most secure version as I call the Secure Domain, where only “display” protocols are allowed and other types of data transfers between different domains are logged and performed in a documented procedure.

All Systems need to be correctly configured; Software and Operating System have to be patched and then reviewed again. The Secure Domain gives the Administrator a smaller environment to secure. The servers can also easily be placed in physical secure places.
Of course all servers and clients should have a reasonable high security level that can withstand at least the most common attacks, but the servers in a Secure Domain should have hardened Operating Systems and be configured as securely as possible. With multiple interfaces on the gateway it’s possible to separate traffic between the application servers within the Secure Domain to avoid unauthorized traffic.

Building a Secure Domains can create many “Single points of failure”. But availability and scalability increases if gateways and servers are built as Clusters or with Hot Standby Servers.

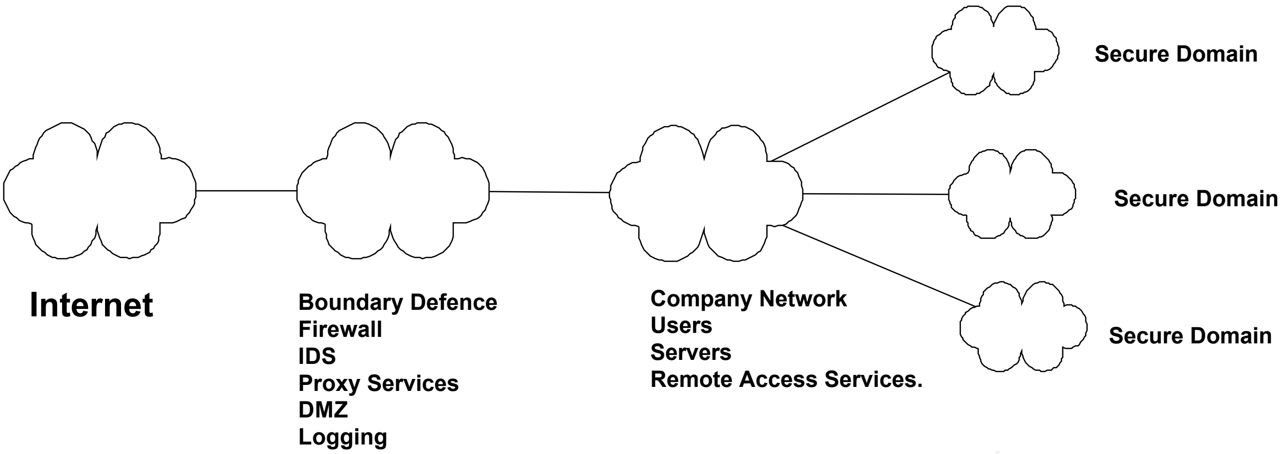
For some users it is possible to change the workstation to a thin client, and, through this, increase security by providing better control of the user’s desktop equipment.

Old topology



The old topology contains a good security between Internet and the Internal network.
But there is limited “Defence in depth”. The Internal Network grows and contains both users and servers. There is also a connection between the users and the Internet, rendering workstations and servers vulnerable to attacks direct from the Internet or by malicious software (virus or Trojan horses).
There probably is a Remote Access Solution or a modem pool that an external attacker will try to use. If one internal server is vulnerable, the intruder could take over that computer and attack the rest of the computers as an internal user from an internal host.

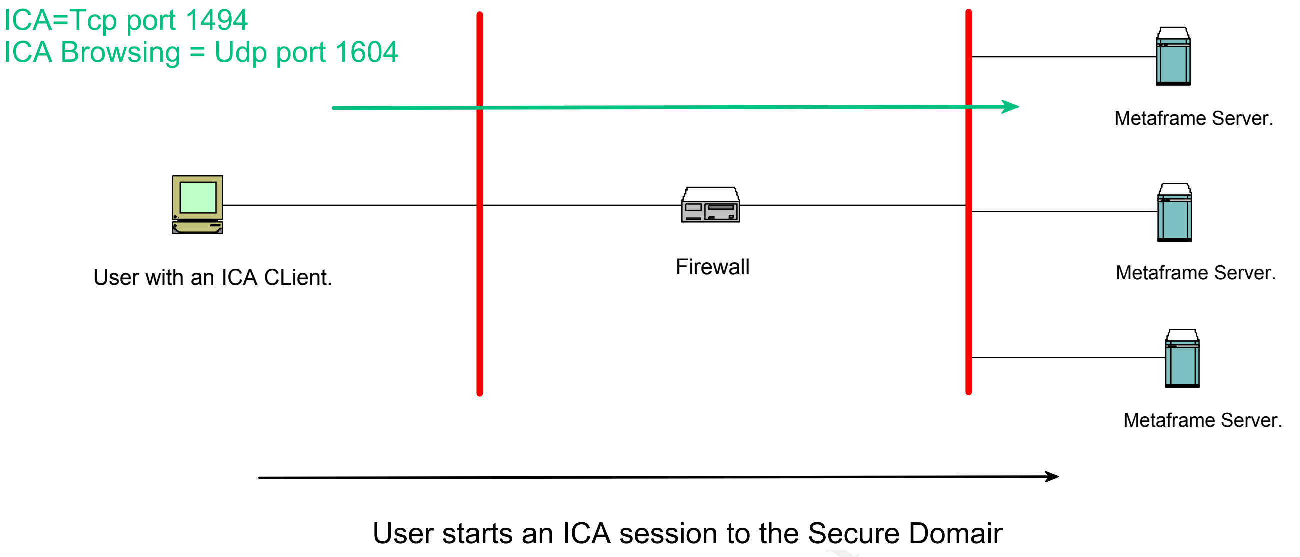
New topology



In the new topology, a project with sensitive data has been moved out to a Secure Domain. The users are still in the Company network, but their access to each Secure Domain is either permitted or denied by the responsible administrator for each domain. If there is a successful attack or a virus incident in the corporate network there is a problem, but there is a maximum limit to the amount of damage an intruder can cause. If there is an incident in one of the Secure Domains, the damage is limited to the local zone.

Three examples of configurations

Using Ica and Metaframe Servers.



The user starts a virtual workspace within the Domain, using a local ICA client connecting to a Windows Terminal Server or a Unix computer with Metaframe from Citrix Installed

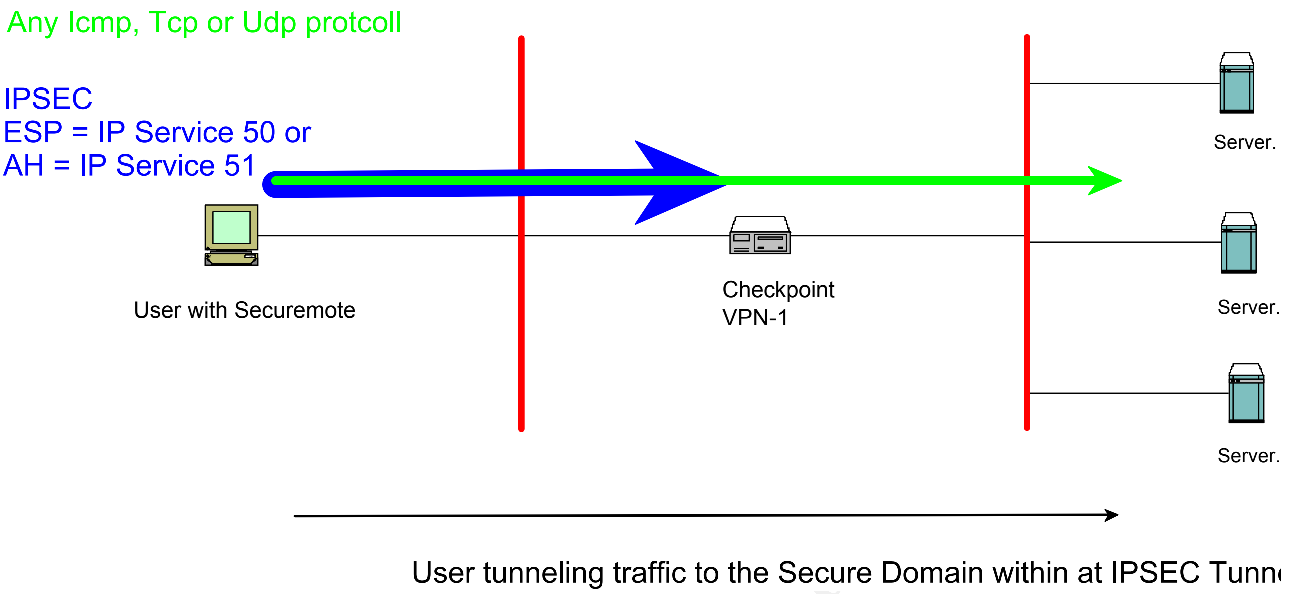
The ICA protocol uses tcp port 1494 as a main port and udp port 1604 for load balancing and for Published Application. The session can be encrypted with 128 bits RC5.

In this solution it is possible to map local disks and printers on the client to the Metaframe server. This function is also possible to turn off at the server, should it not be permitted.

ICA is excellent to use on a slow WAN, because of its design to run on everything from 28 kbs modems to LAN. In using techniques that only transfer changes on the screen, bandwidth is saved.

The connection is directly from the client to the server, so authentication and logging has to be solved on each server.

Using SecuRemote or SecureClient from Checkpoint.

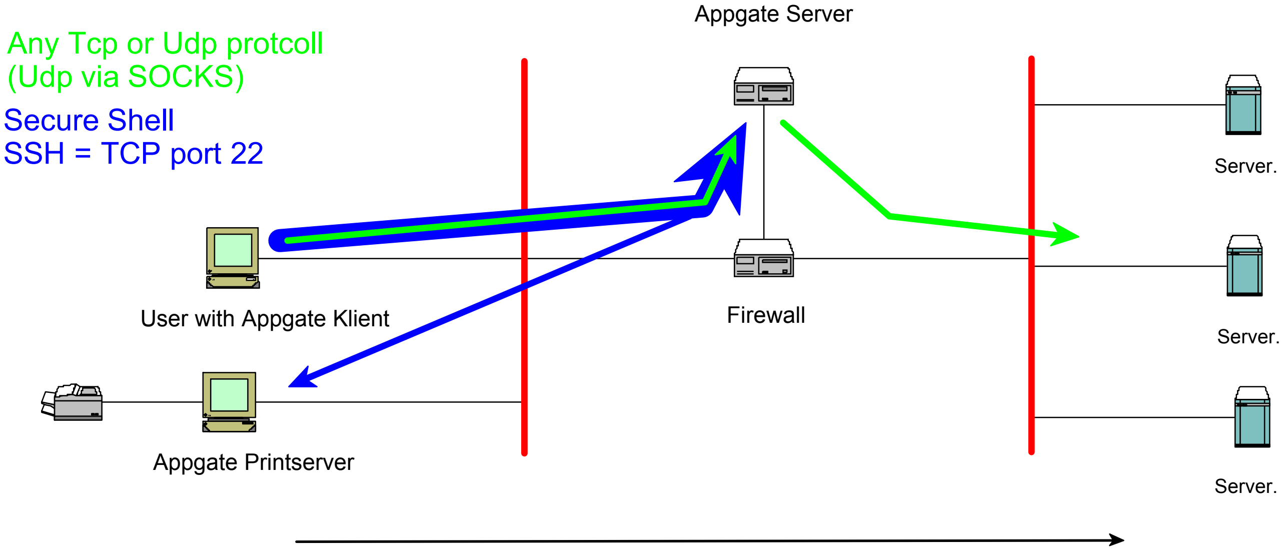


SecuRemote and SecureClient are two IPSEC clients from Checkpoint that can be used to connect to a Checkpoint VPN-1 Firewall. The difference between them is that SecureClient can download a policy setting from the VPN-1 Gateway and, through this, it is possible to demand some settings on the client. For example, when it is connected to the VPN Gateway, it permits only outgoing encrypted packets on the client. Another difference is that SecureClient costs money.

- The user starts the IPSEC client and authenticates to the gateway. One IPSEC tunnel is established to the VPN-1 Gateway. Any TCP/IP communication may be transparently encrypted
- Configuration of allowed services, authentication services, logging and alerts is done using the rule-based editor in Checkpoint VPN1.
- Try to avoid FWZ as a Client Encryption Method, because it's not a standard algorithm; use ISAKMP/OAKLEY with 3DES instead.

If this is to be a Secure Domain, only protocols like ICA and X11 should be allowed. Data can be transferred using the ftp proxy in the Firewall. The FTP Security Server in the firewall logs filenames and sizes and the files can be transparently anti-virus inspected by a CVP server (Content Vectoring Protocol)

Using AppGate.



User tunneling traffic to the Secure Domain within at SSH Tunnel to the Appgate Server.

The AppGate Concept is to protect sensitive application by moving them to secure domains. Access to services (Applications) will be controlled by the AppGate server. Therefore the AppGate Server protects the servers from any unauthorized network packets.

In order to connect to the Secure Domain, the user first starts a local AppGate Client, which sets up a tunnel between the workstation and the AppGate Server. If the authentication is successful, the AppGate Server consults its authorization database to determine which services should be available. Then, the current configuration is sent to the client and the user can start allowed services by clicking on an icon.

The AppGate Server logs every service that is started and stopped, and each session has a unique key to make it possible to trace a user for a period of time.

TCP-port 22 is used for establishing a secure tunnel to the server and it is the only port that needs to be open in a firewall from the External network.
SSH normally only supports tcp ports to be tunnelled, but with socks it is also possible to tunnel UDP ports over SOCKS and then tunnel SOCKS over the encrypted SSH tunnel, this is supported in the AppGate Client.

There is Support for standard ftp over SSH, and an ftp proxy is included in the software.
If FTP is allowed in the rule base on the AppGate server and the AppGate Client is logged in. The user can start the services and then type “ftp localhost” to connect to the ftp proxy over the SSH tunnel. File transfers are logged and the direction can be specified (allow only sending or receiving files).

AppGate Secure Print Module allows Servers in the Secure Domain to send their print jobs to a virtual printer on the AppGate Server. The print jobs can then be fetched from an AppGate Print Server by the user who logs in and authenticates himself, and be printed out on a local printer. The connection between the Print Server and the AppGate Server is encrypted and the actions are logged.

Conclusion

The VPN today contains many features. It is used to build remote access, Intranets and Extranet solutions. It's also possible to use this technique to build Secure Domains. The difference is how the environment is set up and how the software is configured. But it is also a Security Policy issue; is there a need for a Secure Domain? The answer is to make a risk analysis and create a policy that meets the risks. This will result in some functionality and security demands. A "Remote Access solution" configured as a Secure Domain Gateway could be a solution that fulfils the Security Policy.

References

Web Resources.

Strong Authentication with SecurID from RSA Security:
http://www.rsasecurity.com/products/securid/whitepapers/ace5/AS50_WP_0601.pdf

Total Secure Access from AppGate.
http://www.appgate.com/docs/whitepaper4_01.pdf

Technical Description AppGate 4.0
http://www.appgate.com/docs/wpaper_40.pdf

SecuRemote, SecureClient and Checkpoint:
http://www.phoneboy.com and then choose "Secure Client"
http://www.checkpoint.com/products/downloads/securemote.pdf
http://www.checkpoint.com/products/downloads/SecureClient_DataSheet.pdf

Books:

Bruce Schneier, Secrets & Lies. Digital Security in a Networked World.