

A Segurança de redes baseada em perímetros, é possível obter segurança sem firewall?

Por André Fucs de Miranda, CISSP, <afucs@cfsec.com.br>

IRRESTRITO / PÚBLICA / ORDINÁRIA

Grupo de Restrição: Irrestrito	Emissão: 29.01.2002
Arquivo: YSP_0001	Versão: 23.09.2002

Declaração de exoneração de responsabilidade

Este documento foi publicado pela CFSEC Security Architects com o intuito de fornecer, de forma rápida, informações precisas e atualizadas. A CFSEC Security Architects tentará corrigir qualquer erro que possa estar presente neste documento, tão logo seja avisada.

Entretanto, a CFSEC Security Architects não pode garantir que as informações apresentadas no mesmo estejam corretas.

A CFSEC Security Architects alerta ainda para os seguintes aspectos:

- O material difundido comporta exclusivamente informações de caráter geral, que não pretendem referir a situação específica de um indivíduo ou de uma entidade;
- Este documento pode incluir informações que não devem necessariamente estar completas, ser exaustivas e exatas ou estarem atualizadas;
- Este documento remete para sites externos, sobre os quais a CFSEC Security Architects não tem qualquer controle e relativamente aos quais declina todas as responsabilidades;
- As informações disponíveis neste documento não são pareceres de caráter profissional ou jurídico.

Todas as informações são providas pela CFSEC somente em uma base "no estado". Em nenhum evento a CFSEC será responsável pelos possíveis danos diretos, indiretos, especiais ou de qualquer outro tipo, derivados do uso deste web site, ou de qualquer outro web site que esteja ligado a este, incluindo, sem limitação, qualquer perda de lucros, interrupção de negócios, perda de programas ou outros dados de informação relacionados ao seu sistema, incluindo o caso de que nos seja expressamente informado a possibilidade de tais danos.

CFSEC Security Architects é marca registrada da CFSEC Sistemas Ltda. As demais marcas registradas são respeitadas.

Agradecimentos

Aos amigos Bruno Coelho, Bruno Ferreira, Gustavo Zeidan, Hiro Kozaka, Jotapê França, Marcelo Borges, Victor Pereira e Vitor Conceição.

Prefácio

Este documento é um dos primeiros frutos de pesquisa da CFSEC Security Architects. Esta jovem empresa, fundada por André Fucs e Nelson Corrêa procura desde seus primeiros dias de existência, apresentar ao mercado uma visão diferente da segurança, focada nas necessidades do negócio, sem esquecer da realidade tecnológica.

Na visão de nossa empresa, a segurança não existe por si só e como consequência, as soluções de segurança adotadas por uma empresa não devem possuir orientação puramente tecnológica.

Nosso primeiro Yellow Security Paper, não poderia deixar de ser mais polêmico. A possibilidade de se criar redes seguras sem necessidade de um firewall tradicional, é para nós, a quebra de um paradigma, amplamente aceito. Ainda que as idéias aqui apresentadas não sejam de fácil difusão e uso, procuramos através deste documento destacar um de nossos diferenciais, a capacidade de criatividade e questionamento.

Esperamos alcançar nossos objetivos.

Introdução

Durantes os primeiros dias da informática, um modelo centralizado de trabalho, representado pelos enormes computadores oferecia para estes ambientes a segurança que o fim da Segunda Guerra Mundial exigia. Apesar do uso específico e da ausência de teleprocessamento, o rigor imposto pelo modelo centralizado iria marcar as duas gerações seguintes de computadores. Anos mais tarde, estes grandes cérebros eletrônicos viriam a ser conhecidos como *mainframes* e se tornariam presentes em praticamente todas as grandes corporações mundiais.

Em 1962 quando a IBM e a American Airlines demonstraram o SABRE, um sistema de reserva de passagens aéreas, o mundo viu pela primeira vez o uso comercial de terminais. O modelo centralizado e baseado em terminais não processados, utilizado pela solução dominaria sozinho o mercado por praticamente 20 anos.

O modelo distribuído só viria a tomar o mercado anos após o lançamento dos primeiros computadores pessoais. Nos anos seguintes, o mercado corporativo seria tomado por *softwares* de automação de escritórios como o WordStar e o VisiCalc. A facilidade oferecida pelos micro-computadores foi fundamental para o crescimento do modelo distribuído. Entretanto a antagonista necessidade de centralizar e distribuir as informações levou a evolução do modelo cliente-servidor, que pode ser considerado um híbrido entre os dois outros modelos.

Tendo sido drasticamente orientado pelo mercado corporativo e não pelo mercado militar, o modelo distribuído nunca teve na segurança o seu ponto forte. Confidencialidade, integridade e disponibilidade seriam pouco aplicadas em redes locais até os anos 90. Com a explosão da Internet comercial, o modelo cliente-servidor foi consolidado e o mercado pode conhecer a capacidade de interligação do até então desconhecido TCP/IP. Neste mesmo período surgem os primeiros exemplares comerciais dos *firewalls* como os conhecemos hoje. Anos depois, o mercado passaria a ser dividido por 3 tipos principais de *firewalls*, a saber:

- Packet-filter – é o tipo mais simples de firewall, capaz de julgar apenas pacotes de rede com base em regras pré-estabelecidas pelo administrador sem preocupação com a aplicação ou detalhes dos pacotes que passam por ele tais como, sessão, conteúdo, etc.
- Circuit-level – ao contrário do tipo anterior, é um firewall capaz de analisar e julgar de forma automática o estabelecimento de sessões de tráfego feitos por algumas aplicações e protocolos. Normalmente são conhecidos como Stateful Inspection Firewalls.
- Application-level – também denominados Proxy firewalls, estes dispositivos controlam a conexão entre duas redes dentro da camada

de aplicação e por consequência disso, é capaz de controles mais rígidos.

A popularização dos *circuit level firewalls* reforçou no mercado corporativo, o uso de perímetros de segurança. Ainda que seja utilizado de forma moderada, este conceito quando aplicado na segregação de redes oferece um alto nível de proteção, pois é capaz de controlar todos os pontos de entrada e saída de uma rede. O exemplo mais comum de um perímetro de segurança nos dias de hoje é a chamada DMZ, rede desmilitarizada, onde todo o tráfego de dados é feito através de um mecanismo controlador (ex. *firewall*).

O modelo de segmentação tradicional

O modelo mais popular de segregação de redes divide-as em dois níveis de segurança através do uso de algum tipo de *firewall*. Em uma forma similar ao modelo adotado em *sites* Internet, sugere-se dividir uma rede em três níveis de acesso:

- Externo ou vermelho – é aquilo que não é confiável;
- DMZ ou laranja – é aquilo que é confiável, mas está exposto a um maior risco, e
- Interno ou verde – é aquilo que é confiável.

O ambiente interno representa o local sobre o qual é possível exercer, ao menos na teoria, controles operacionais ou aquele que apresenta um maior grau de confiabilidade. O ambiente externo representa aquele onde a ausência de controle sobre o ambiente leva a um menor nível de confiabilidade.

Nesse modelo tradicionalmente utilizado, o ponto de ligação entre os três níveis de segurança é alguma espécie de *firewall*.

Apesar de ser amplamente utilizado em conexões com a Internet de ambientes corporativos, este modelo demonstrou-se dispendioso quando utilizado na proteção de grandes redes corporativas. Enquanto em uma conexão Internet é comum se determinar o que é ou não confiável de uma forma maniqueísta, em uma rede local tal diferenciação torna-se mais complexa. Em outras palavras, em um ambiente já controlado, o equipamento de segregação deve ser capaz de diferenciar acessos de forma individual e amplamente flexível, limitando por exemplo que um usuário responsável apenas pela operação de um equipamento não tenha acesso aos computadores do presidente de uma empresa.

Soma-se a isso o fato de que enquanto uma saída típica com a Internet não possui mais do que dois roteadores, uma rede corporativa típica apresenta um emaranhado de roteadores, *switches* e protocolos de roteamento,

exigindo paralelamente dos sistemas um maior patamar de capilaridade e desempenho. Mesmo sendo teoricamente capazes de exercer o devido controle sobre um ambiente a manutenção de um ambiente segmentado nos moldes atuais, é extremamente complexa. O modelo tradicional, baseado na segregação da rede corporativa em três níveis de acesso, é pouco prático e extremamente caro.

Um modelo de segurança diferente

Ao elaborar este documento, a equipe da CFSEC tomou como base, experiências anteriores com segurança da informação e operação de ambientes seguros e procurou elaborar um modelo de segurança com capacidade de atender as necessidades de disponibilidade, confidencialidade e integridade, tidos em todo o meio como as três bases da segurança.

Visando atender não somente as necessidades econômicas de uma empresa, mas às suas necessidades de segurança, o modelo encontrado baseou-se na modificação do modelo de *thin-computing*. Nesse modelo computacional, o processamento é deslocado do computador pessoal, para um servidor de terminais, capaz de oferecer de forma quase transparente uma experiência operacional idêntica a de um computador pessoal.

Apesar de pouco popular, este modelo computacional apresenta naturalmente diversas características diretamente ligadas a segurança e a forma com que a CFSEC Security Architects, vê a segurança corporativa. Ao centralizar a execução de aplicações e o armazenamento de dados em servidores, torna-se economicamente viável oferecer de forma transparente recursos que garantam a segurança da informação a todos os usuários de informática de uma empresa. Dentre esses recursos podemos citar:

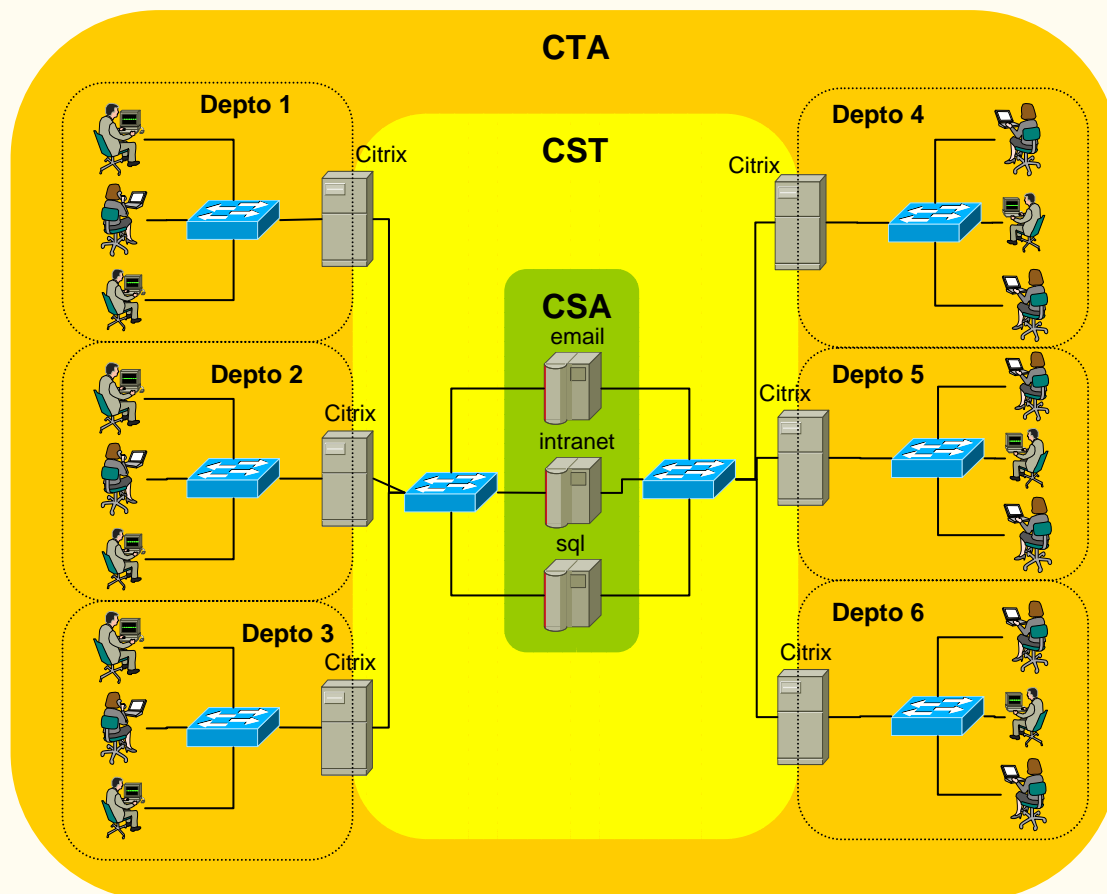
- Sistemas de armazenamento de dados redundantes (RAID, SAN, etc);
- Backup de informações pessoais centralizado;
- Atualização de aplicativos e sistema operacional;
- Configuração de sistemas de segurança centralizada;

O modelo centralizado apesar de possuir menor escalabilidade é capaz de oferecer recursos de segurança que em um ambiente distribuído só são disponibilizados através de ferramentas e recursos nem sempre transparentes ao usuário.

O modelo desenvolvido pela CFSEC vai além dessa arquitetura tradicional de ambientes centralizados ao agregar a segmentação de rede o conceito de perímetros concêntricos de segurança implementados na camada de aplicação através de sistemas de uso geral. Ou seja, utilizar servidores *web*, servidores de terminal e servidores de bancos de dados como dispositivos de controle.

O conceito é muito próximo ao atualmente utilizado por servidores de Proxy, onde a conexão entre redes é feita a partir da camada de sessão¹ ou ao invés da camada de rede.

A figura abaixo, mostra de forma resumida o modelo proposto.



As três camadas do modelo são assim descritas:

CTA – Camada de Terminais de Acesso:

Conjunto de computadores, responsáveis por prover acesso ao usuário final e às estações de trabalho remotas. Por exemplo: *Thin-Clients*, *X-Terminals*, *browsers*. Nessa camada seriam aplicados sistemas simples de proteção como **Criptografia**, **Private VLANs** e **Tokens de acesso**.

CST – Camada de Servidores de Terminais

Conjunto de equipamentos responsáveis por **processar** as funções de estação de trabalho. Nesses servidores são implementados mecanismos de proteção como RAID, backup, política de configuração de segurança de

¹ Este documento compreende que o protocolo TCP/IP e as aplicações criadas a partir do mesmo, não se encaixam perfeitamente ao modelo OSI de rede.

sistemas operacionais, controle de conteúdo, antivírus, etc.

É interessante lembrar que apesar desses dois componentes serem tipicamente apresentados em soluções de computação centralizada como o Citrix Metaframe e Microsoft Terminal Server, o modelo proposto não se resume a estas soluções. Do ponto de vista da segurança, o acesso às informações pode ser oriundo de navegadores Internet ou demais formas de interface sendo estes princípios amplamente utilizados em sistemas de Internet banking. O documento toma como exemplo os sistemas de *thin-client* por serem mais genéricos e mais completo.

CSA – Camada de Servidores de Aplicação

Conjunto de servidores de aplicação tais como, correio eletrônico, Intranet, bancos de dados, etc. Procedimentos de configuração segura, criptografia de dados, *Network based IDS* e outras tecnologias, assegurariam que um atacante que conseguir acesso às camadas externas, não seria capaz de obter acesso a esta e às camadas internas da rede.

Considerando-se que a relação de hierarquia entre servidores de rede é peculiar a cada empresa, esta camada pode ser dividida em duas outras camadas, denominadas **Camada de Servidores de Interface** e a **Camada de Núcleo de Rede**. Desta forma, a arquitetura é capaz de restringir usuários a um ou mais servidores de aplicação. Um exemplo disso seria oferecer a um usuário acesso a um servidor de Intranet com acesso a uma base de dados, mas não oferecer acesso ao banco de dados em si.

Segmentando uma rede local

Um fator interessante da arquitetura proposta nesse documento é a grande flexibilidade que ela apresenta. Visto que dentro de uma corporação, diferentes departamentos possuem necessidades individuais de acesso às informações da empresa, diferentes mecanismos de acesso poderão ser configurados. É perfeitamente possível que os modelos de segmentação atual co-existam em uma mesma rede com o aqui sugerido, diminuindo assim o impacto de implantação do novo sistema.

Independente desse fato, ao adequar um ambiente seguindo os princípios deste documento, é importante que a segmentação seja feita de acordo com o perfil de aplicações e informações às quais um usuário tem acesso. A forma mais convencional de fazê-lo seria a segregação por departamentos, com a criação de um ou mais servidores de terminal para cada departamento segregado.

Um novo paradigma para a segurança da informação

Visto em seu conjunto, o modelo supera o tradicional ao agregar à segurança de redes, a capacidade de gerenciamento centralizado e alta-disponibilidade típicas dos ambientes de computação centralizada. Na arquitetura proposta neste documento, a segurança dá um passo à diante, ao oferecer ao usuário, capacidades de redundância, como multi-processamento, fontes redundantes e *arrays* de discos, antes disponíveis apenas para servidores de rede.

A estrutura apresentada não só é capaz de segmentar uma rede de dados como também é capaz de facilitar a gestão de pontos normalmente esquecidos como o backup de dados armazenados em estações de trabalho e a aplicação e manutenção das configurações de segurança dos ambientes computacionais para todos os usuários.

Ao delegar as responsabilidades de controle e acesso entre diversas tecnologias, o ambiente aqui sugerido é capaz de minimizar os problemas de latência e *performance* normalmente presentes em soluções de segmentação em camada de aplicação. Mais do que isso, o modelo apresentado se diferencia dos demais modelos de segmentação ao tratar a segurança como um todo ao invés de restringir-se ao controle de acessos. Ainda assim, a **CFSEC Security Architects**, não vê nesse modelo um total substituto aos bons e velhos firewalls.

Sobre o autor

André Fucs de Miranda é Diretor de Tecnologia da **CFSEC Security Architects**. *Certified Information Systems Security Professional* pelo ISC2 e participante de diversos congressos e eventos no Brasil e no exterior, participou durante sua carreira de alguns dos mais importantes projetos brasileiros de Segurança da Informação. Membro do Association for Computer Machinery e do Information System Security Association, participa ativamente de diversos debates sobre a Segurança da Informação no Brasil e exterior.