UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

BÁRBARA VALESKA SOEIRA
FERNANDO CÉSAR DA SILVA
LETÍCIA BATISTA TABORDA

IMPLEMENTAÇÃO DO *FIREWALL* CISCO ASA 5500

TRABALHO DE CONCLUSÃO DE CURSO

CURITIBA
2013

BÁRBARA VALESKA SOEIRA
FERNANDO CÉSAR DA SILVA
LETÍCIA BATISTA TABORDA

IMPLEMENTAÇÃO DO *FIREWALL* CISCO ASA 5500

Trabalho de Conclusão de Curso de graduação, apresentado à disciplina de Trabalho de Diplomação, do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica – DAELN – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA
2013

TERMO DE APROVAÇÃO

BÁRBARA VALESKA SOEIRA
FERNANDO CÉSAR DA SILVA
LETÍCIA BATISTA TABORDA

IMPLEMENTAÇÃO DO *FIREWALL* CISCO ASA 5500

Este trabalho de conclusão de curso foi apresentado no dia 04 de Julho de 2013, como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Telecomunicações, outorgado pela Universidade Tecnológica Federal do Paraná. Os alunos foram arguidos pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Luis Carlos Vieira
Coordenador de Curso
Departamento Acadêmico de Eletrônica

_____
Prof. Esp. Sérgio Moribe
Responsável pela Atividade de Trabalho de Conclusão de Curso
Departamento Acadêmico de Eletrônica

BANCA EXAMINADORA

_____
Prof. Dr. Kleber Nabas
UTFPR

_____
Prof. MsC. Lincoln Herbert Teixeira
UTFPR

_____
Prof. Dr. Augusto Foronda
Orientador – UTFPR

"A Folha de Aprovação assinada encontra-se na Coordenação do Curso"

RESUMO

SOEIRA, Bárbara Valeska; SILVA, Fernando César da; TABORDA, Leticia Batista. **Implementação do *Firewall* Cisco ASA 5500**. 2013. 64 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

Sigilo da informação sempre foi uma das principais preocupações no mundo dos negócios e a sua relevância vem crescendo à medida que novas soluções são criadas para a proteção de dados e controle de acessos. Este trabalho tem por objetivo apresentar a necessidade e a importância de um dos principais componentes de um sistema de segurança de rede: o *firewall.* O desenvolvimento consiste na pesquisa deste equipamento, mostrando as suas funcionalidades e formas de implantação em ambientes corporativos, o qual pode ser aplicado desde a sua maneira mais clássica de arquitetura até em novos modelos, mais avançados e complexos. Dentro deste tema de pesquisa e avaliando as melhores soluções disponíveis no mercado, encontramos o *firewall* da família Cisco ASA 5500 e através da análise deste equipamento específico poderemos observar como um determinado modelo de *firewall* pode conter diversas técnicas e aplicações que poderão auxiliar nas mais variadas estratégias de segurança dentro de qualquer empresa.

Palavras chave: *Firewall*. Segurança de rede. Filtro de pacotes. ASA 5500.

ABSTRACT

SOEIRA, Bárbara Valeska; SILVA, Fernando César da; TABORDA, Leticia Batista. **Implementation of *Firewall* Cisco ASA 5500.** 2013. 64 f. Trabalho de Conclusão de Curso (Curso Superior de Tecnologia em Sistemas de Telecomunicações), Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná (UTFPR), Curitiba, 2013.

Confidentiality of information has always been a major concern in the business world and its relevance is increasing, in that new solutions are created for data protection and access control. This work aims to present the need and importance of one of the main components of a security system network: the firewall. The development consists in the research of this equipment, showing its features and forms of deployment in enterprise environments and can be applied since its way more classical architecture or new models, more advanced and complex. Within this research theme and evaluating the best solutions available in the market, is the family firewall Cisco ASA 5500 and through analysis of this specific equipment, you can see how a particular model may contain several firewall techniques and characteristics of network application that assist
in various security strategies within any company.

Keywords: Firewall. Network security. Packet filter. ASA 5500.

LISTA DE FIGURAS

LISTA DE SIGLAS E ABREVIATURAS

ACL	Access Control List
AIP	Advanced Inspection and Prevention
ASA	Adaptive Security Appliance
ASDM	Adaptive Security Device Manager
CSM	Cisco Security Manager
CLI	Command-Line Interface
CSC	Content Security and Control.
DMZ	Desmilitarizada
DoS	Denial of Service
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IoS	Internetwork Operating System
IP	Internet Protocol
IPS	Intrusion Prevention Service
IPsec	Internet Protocol Security
LAN	Local Area Network
MPF	Modular Policy Framework
NAT	Network Address Translation
OSI	Open Systems Interconnection
RAM	Random Access Memory
RFC	Request for Comments
RR	Risk Rating
SLA	Service-Level Agreement
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
SSMs	Security Services Modules
SSP	Security Services Processor
SYN	Synchronize/Start
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

SUMÁRIO

1. INTRODUÇÃO

O desenvolvimento de ambientes seguros que garantam a segurança das informações e a integridade dos dados, atualmente é fundamental e vital para as empresas se manterem no mercado. Diante deste contexto, torna-se essencial a utilização de tecnologias que evitem a exposição de informações confidenciais e manipulação de dados corporativos por usuários não autorizados.

Os acessos às informações foram se modificando com o passar do tempo, assim como a implementação de novas tecnologias para proteger os dados corporativos.

O mercado disponibilizou diversos recursos como antivírus, *firewalls*, *proxy*, NAT (*Network Address Translation*), entre outros, que provêm ferramentas que ajudem na proteção dos dados e minimizem os ataques à rede.

Enquanto o antivírus é responsável por proteger o sistema contra vírus, como cavalos de tróia, *spyware*, *worms*, o *firewall* atua com o objetivo de proteger a rede e não permitir que informações sejam extraídas ou perdidas da LAN (*Local Area Network*), ou até mesmo a entrada de usuários não cadastrados.

Objetivo de estudo desse projeto, o *firewall* é uma das tecnologias mais utilizadas e sua função básica é filtrar os pacotes da rede (tanto entrada como saída), de forma que se possa evitar que os pacotes que contenham conteúdo nocivo à rede entrem na LAN e cause prejuízos.

Dentro desse contexto, o *firewall* ASA (*Adaptive Security Appliance*) 5500 é um exemplo de uma nova ferramenta com este propósito.

1.1. PROBLEMA

Invasões nos sistemas internos das empresas têm preocupado os profissionais da área de segurança de redes. Ataques que antes visavam apenas reafirmar a ousadia dos *hackers*, hoje se mostram com objetivos mais claros, como roubos de informações confidenciais, desvio eletrônico de recursos e congestionamento de serviços.

Observa-se que a demanda por controle e segurança de rede tem aumentado e com isso surgem alguns questionamentos: Qual o melhor sistema de segurança a ser implantado? Onde, dentro da LAN, esse sistema deveria ser implantado? Depois de implantado quais serão os benefícios desse sistema?

Perante o exposto, será apresentado um estudo sobre o *firewall*, assim como a importância de implementar esse sistema no âmbito corporativo. Porém é importante salientar que não é o único dispositivo de segurança de rede, contudo um dos mais importantes.

Através do estudo do funcionamento do *firewall*, suas configurações e formas de implementação, iremos apresentá-lo como uma opção para a resposta das perguntas acima e demonstrar a importância da implantação desse sistema.

1.2. JUSTIFICATIVA

A implementação de equipamentos na rede com o objetivo de promover e garantir a segurança de dados tem sido utilizada cada vez mais pelas empresas e o *firewall* é uma das alternativas para isso. Dentre as várias opções e modelos de *firewall* um dos mais bem conceituados é o ASA 5500 do fabricante CISCO, equipamento que vai ser apresentado como solução viável no decorrer desse projeto.

A utilização deste equipamento como solução se explica pelas diversas vantagens oferecidas, tais como:

- Serviços de inspeção capaz de fornecer às empresas o controle sobre o que

os usuários podem executar e quais ações ao acessar *websites*;

- Suporta comando HTTP (*HyperText Transfer Protocol Secure*) de filtragem para um controle preciso sobre como *Web* servidores são acessados, proporcionando uma forte linha de defesa;
- Capacidades de validação de conteúdo;
- Serviços de inspeção no HTTP que ajudam a proteger contra ataques baseados na *Web* e outros tipos de "mau uso da porta 80";
- Inclui políticas personalizáveis para detectar e bloquear acessos;
- Facilidade de gerenciamento.

1.3. OBJETIVOS

1.3.1. Objetivo geral

Demonstrar a importância da implantação do *firewall* nas redes corporativas, através do estudo das características e dos aspectos técnicos desse sistema, assim como apresentar uma possível solução de *firewall* que garanta a segurança e gerenciamento da rede.

1.3.2. Objetivos específicos

- Expor como as novas tecnologias trazem consigo novas vulnerabilidades.
- Descrever os conceitos, características e a importância do *firewall* em ambientes corporativos.
- Demonstrar as configurações da tecnologia ASA 5500 e apresentar esse sistema como uma possível solução de segurança.
- Apresentar ambientes de implantação do sistema *firewall*.

1.4. MÉTODO DE PESQUISA

A implementação deste projeto será orientada pelos manuais, normas, tutoriais e bibliografias que tratam do escopo do projeto.

A primeira etapa do trabalho será baseada na contextualização do tema, invasões recentes e motivações que levaram ao desenvolvimento do *firewall*, através de sites da Internet e livros técnicos. Seguido dessa pesquisa, iremos apresentar o conceito *firewall*, sua importância, as divisões existentes e os principais *firewalls* utilizados nos ambientes corporativos.

Em um segundo momento será analisado a tecnologia ASA 5500, suas funções, programação e formas de implantação. A base dessa parte do estudo será a utilização de apostilas e site da Cisco, que traz uma grande quantidade de informações sobre este equipamento e detalhes técnicos sobre sua implementação.

Posteriormente, serão apresentadas implementações que capacitarão os membros da equipe à analisar comandos de configuração e o funcionamento de uma rede com um *firewall*, verificando principalmente os parâmetros que devem ser atribuídos à rede para operação compatível com esta tecnologia.

A última etapa do trabalho será vincular os conhecimentos técnicos adquiridos com as implementações apresentadas para que possamos demonstrar os benefícios da implantação de um *firewall* à redes corporativas.

2. CONCEITO DE *FIREWALL*

Com a inclusão digital, está cada vez mais democrático o acesso as informações, e a Internet tornou-se o principal e mais rápido meio de comunicação mundial. Com a possibilidade de qualquer pessoa ter acesso à Internet, prover a segurança da informação tornou-se essencial, e por consequência o mercado tem visado cada vez mais o desenvolvimento de equipamentos que tenham por objetivo regulamentar o tráfego de dados, assim como realizar um controle das trocas de informações, evitando dessa forma acessos nocivos ou não autorizados de uma rede para outra (TABENBAUM, 2003).

De acordo com a norma ISO/IEC 17799, a segurança da informação pode ser definida da seguinte forma (TÉCNICAS, 2005):

> Segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessários, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Com esse novo ambiente em desenvolvimento, um novo campo de estudo tem estado em evidência, a segurança de redes. Essa área é marcada pela evolução contínua, conforme novos ataques surgem, novas formas de defesas também. Sendo assim, podemos considerar alguns pontos que justifiquem (GONÇALVES, 2000):

- Compreender que as maiorias das invasões são resultado da exploração de vulnerabilidades, ou seja, eles podem ocorrer nas falhas de implementação do sistema de segurança, inclusão de novas tecnologias e novos sistemas de conectividade.
- As diferentes formas e a facilidade de acesso a Internet, possibilitam novos ataques e por conseqüência devem ser desenvolvidas novas formas de defesa, o que torna a defesa mais complexa que o ataque. Enquanto em um ataque o criminoso deverá identificar apenas um ponto de falha para prover a invasão no sistema, a defesa deve se

preocupar com todos os possíveis pontos de invasão para mitigar os riscos.

- Entender os motivos dos ataques facilita no desenvolvimento de sistemas de segurança. Os ataques podem ter diferentes propósitos, por exemplo, interromper serviços específicos, comprometendo dados ou *softwares*, desestabilizar uma rede com o objetivo de coletar informações que serão utilizadas posteriormente em uma nova invasão e o ataque com a finalidade do roubo de dados.

Neste contexto surge o *firewall* como um mecanismo de defesa, que pode ser definido como um ponto entre duas ou mais redes, no qual circula todo o tráfego. A partir desse único ponto, é possível controlar e autenticar o tráfego, além de registrar, por meio de *logs*, todo o tráfego da rede, facilitando sua auditoria (CHESWICK; BELLOVIN; RUBIN, 2003).

Baseado nessas definições apresentadas pode se descrever um *firewall* como um ponto entre duas ou mais redes, composto por um elemento ou conjunto de componentes, que possui a capacidade de restringir, controlar, autenticar e registrar todo o tráfego de uma rede.

O objetivo do *firewall* é basicamente proteger uma rede especifica das ameaças que uma rede pública não confiável pode oferecer. Essa rede específica pode ser toda uma LAN de uma empresa da Internet, por exemplo, ou até mesmo uma sub-rede específica da empresa ou grupos de trabalho exclusivo das demais áreas da empresa. Por exemplo, a área financeira de um banco possui um maior controle das informações, e deve possuir um controle dos pacotes trocados entre as áreas da própria empresa para evitar que informações sejam repassadas as pessoas erradas ou evitar que um pacote nocivo entre nessa sub-rede.

O *firewall* pode ser caracterizado como um conjunto de elementos e funcionalidades que determinam a arquitetura de segurança de uma empresa, e para isso pode utilizar uma ou mais tecnologia de filtragem. Hoje em dia o que ocorre é que essas diferentes tecnologias podem ser incorporadas em um único equipamento, o que faz como que as pessoas façam a analogia do *firewall* a um único componente da rede, porém, um produto isolado não é o que faz uma rede se tornar segura, mas sim, um sistema estruturado com elementos físicos, funcionalidades, arquitetura, tecnologias e uma política de segurança confiável (AWICHY; CHAPMAN, 1995).

Justamente por vários conceitos de segurança terem sido associados ao *firewall*, não podemos afirmar que este é uma tecnologia estável, pois ele continua em processo de evolução. Isso ocorre, principalmente, por estarmos vivendo um grande e rápido desenvolvimento tecnológico, no qual as informações têm que estar cada vez mais protegidas e por consequência as redes no qual essa informação está, também, aumentando a complexidade das redes corporativas, assim como a complexidade de como deve ser implementada a segurança dessa rede, e o *firewall* atrelado a essa segurança.

Algumas funcionalidades que foram atreladas ao *firewall* estão diretamente envolvidas com a produtividade de uma rede, como por exemplo, nos casos de NAT e VPN (*Virtual Private Network*). O crescente uso da Internet como ferramenta essencial ao desenvolvimento de uma empresa, é um dos motivos que motivou o desenvolvimento de *firewall* e tem motivado o seu desenvolvimento a cada dia.

Hoje em dia a tendência é adicionar cada vez mais funcionalidades aos *firewalls*, que podem não estar relacionados à segurança, como por exemplo, gerenciamento de banda ou balanceamento de carga de serviços. Esses equipamentos são conhecidos como *firewall appliance.* Porém essas funcionalidades devem ser incorporadas com cuidado, tendo em vista que algumas delas podem comprometer a segurança ao invés de aumentá-la, (FILIPPETTI, 2008).

2.1. TIPOS DE *FIREWALL*

Firewall pode ser classificado, como componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a Internet, ou entre outros conjuntos de redes.

É possível compreender que ele também vai além de uma simples barreira de proteção contra ataques externos, pois pode ser utilizado como uma proteção dentro da rede, controlando de tráfegos a servidores específicos (AWICHY; CHAPMAN, 1995).

Podemos definir como componentes básicos de um *firewall*: filtros, *proxyes, bastion hosts* e zonas desmilitarizadas. Porém, essa definição vem sofrendo uma evolução natural e devido às novas necessidades de segurança algumas

funcionalidades como NAT, VPN, autenticação/certificação, balanceamento de cargas e alta disponibilidade foram incorporadas ao *firewall*, tendo em vista que todo o tráfego entre as redes deve passar por ele (AWICHY; CHAPMAN, 1995).

2.1.1. Filtros de pacotes

O filtro de pacotes realiza a filtragem baseado no endereço de origem e destino, porta de origem e destino e a direção das conexões. Essas definições são identificadas nos cabeçalho do TCP/IP (*Transmission Control Protocol*)/(*Internet Protocol*), o que faz com que esse filtro trabalhe nas camadas de rede e de transporte.

Para as conexões UDP (*User Datagram Protocol*) e ICMP (*Internet Control Message Protocol*) a filtragem é um pouco diferente. Como o UDP não é orientado a conexões, não conseguimos filtrar os pacotes com base no sentido das conexões, logo as filtragens são definidas de acordo com endereços IP ou com os serviços e a filtragem do ICMP é realizada baseada nos tipos e códigos das mensagens de controle ou erro. (ALECRIM, 2004).

Na figura 1 temos um exemplo básico deste tipo de *firewall*, dentro da rede. Ele é conhecido também como *static packet filtering,* pois os endereços e serviços são permitidos ou proibidos e são estáticos, (NAKAMURA; GEUS, 2007).

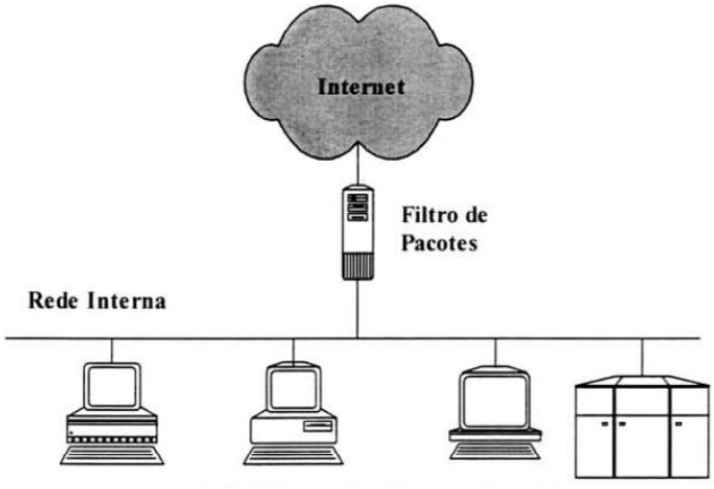

Figura 1 – Filtro de pacotes
Fonte: SPOHN, 1997.

Vantagens desse *firewall* (NAKAMURA; GEUS, 2007):

- Simples, barato e flexível;
- Baixo *overhead*/alto desempenho na rede;
- Transparente ao usuário;
- Maior desempenho comparado ao Proxy;
- Gerenciamento de tráfego.

Desvantagens desse *firewall*

- Menor grau de segurança;
- Vulnerável a ataques por falsificação de IP;
- Difícil gerenciamento em ambientes complexos;
- Não oferece a autenticação do usuário;
- Dificuldade de filtrar pacotes que utilizam portas dinâmicas, como o RPC;
- Regras específicas de permissão passam livremente pelo *firewall,* permitindo aberturas permanentes na rede.

2.1.2. Filtros de pacotes baseado em estados

Conhecido também como filtro de pacotes dinâmicos (*dynamics packet filter*) ou filtros de pacotes baseado em estados (*stateful packet filter*), esse filtro considera dois dados para realizar as filtragens:

1° Informações dos cabeçalhos, conforme o filtro de pacotes;

2° Os estados de todas as conexões, que são salvas em uma tabela.

Em conexões TCP/IP, apenas os pacotes SYN (*synchronize/start*) podem iniciar uma conexão, então será esse pacote que será analisado inicialmente. Conforme mostra a figura 2, a filtragem desse *firewall* começa inicialmente igual o filtro de pacotes, avaliando se o pacote da conexão estabelecida atende ou não as regras do *firewall*, em ordem sequencial. Se todas as regras são atendidas, o pacote é aceito e essa sessão é inserida em uma tabela de estados do *firewall*, caso contrário, a conexão é rejeitada ou ignorada, conforme definições do *firewall*. Para

que os demais pacotes sejam aceitos, eles sempre devem estar inseridos em uma sessão, caso contrário eles serão descartados. Para que isso funcione de forma a aumentar o desempenho do sistema, apenas os pacotes SYN serão comparados com as tabelas de regras e os demais pacotes são comparados com a tabela de estados, o que torna o processo dinâmico, (NAKAMURA; GEUS, 2007).

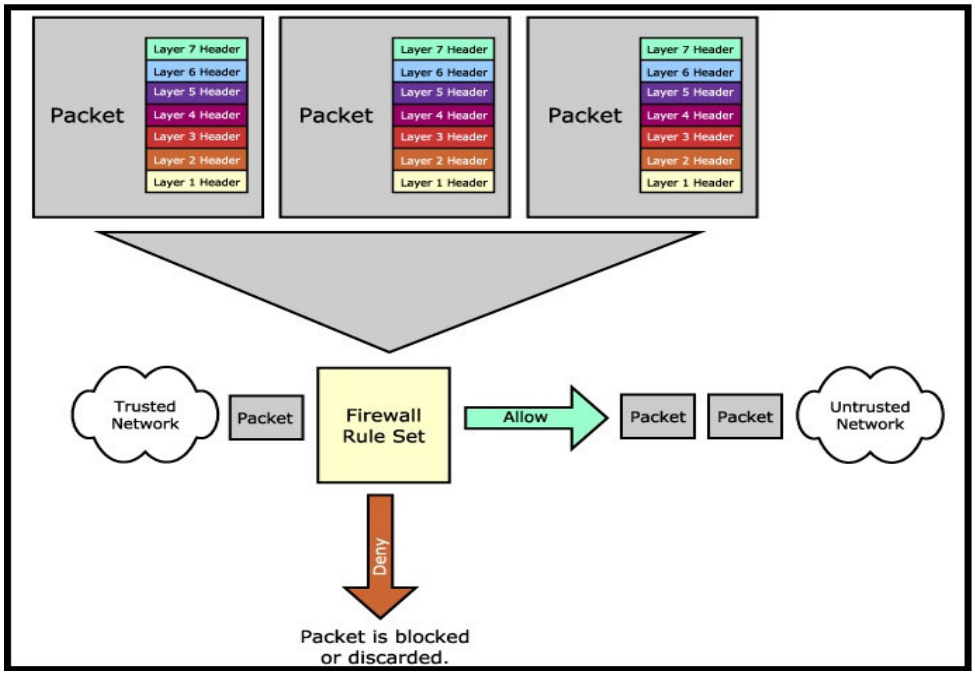

Figura 2 – Filtro de pacotes baseado em estados
Fonte: SPOHN, 1997.

Esse filtro se torna mais eficaz, pois o conjunto de regras é utilizado apenas no início das conexões, as quais usam os *flags* SYN. Esse fato faz com que se torne mais fácil administrar o sistema diminuindo as possíveis falhas que podem ocorrer quando implementado somente o filtro de pacotes (ALECRIM, 2004).

Para filtragem de pacotes UDP, que não temos conexão orientada, ou de pacotes RPC, o qual tem alocação dinâmica de portas, o *firewall* de pacotes baseado em estados apenas armazena dados de contexto, ou seja, o *firewall* mantém uma conexão virtual das comunicações UDP e RPC, e quando um pacote chega à rede ele é verificado com a tabela de estados e se a tabela indicar que existe uma sessão pendente desse tipo de pacote, o mesmo é aceito, caso contrário é negado, (NAKAMURA; GEUS, 2007).

Vantagens desse *firewall* (NAKAMURA; GEUS, 2007):

- Abertura temporária da rede;
- Baixo *overhead*/alto desempenho na rede;
- Aceita quase todos os tipos de serviço.

Desvantagens desse *firewall*

- Permite a conexão direta com redes externas;
- Não oferece autenticação de usuário.

2.1.3. *Firewall* em nível de aplicação

Funciona nas camadas de aplicação, sessão e transporte, como mostra na figura 3. Também conhecido como servidor *proxy*, proporciona tomada de decisões baseados nos dados da aplicação, além da análise de cabeçalhos TCP, UDP e IP (SPOHN, 1997).

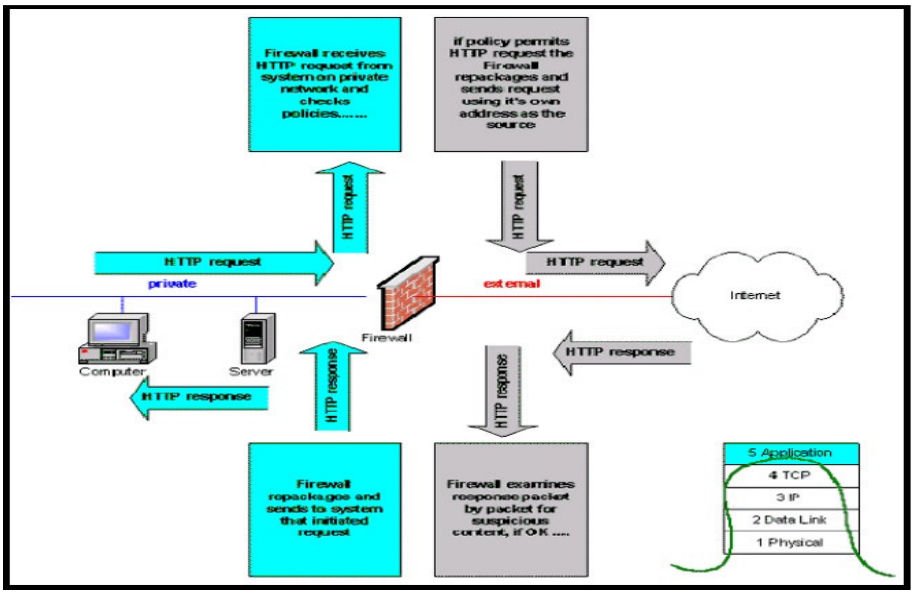

Figura 3 – *Firewall* em nível de aplicação
Fonte: SPOHN, 1997.

2.1.4. *Firewalls* Híbridos

Apesar das funcionalidades acima terem sido apresentadas separadamente, o que ocorre hoje em dia é a vinculação das três tecnologias no mesmo *firewall,* utilizando as vantagens de cada um deles acima paralelamente, esse modelo é conhecido como *firewall* híbrido. Na prática para os serviços que exigem alto grau de segurança são utilizados os *proxies* e para serviços que o desempenho é mais importante é utilizado os *firewalls* de pacotes e com base em estados (NAKAMURA; GEUS, 2007).

2.1.5. Proxy

Para o *proxy* funcionar corretamente, a conexão deve ser por TCP, pois precisamos que ela seja orientada. Resumidamente o usuário se conecta a uma porta TCP no servidor *proxy* e depois dessa conexão estabelecida, é liberado o acesso a conexão de uma rede externa após uma autenticação no *firewall*. O *proxy* pode trabalhar em três camadas: sessão, transporte (*circuit level gateway*) ou aplicação (*application level gateway*) (Figura 4), e por trabalhar na camada de aplicação, isso faz que ele tenha um maior controle sobre a interação cliente-servidor (NAKAMURA; GEUS, 2007).

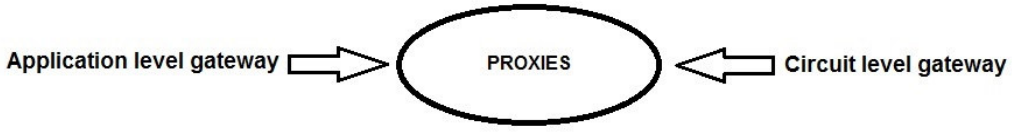

Figura 4 – Tipos de *proxies*
Fonte: NAKAMURA; GEUS, 2007.

O *proxy* também não permite a conexão direta do *host* interno com um servidor externo, pois ele mascara o IP do *host* interno e faz parecer que o tráfego teve origem no *proxy*, o que garante uma segurança a mais para a LAN. Basicamente temos duas conexões a cada requisição: uma do cliente para o *proxy* e outra do *proxy* para o servidor. Dessa maneira podemos proteger o cliente e o

servidor por meio do controle de requisição de serviços e garantir que certos eventos sejam proibidos (ALECRIM, 2004).

O servidor *proxy* é flexível e permite a criação de um código especial para cada serviço a ser aceito. Ele não é suficiente para se evitar ataques, porém agrega uma segurança a mais a rede. O *proxy* permite também a possibilidade de registrar todos os tráfegos da rede, possibilitando um aviso quando se tem um tráfego não confiável em andamento na rede (NAKAMURA; GEUS, 2007).

Vantagens do Proxy (NAKAMURA; GEUS, 2007):

- Não permite conexões diretas entre cliente-servidor;
- Autenticação de usuário;
- Analisa comandos da aplicação;
- Permite criação de logs do tráfego e de atividades especificas.

Desvantagens do Proxy:

- Mais lento comparado aos filtros de pacotes;
- Requer um *proxy* específico para cada aplicação;
- Não trata pacotes ICMP;
- Não aceita todos os serviços.

2.1.6. *Proxies* adaptativos

Diferentemente dos *firewalls* híbridos, os *proxies* adaptativos conseguem utilizar as diferentes tecnologias acima descritas de forma simultânea, ou seja, ele é capaz de utilizar dois mecanismos de segurança diferentes em um mesmo protocolo, garantindo assim um maior controle dos pacotes que entram e saem da rede, assim como uma maior segurança. O que caracteriza os *proxies* adaptativos são suas funções exclusivas (NAKAMURA; GEUS, 2007):

- Monitoramento bidirecional;
- Mecanismos de controle entre o *proxy* adaptativo e o filtro de pacotes baseado em estados;

- Controle dos pacotes que passam pelo *proxy* adaptativo;
- Habilidade de dividir o processamento do controle e dos dados entre a camada de aplicação e a cama de rede.

Baseado nas regras definidas no *proxy* adaptativo e com as características acima, quando um fluxo de pacotes precisa de uma maior segurança ele é direcionado para o *proxy* que realiza um controle a nível de aplicação e quando é identificado que um pacote precisa de mais desempenho do que segurança ele é direcionado aos filtros de pacotes e de estados (ALECRIM, 2004).

Em exemplo dessa aplicação é quando trabalhamos com o protocolo FTP (*File Transfer Protocol*). Esse protocolo utiliza duas conexões. A primeira conexão é para o tráfego de controle, essa conexão de controle envia os comandos FTP e é processado na camada de aplicação, de modo a garantir quais comandos serão permitidos e quais serão bloqueados. Após receber os pacotes da conexão de dados, o *proxy* adaptativo encaminha esses pacotes as regras de filtragem de filtros de pacotes para decidir se a transferência é permitida ou não.

Esse é um exemplo no qual o *proxy* adaptativo combina o controle da camada de aplicação, aumentando a segurança, e aumenta o desempenho na camada de rede através do uso dos filtros de pacotes e estados. Um exemplo desse *firewall* adaptativo é o Gauntlet, da Network Associates Inc. (NAKAMURA; GEUS, 2007).

2.2. ARQUITETURA

O principal objetivo de um *firewall* é garantir que todos os dados que trafeguem de uma rede para outra passem obrigatoriamente por ele, como mostra a Figura 5. Para isso é aconselhável realizar uma avaliação da arquitetura no qual o sistema será implantado, assim como o grau de segurança exigido, podendo ser utilizado quantos níveis de acesso forem necessários para adequar esse sistema (AWICHY; CHAPMAN, 1995).

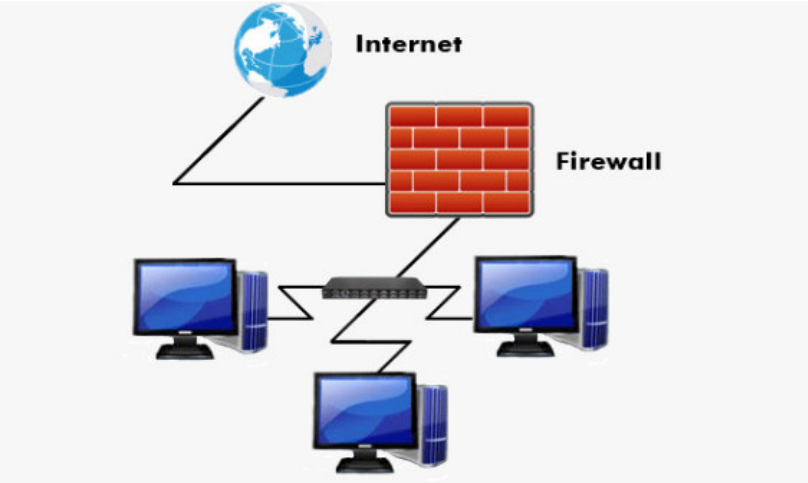

Figura 5 – Ilustração de um *firewall* na rede.
Fonte: COMPUTER COMPANY, 2012.

Existem algumas arquiteturas que servem como base para a implantação de um *firewall*, tais como: *Dual-homed Host, Screened Host e Screened Subnet.*

O *firewall* pode ser composto e agrupado de diversas formas, e sua arquitetura varia conforme as suas funcionalidades e necessidades dentro de um sistema de segurança. Algumas arquiteturas, podemos definir como clássicas, pois são modelos nos quais uma infinidade de outras variantes podem ser obtidas através delas (NAKAMURA; GEUS, 2007).

Nesse conceito de arquitetura, destaca-se a rede desmilitarizada (DMZ), ficando esta entre a rede externa e a interna, em um segmento separado. A Zona DMZ tem a função de separar os serviços externos, para minimizar os danos que uma invasão da rede local pode causar. Para isto, os computadores dentro de uma DMZ devem conter o mínimo de recursos possíveis, pois caso haja um ataque, a rede interna será protegida.

Para que isto ocorra são sugeridos vários modelos de segurança, formas de gerenciamento e implementação do *firewall*. Neste conceito, existem três arquiteturas clássicas, apresentadas abaixo (NAKAMURA; GEUS, 2007).

2.2.1. Dual-Homed Host Architecture

Na arquitetura *dual-homed host* pode ser implementada por um *host* que apresenta duas interfaces de rede, uma para LAN e outra para a rede externa, se tornando a única porta de entrada. Nessa arquitetura o roteamento é desabilitado, fazendo com que os pacotes não possam ser roteados entre as redes, garantindo o isolamento do tráfego, conforme apresenta a Figura 6 (AWICHY; CHAPMAN, 1995).

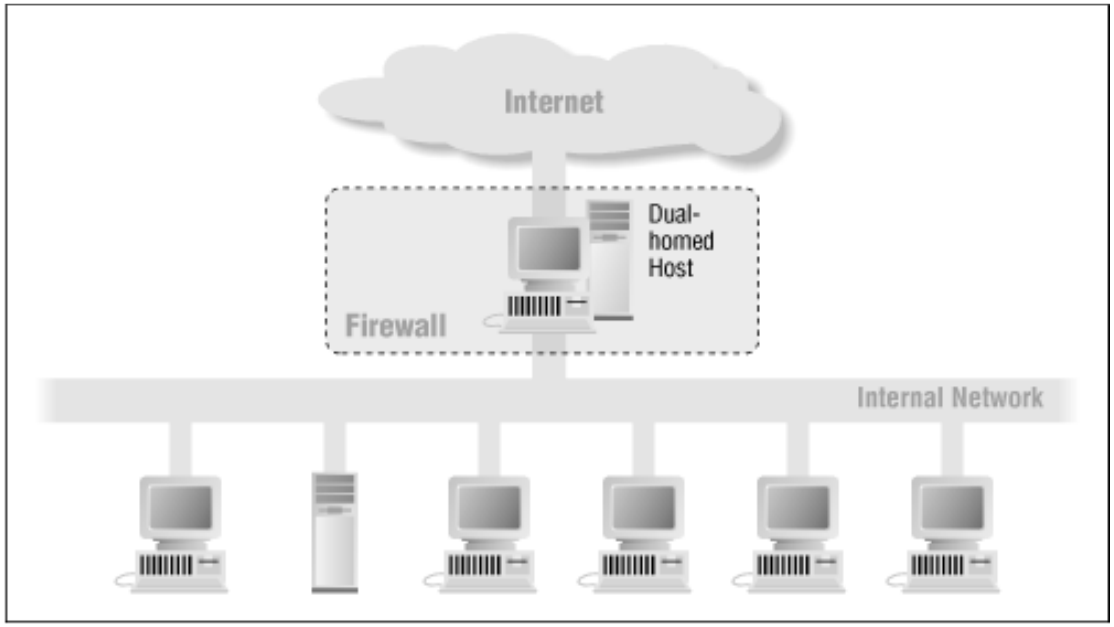

Figura 6 – *Dual-homed host architecture*
Fonte: AWICHY; CHAPMAN, 1995.

Assim, os pacotes IP de uma rede (por exemplo, a Internet) não são diretamente encaminhados para a outra rede (por exemplo, a rede interna protegida). Os sistemas externos e internos do *firewall*, podem se comunicar com *dual-homed host*, mas esses sistemas não podem se comunicar diretamente uns com os outros. O tráfego IP entre eles é completamente bloqueado.

É um sistema de arquitetura simples, mas pode se tornar um problema, pois o acesso externo para o usuário não é transparente, podendo tornar a rede indisponível (AWICHY; CHAPMAN, 1995).

Essa arquitetura é indicada para: uma rede que possua um tráfego pequeno para Internet, o tráfego para a Internet não seja vital para o negócio da empresa e que a mesma não provenha nenhum serviço para a Internet.

2.2.2. Screened Host Architecture

Em geral, arquiteturas desse tipo são seguras, porém não muito simples de se implementar. Tipicamente, configura-se um servidor principal com segurança reforçada, sendo ele o único ponto de comunicação entre a rede interna e a externa. Esse servidor é chamado de *bastion host (*o único *host* da rede interna acessível por *hosts* externos), conforme pode ser visto na Figura 7.

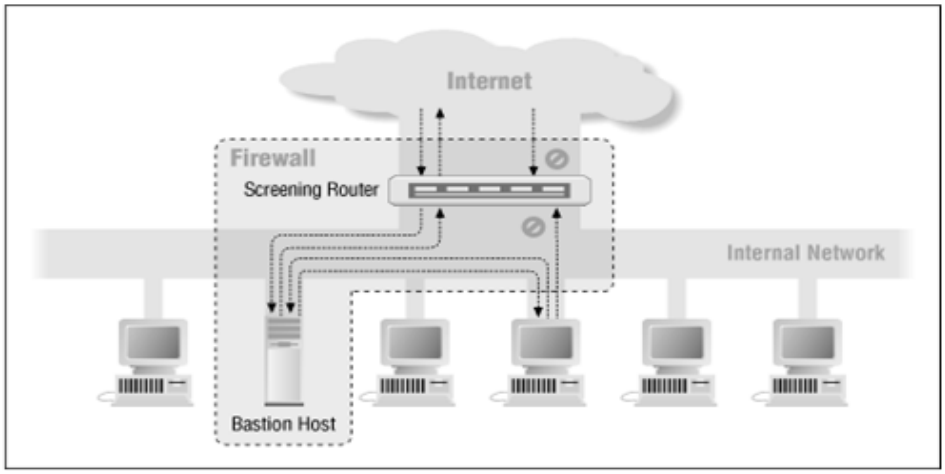

Figura 7 – *Screened host architecture*
Fonte: AWICHY; CHAPMAN, 1995.

A arquitetura *screened host* é formada por um filtro de pacotes que atua em um primeiro nível de defesa e é responsável por restringir conexões externas que não sejam direcionadas ao *bastion host*, ou seja, os usuários externos que quiserem acessar os sistemas internos deverão se conectar primeiramente com o *bastion host.*

Um problema dessa arquitetura, que pode ser observado é que, se o *bastion host* for comprometido o invasor terá acesso total à rede interna da organização (NAKAMURA; GEUS, 2007).

2.2.3. Screened Subnet Architecture

É considerada a mais segura, pois adiciona uma nova camada de segurança à arquitetura *screened host*. Baseia-se na criação de uma sub-rede, podendo ser uma zona DMZ, que isola a rede interna da externa, sendo ela a responsável por toda a comunicação entre as redes, além da criação do *bastion host*.

Conforme ilustra a Figura 8, uma arquitetura *screened subnet* é formada por um *bastion host* isolado pela sub-rede (ele fica na DMZ e caso seja comprometido, o filtro interno ainda protegerá a rede interna), um roteador responsável pela comunicação entre a rede interna e o *bastion host* e outro responsável pela comunicação entre o *bastion host* e a rede externa.

Para invadi-lo o ataque teria que passar por ambos os roteadores. Dessa forma, a zona de risco é reduzida drasticamente (AWICHY; CHAPMAN, 1995).

Vale ressaltar que as arquiteturas apresentadas são as mais comumente utilizadas, porém não são regras, elas servem apenas como orientação e referência teórica, não existindo uma arquitetura única, a qual irá resolver todos os problemas de segurança.

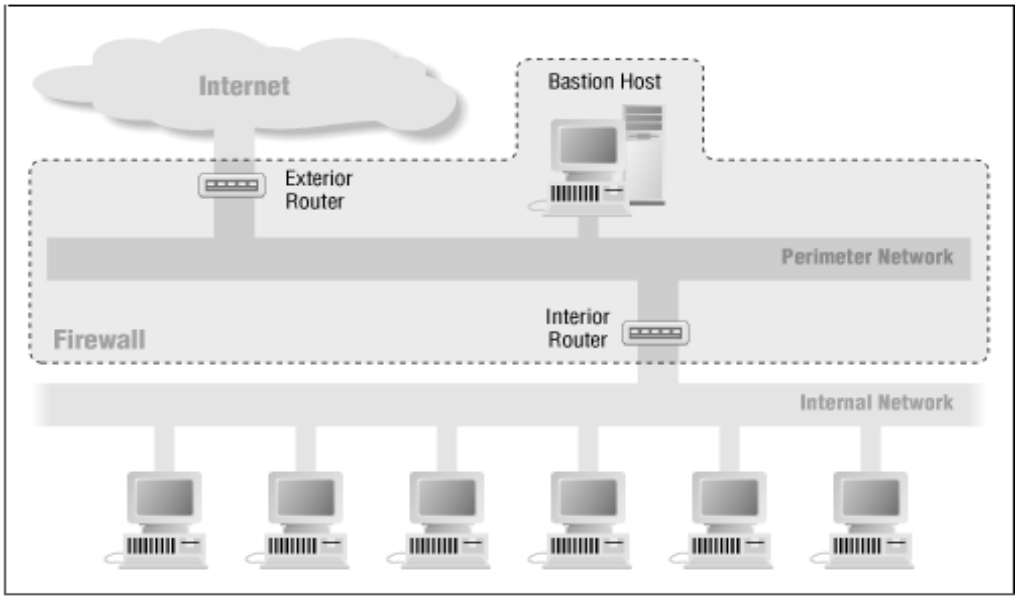

Figura 8 – *Screened subnet architecture*
Fonte: AWICHY; CHAPMAN, 1995.

2.3. NECESSIDADE DE UM *FIREWALL* NA EMPRESA

Com um sistema de segurança *firewall* podemos controlar inspecionar, aprovar ou rejeitar cada tentativa de conexão feita entre a rede interna e a rede externa, Internet. Os *firewalls* de grande eficiência devem proteger uma rede em todas as camadas do sistema OSI (*Open Systems Interconnection*), que vai da camada de enlace até a camada de aplicação. No entanto, um *firewall* sozinho, ou seja, um *software* dele instalado sem estar configurado devidamente, com um banco de regras bem definido, somente irá consumir inutilmente recursos de *hardware* e *software*, aumentando assim, o tempo necessário para conectar, autenticar e criptografar os dados em uma rede.

Devemos estar atentos a estes problemas, e configurar adequadamente o *firewall* e seus componentes nas fronteiras da rede, interconexões ou *gateways*, que fornecem o acesso a outras redes. É de suma importância observar que a implantação de um *firewall* em uma rede serve somente como uma ferramenta utilizada para impor uma política de segurança, tão eficiente quanto à própria política de segurança empregada na rede pelo projetista ou administrador, mas que não é capaz de resolver as questões de segurança sozinho (GONÇALVES, 2000).

É bom ter em mente que as políticas de segurança precisam estar bem estruturadas, pois elas ditam muitas das configurações do *firewall*. Abaixo segue alguns itens que devem ser considerados na implantação de um *firewall*:

- Uso indevido dos serviços autorizados. Um *firewall* não pode impedir que alguém use uma sessão *telnet* (serviço que permite que uma máquina cliente possa acessar e executar tarefas em um servidor) autenticada, para comprometer as máquinas internas, por exemplo.
- Usuários conectados antes do sistema de proteção *firewall*. Um *firewall* não poderá restringir as conexões que não passam por ele. Portanto, não poderá protegê-lo contra pessoas que evitam o *firewall*, por exemplo, por meio de um servidor *dial-up*, que pode ser implantado antes do *firewall*.
- Engenharia social. Se os intrusos puderem, de alguma forma, obtiver senhas, as quais não estão autorizados a ter ou comprometer de alguma outra forma os mecanismos de autenticação por meio de engenharia social, o *firewall* não os impedirá. Por exemplo, um invasor poderá ligar para um de seus usuários

fingindo ser o administrador do sistema e pedir sua senha para resolver um problema.

- Falhas no sistema operacional. Um sistema de segurança baseado em um *firewall* oferece segurança tão quanto o sistema operacional em que está instalado. Existem muitas falhas presentes nos sistemas operacionais, contra as quais um *firewall* não pode protegê-lo. É por isso que é importante proteger corretamente o sistema operacional aplicando os *patches* (aplicativos utilizados pra corrigir possíveis erros em um sistema operacional) de segurança necessário antes de instalar o *firewall* e atualizando periodicamente os *patches* após a completa instalação do *firewall*.
- Evolução das ameaças. Normalmente os invasores estão à frente dos projetistas e fabricantes de *firewalls*, os quais desenvolvem aplicativos sobre os problemas e falhas descobertos pelos invasores. Assim, um *firewall* por mais atual que seja não pode proteger a rede e o sistema com totalidade.

Assim sendo, alguns outros itens também são relevantes e necessários para aprimorar a segurança do *firewall* em si, como evitar ataques de diversos tipos, tais como:

- Ataques DoS (*Denial of Service*) – Ataques a servidores para impedir que usuários consigam resposta para suas requisições. Isso pode ser realizado inundando o servidor, e seus roteadores conectados, com pedidos de informações numerosos demais para que o sistema possa gerenciar (FRANKLIN, 2013).
- Ataques *Spoofing* – Ataques que consistem em mascarar (*spoof*) pacotes IP utilizando endereços de remetentes falsificados (INTERNET SECURITY SYSTEMS, 2013);
- Bloqueio qualquer e todo tipo de conexão SYN;
- Bloqueio de serviços;
- Bloqueio de acesso não-autorizados.

3. *FIREWALL* ASA 5500

Atualmente existe uma infinidade de modelos de *firewall* disponíveis no mercado, que abrangem desde tecnologia proprietária até *softwares* gratuitos ou de código aberto. Não há um modelo universal apropriado para todos e para a escolha do *firewall* deve ser considerado alguns pontos como a estrutura particular da rede o qual é diferente para cada empresa, assim como as suas políticas de segurança e o objetivo ao qual o *firewall* precisa cumprir na estrutura da empresa (GONÇALVES, 2000).

O mercado de hoje possui empresas como StoneSoft, WatchGuard, Fortinet, SonicWALL, Juniper, Checkpoint, BRconnection e Cisco que desenvolvem soluções completas na área de segurança e cada empresa amplia características diferentes nos seus *firewalls* fazendo com que cada uma delas se torne particular no mercado e sendo o ideal dependendo do dependendo da necessidade do cliente.

Nesse trabalho será analisado o *firewall* ASA, que se trata da nova geração de equipamentos de segurança da empresa Cisco, a qual aposentou a antiga marca conhecida como “PIX”. A escolha desse *firewall* em especifico se deu pelo fato do fabricante Cisco ser um dos líderes no mercado nas soluções de rede e o uso desse *firewall* tem se popularizado em ambientes corporativos.

A solução de *firewall* da Cisco é projetada de acordo com as melhores práticas e orientações desenvolvidas pelas soluções do mundo real, visando que todo *firewall* baseia-se em plataformas modulares e escalonáveis, e são projetadas para acomodar requisitos de segurança de diversos ambientes da rede. O *firewall* ASA pode ser implantado de forma independente para proteger uma área específica da infra-estrutura de rede ou pode ser combinado a uma abordagem de defesa profunda e em camadas ao ser combinada com outros equipamentos.

Pelo fato do *firewall* da família ASA ser totalmente adaptável a diferentes ambientes, e podendo ser implantado desde uma pequena empresa até uma de grande porte, o mesmo foi escolhido para ser apresentado como solução nesse trabalho.

3.1. INTRODUÇÃO AOS SISTEMAS CISCO ASA

Os sistemas ASA foram apresentados pela Cisco Systems em 2005, com o objetivo de unificar os serviços de três famílias de *appliances* existentes:

- l Cisco PIX *Appliances* – fornecia serviços de filtragem de pacotes e tradução de endereços;
- l Cisco VPN *Concentrators* – suportava redes privadas virtuais;
- l Cisco IPS *Series* – sistemas de detecção e prevenção de intrusão.

O Cisco ASA 5500 Series inclui o Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580 e 5585-X *Adaptive Security*, esta linha de equipamentos traz um novo nível de segurança e controle de políticas de aplicativos e redes. O MPF (*Modular Policy Framework*) permite políticas de segurança específicas de fluxo altamente personalizável que são adaptáveis às necessidades de aplicação em cada empresa.

O desempenho e a extensibilidade da Cisco ASA 5500 *Series* é reforçada através SSMs (*Security Services Modules*) instalados pelo usuário. Essa arquitetura flexível permite às empresas implementar rapidamente serviços de segurança quando e onde eles são necessários, tais como a adaptação de técnicas de inspeção para aplicação específica e as necessidades do usuário ou a adição de prevenção de intrusão adicional e serviços de segurança de conteúdo, como aqueles entregues pela AIP (*Advanced Inspection and Prevention*) e CSC (*Content Security and Control*). Além disso, a arquitetura de *hardware* modular do Cisco ASA 5500 Series, juntamente com o poderoso MPF, proporciona a flexibilidade necessária para atender às futuras exigências de segurança da rede e, estendendo a excelente proteção de investimento fornecidos pela Cisco ASA 5500 *Series* e permitindo que as empresas se adaptarem as suas defesas de rede a novas ameaças que possam surgir.

Na figura 9 são apresentadas as características básicas dos modelos ASA:

Característica	5505	5520	5540	5550	5580-40
Memória RAM	512 MB	1 GB	2 GB	4 GB	12 GB
Capacidade de filtragem	150 Mbit/s	450 Mbit/s	650 Mbit/s	1 Gbit/s	10 Gbit/s
Máximo de ligações simultâneas	10,000	280,000	400,000	650,000	2,000,000
Máximo de ligações por segundo	4,000	12,000	25,000	36,000	150,000
Capacidade VPN 3DES/AES	100 Mbit/s	225 Mbit/s	325 Mbit/s	425 Mbit/s	1 Gbit/s
Máximo de sessões VPN SSL	25	750	2500	5000	10,000
Capacidade de expansão	1 SSC	1 SSM	1 SSM	Não	6 IC
Prevenção de intrusão	Sim, c/ AIP SSC	Sim, c/ AIP SSM	Sim, c/ AIP SSM	Não	Não
Filtragem de conteúdos	Não	Sim, c/ CSC SSM	Sim, c/ CSC SSM	Não	Não
Tolerância a falhas	Não	Sim	Sim	Sim	Sim
Balanceamento de carga	Não	Sim	Sim	Sim	Sim
Contextos de segurança (max)	0	20	50	100	250

Figura 9 – Modelos da família ASA 5500
Fonte: CISCO SYSTEM, 2013

Todos os aparelhos da série ASA 5500 da Cisco oferecem soluções de VPN, IPsec (*Internet Protocol Security*) e SSL (*Secure Sockets Layer*) / DTLS (*Datagram Transport Layer Security*), *Clientless* e recursos *AnyConnect* VPN licenciados, convergindo SSL e serviços de VPN IPsec com tecnologias abrangentes na defesa contra ameaças, o Cisco ASA 5500 *Series* fornece acesso à rede altamente personalizável adaptados para atender os requisitos de ambientes de implantação diversos. Dentre os vários equipamentos Cisco 5500 *Series* destacaremos o modelo 5520 e o 5585 devido sua ampla utilização nas empresas.

3.1.1. Modelo ASA 5520

O Cisco ASA 5520 oferece serviços de segurança com ativo/ativo de alta disponibilidade e conectividade, *Gigabit Ethernet* para redes corporativas de médio porte em um aparelho modular, de alto desempenho. Com quatro interfaces *Gigabit Ethernet* e suporte para até 100 VLANs (*Virtual Local Area Network*), as empresas podem facilmente implantar o Cisco ASA 5520 em várias zonas dentro de sua rede.

As empresas podem aumentar sua capacidade de VPN SSL e IPsec para suportar um maior número de trabalhadores móveis, locais remotos e parceiros de negócios. Até 750 *AnyConnect* e/ou *clientless peers* de VPN, pode ser suportado em cada Cisco

Instalando uma licença Premium ou essencial, a capacidade de VPN e resiliência pode ser aumentada aproveitando o agrupamento integrado VPN do ASA 5520. O Cisco ASA 5520 suporta até 10 aparelhos em um *cluster*, oferecendo um máximo de 7500 AnyConnect e / ou clientless VPN IPsec VPN ou 7.500 pares por *cluster*.

O avançado sistema de segurança de camada de aplicação e as defesas de segurança de conteúdo fornecido pela Cisco ASA 5520 garantem prevenção de intrusão de alto desempenho e capacidades de mitigação da SSM AIP, ou a completa proteção contra *malware* da SSM CSC. Usando os recursos de contexto de segurança opcionais do Cisco ASA 5520, as empresas podem implantar até 20 *firewalls* virtuais dentro de um aparelho para ativar o controle compartimentado das políticas de segurança em nível departamental. Esta virtualização reforça a segurança e reduz o gerenciamento global e os custos de suporte, enquanto há consolidação de vários dispositivos de segurança em um único aparelho.

3.1.2. Modelo ASA 5585

Cisco ASA 5585-X são adaptados para atender as necessidades de alto desempenho dos centros de dados e apoiando as contagens mais altas da sessão VPN e o dobro de conexões por segundo dos *firewalls* concorrentes em sua classe,

Cisco ASA 5585-X. Este equipamento visa atender às crescentes necessidades das organizações mais dinâmicas da atualidade. Os aparelhos combinam *firewall* mais avançados do mundo com IPS *(Intrusion Prevention Service)* eficazes mais abrangentes da indústria, oferecendo a solução de segurança mais eficaz na indústria para diminuir significativamente os riscos a segurança. Há quatro modelos de Cisco ASA 5585:

- Cisco ASA 5585-X com SSP-10 (*Security Services Processor)*-10 oferece 2 Gbps de performance de *firewall* multi-protocolo;
- Cisco ASA 5585-X com a SSP-20 fornece 5 Gbps de multi-protocolo de performance de *firewall*;
- Cisco ASA 5585-X com a SSP-40 oferece 10 Gbps de *firewall* multi-protocolo desempenho;
- Cisco ASA 5585-X com SSP-60 oferece 20 Gbps de *firewall* multi-protocolo.

Todos os quatro modelos ASA 5585-X dispõem de escalabilidade excepcional para atender às exigentes necessidades de expansão das grandes empresas, também podem suportar até 10 mil sessões de VPN simultâneas, ao efetuar até duas vezes as conexões por segundo e até quatro vezes a contagem de sessão de outros *firewalls* semelhantes. Os aparelhos também oferecem o dobro da eficácia e da cobertura ameaça mais abrangente de todas as IPS.

4. EXEMPLOS PRÁTICOS

Visando demonstrar a aplicação do *firewall* ASA na prática, utilizaremos de três exemplos implantados em ambientes corporativos para demonstrar como ocorre a implantação desse equipamento, e como ele pode vir a ser uma das opções favoráveis no mercado.

Os nomes das empresas foram alterados para nomes fictícios, e algumas outras informações de importância relevantes foram retiradas, pois é necessário garantir que as informações pertinentes a segurança de dados da empresa para que não sejam divulgadas a pessoas mal-intencionadas.

4.1. EXEMPLO 1 – EMPRESA ALFA

A empresa Alfa é uma empresa de grande porte que se encontra no Nordeste do país, e presta serviços ao governo e precisa prezar pela segurança dos seus dados, pois trabalha com dados confidenciais. Na sua estrutura inicial, a empresa já possuía *firewalls* da Fortinet, porém o modelo já estava ultrapassado, possuía um desempenho baixo e já não atendia a necessidade da empresa.

No inicio de 2013 a empresa Alfa buscava a substituição dos *firewalls* a fim de manter-se com os seus equipamentos com alta disponibilidade, aproveitar melhor a escalabilidade, e garantir que o desempenho e a segurança dos dados do DataCenter não fossem comprometidos. A empresa também procurava um *firewall* com um *hardware* que possuísse uma arquitetura em forma de *appliance*, e com capacidade para operar com mais de 1 milhão de sessões simultâneas e suportar a criação de no mínimo 50 mil novas conexões por segundo.

A solução para atender as necessidades dessa empresa, envolveu à implantação de dois ASA 5585, juntamente com o Cisco *Security Manager* (CSM) para garantir uma boa gerencia de segurança dos dados da empresa.

Abaixo segue o modelo ASA 5585 implantado no cliente:

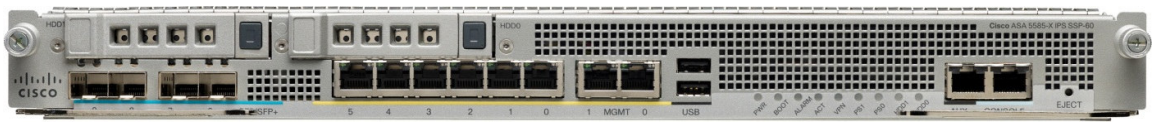

Figura 10 – ASA 5585
Fonte: CISCO SYSTEM, 2013

A primeira parte da implantação foi realizar a atualização do *IoS (Internetwork Operating System)* do equipamento. Devido ao ambiente da empresa exigir alta disponibilidade, principalmente trabalhando com o número de acessos e conexões, o equipamento foi configurado com a versão 8.4(5) ao invés da ultima versão 9.1 disponível, visando obter um ambiente mais estável e seguro. Como não era a ultima versão, foi utilizado o comando abaixo para evitar a atualização automática do sistema e forçar a versão determinada:

```
boot system disk0:/asa845-smp-k8.bin
asdm image disk0:/asdm-711-52.bin
```

Após a atualização do IoS do equipamento, foi realizada a conexão da interface de gerenciamento à rede de gerencia da empresa e através dela foram realizadas as primeiras configurações para permitir o acesso através da rede de gerencia.

Na Alfa, os usuários utilizam autenticação via radius, os acessos foram configurados para utilizarem os protocolos através SSH, HTTPS (*HyperText Transfer Protocol Secure*), SNMP (*Simple Network Management Protocol*) e acesso por VPN não foi configurado. Funcionalidades de *Traffic Shapper*, NAT, *Schedules, Static Routes* não foram implantadas, pois não estavam em uso na empresa, porém seriam posteriormente implementadas.

A fim de garantir alta disponibilidade, os dois *firewalls* foram configurados em redundância ativo/ativo. O *firewall* em modo ativo/ativo na verdade consiste de um *firewall* com um contexto em modo ativo e outro *backup*, da mesma forma que o *firewall* dois estará com um contexto ativo e outro *backup* (inversamente), conforme pode ser observada na Figura 11 abaixo:

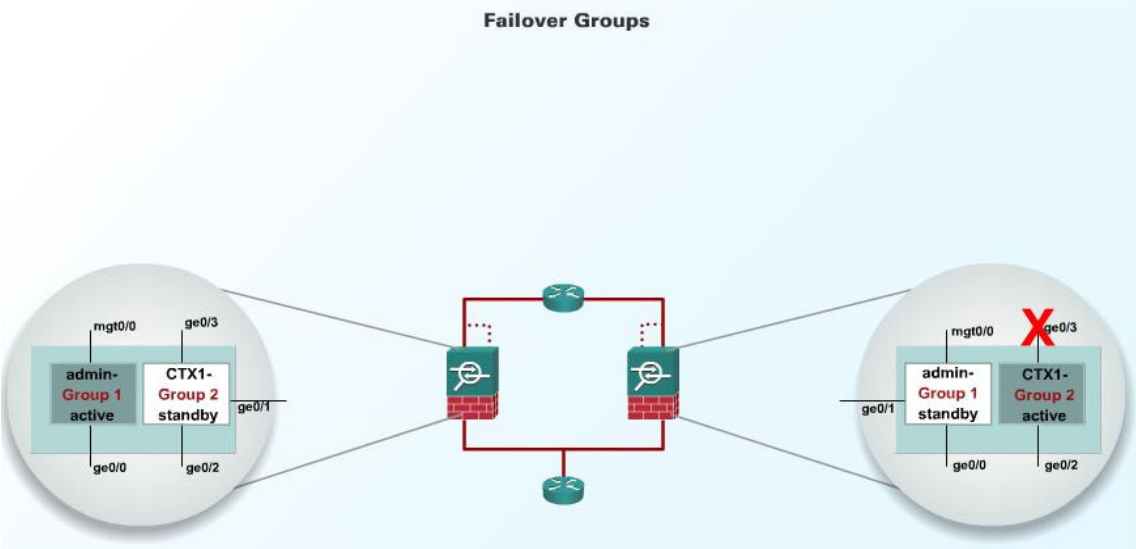

Figura 11 – *Firewalls* em redundância ativo/ativo
Fonte: Autoria Própria

Abaixo segue a topologia (Figura 12) a qual essa configuração foi ativada. Os endereços IPs foram modificados a fim de garantir a seguranças das informações:

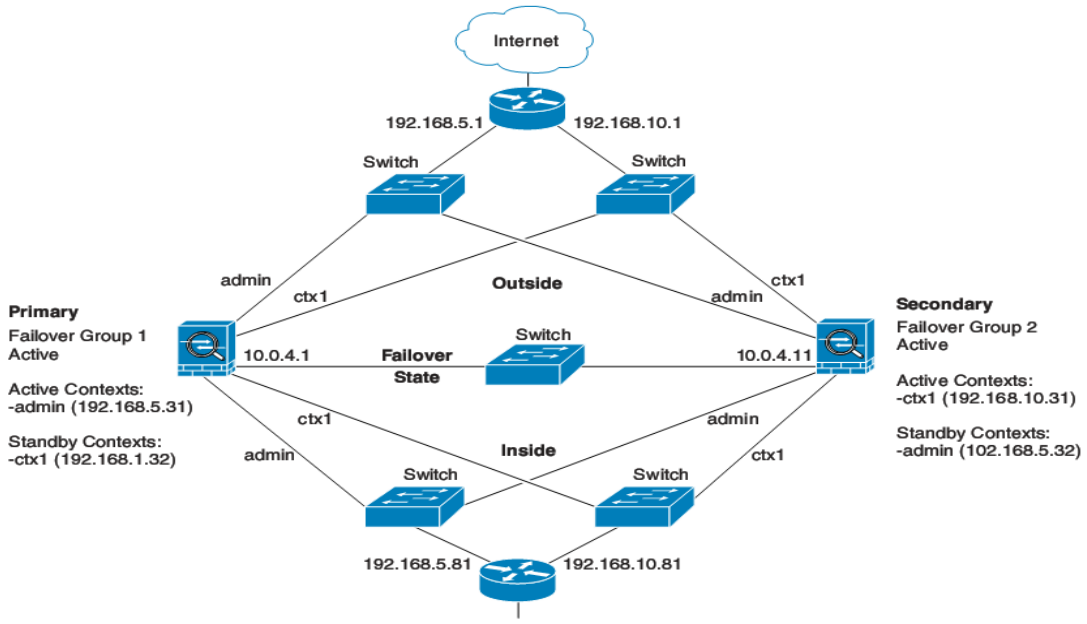

Figura 12 – Topologia da empresa Alfa
Fonte: Autoria Própria

Para trabalhar com uma redundância ativo/ativo, deve-se primeiro configurar o *firewall* com múltiplos contextos, através do comando: "*mode multiple*". Pode-se verificar qual é o modo do equipamento, com o comando "*show mode*":

```
ciscoasa# show mode
Security context mode: multiple
```

É necessário configurar o *firewall* em modo transparente. Tradicionalmente, um *firewall* encaminha os seus pacotes e age como gateway padrão para os *hosts*, um *firewall* em modo transparente, por outro lado, possui suas interfaces configuradas em camada 2 e age como um *firewall* "oculto" na rede e não conseguimos identificá-lo através de saltos, conforme Figura 12.

Na configuração de um *firewall* como transparente, basta na linha de comando entrar em modo de configurar e indicar o *firewall* como transparente:

```
ciscoasa(config)# conf t
ciscoasa(config)# firewall transparent
```

A partir deste ponto, pode-se configurar o *firewall* com redundância ativo/ativo via ASDM (*Adaptive Security Device Manager)* – interface gráfica do *firewall* ou CLI (*Command-Line Interface*) – linha de comando.

Via CLI (no contexto system):

```
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby
10.0.4.11
failover group 1
primary
preempt
failover group 2
secondary
preempt
```

```
admin-context admin
context admin
description admin
allocate-interface Ethernet1
allocate-interface Ethernet2
config-url flash:/admin.cfg
join-failover-group 1
context ctx1
description context 1
allocate-interface Ethernet3
allocate-interface Ethernet4
config-url flash:/ctx1.cfg
join-failover-group 2
```

Via CLI (no contexto admin):

```
interface Ethernet1
nameif outside
security-level 0
interface Ethernet2
nameif inside
security-level 100
ip address 192.168.5.31 255.255.255.0 standby 192.168.5.32
monitor-interface outside
monitor-interface inside
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
ssh 192.168.5.72 255.255.255.255 inside
```

Via CLI (no contexto ctx1):

```
interface Ethernet3
nameif inside
security-level 100
interface Ethernet4
nameif outside
security-level 0
access-list 201 extended permit ip any any
```

```
access-group 201 in interface outside
logging enable
logging console informational
ip address 192.168.10.31 255.255.255.0 standby 192.168.10.32
monitor-interface inside
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.1 1
```

No *firewall* 2, foi executado o seguinte:

```
firewall transparent
failover
failover lan unit secondary
failover lan interface folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby
10.0.4.11
```

Após essa implantação foi observado à necessidade de algumas melhorias no ambiente da empresa Alfa, porém, seria necessário o cliente rever as suas políticas de segurança e ficaram a critério do cliente para futuras implementações.

A primeira observação foi referente as lista de acesso. Foram configuradas somente 3 grandes ACL (*Access Control List*), e esta aplicadas em todas as interfaces *inside* do *firewall*, porém o recomendado é replicar a ACL para outras interfaces e limpar cada ACL deixando somente as regras referentes à aquela interface ao qual a regra está aplicada. Desta forma o gerenciamento será facilitado e o uso de CPU do *firewall* pode ser otimizado.

A segunda observação, foi referente as regras e seus vencimentos, pois a empresa resolveu adotar o método de agendamentos para vencimentos de regras, porém isso não é muito comum. Foi aconselhado revisar esse ponto e implantar um mecanismo de verificação, o qual possa validar e remover estas regras, fazendo com que o *firewall* acompanhe as mudanças do ambiente. As melhores práticas sugerem que toda concessão no *firewall* deve ter prazo de validade e deve ser renovado se este prazo persiste desta forma há um controle das regras e uma validação da sua necessidade.

4.2. EXEMPLO 2 – EMPRESA BETA

A empresa Beta é um órgão governamental presente no Brasil todo, com uma matriz e 25 filiais, as quais trabalham com informações confidenciais e é essencial que o seu sistema de segurança esteja sempre protegido e disponível. Visando principalmente a alta disponibilidade o órgão decidiu substituir os seus *firewall por uma s*olução de *firewall* em *cluster* composto por 2 nós, que permitisse realizar a gerência de cada *cluster* e capaz de realizar a emissão de relatórios.

A solução adquirida possui como características a alta disponibilidade e redundância por meio de *cluster* em modo ativo/ativo com balanceamento de carga, de maneira que caso um dos nós do *cluster* fique indisponível, todas as conexões sejam direcionadas para o nó ativo de forma transparente para os usuários finais, sem perdas das conexões ativas em caso de falhas em uma das unidades.

As funcionalidades de gerência da solução de cada *cluster* deveriam possuir características como manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de *firewall*, gerência, armazenamento de logs, permitindo autenticação dos usuários em VPNs e emissão de relatórios.

Para atender a essa demanda, foi instalado em cada filial dois *firewalls* ASA 5585 e dois módulos ASA 5585-SSM-IPS10. Os módulos instalados permitem a configuração das funcionalidades de IPS e VPN acelerada por *hardware*. O módulo AIP-SSM em si possui apenas 1 interface *Gigabit* para gerência (configuração, *download* de atualizações, etc.).

O módulo SSM pode operar no modo promíscuo ou no modo *inline*. No modo promíscuo, apresentado na Figura 13, os pacotes são duplicados para que o módulo analise o tráfego, mas não tendo domínio sobre o fluxo, sendo que apenas pode solicitar (via pacotes) que uma conexão seja bloqueada ou reiniciada, bem como que um alerta seja gerado.

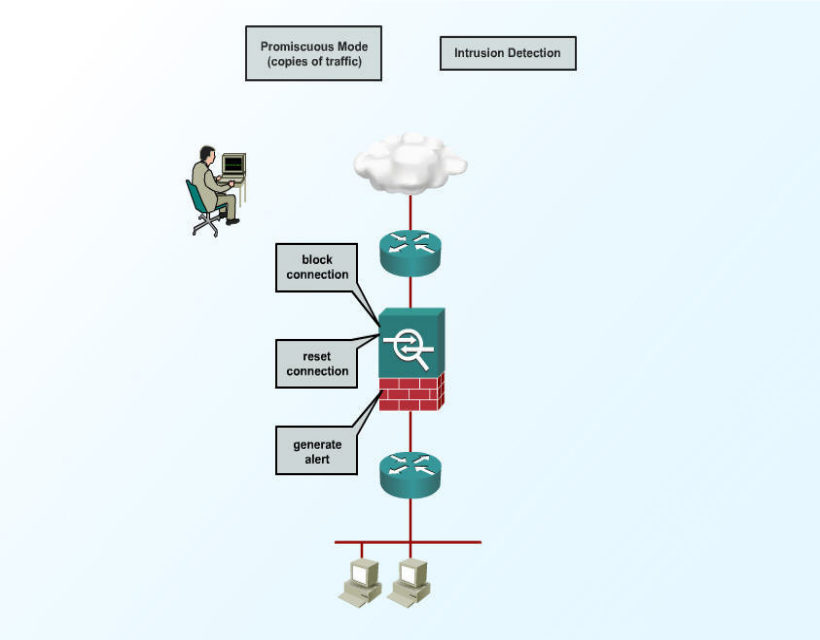

Figura 13 – Modos de operação – Promíscuo
Fonte: Autoria própria

No modo *inline*, apresentado na Figura 14, o módulo sempre estará “no meio” do fluxo, podendo tomar a liberdade de bloquear o mesmo sem que este saia do *firewall*. Caso o módulo falhe, pode-se configurar para que o tráfego passe desprotegido (sem resultar em perda), ou seja, bloqueado.

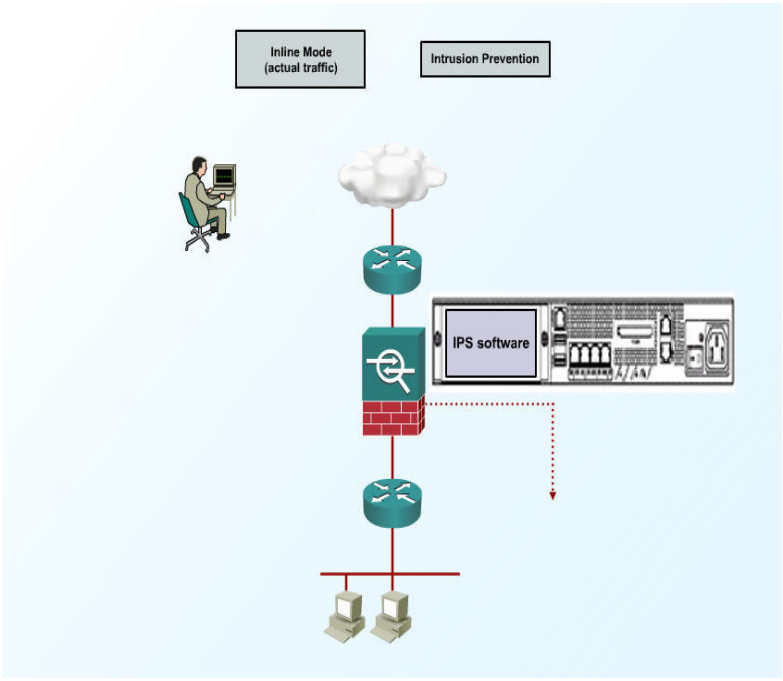

Figura 14 – Modos de operação – *Inline*
Fonte: Autoria própria

Para exemplificar, utilizaremos a implantação da filial do Pará. Para atender essa filial foi instalado dois ASA 5585 com o sistema operacional 8.4(4)9 e o sistema operacional do IPS foi o 7.1(6)E4. Antes da implantação, a rede interna da filial possuía apenas uma VLAN e os servidores que fornecem serviços externos eram hospedados na rede interna. Para uma melhora implantação as migrações dos serviços externos para a DMZ foi feita gradativamente e quando migrados os serviços foram publicados com NAT 1:1 configurado nos objetos. A rede interna também foi gradativamente migrada para o bloco 10.22.0.0/16 e foram criadas inicialmente 4 VLAN, assim todos os serviços, servidores e usuários forem migrados para a DMZ e para a nova rede interna o *firewall* Linux foi desativado.

Foram usadas listas de acesso por interface ao invés de ACL global e foi adicionada à inspeção de protocolos padrão a inspeção de ICMP, conforme abaixo:

```
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
inspect icmp
!
```

As principais formas de detecção de intrusos, através do módulo de IPS são:

- *Stateful pattern recognition* – Reconhecimento do perfil de tráfego por assinatura;

- *Protocol analysis* – Análise de protocolos, verificando se o protocolo se encontra em conformidade com as RFCs (*Request for Comments*), etc.;
- *Traffic anomaly detection* – Detecção de anomalia no tráfego, como comportamento anormal de um conjunto de protocolos, alta utilização, etc.;
- Protocol anomaly detection – Detecção de anomalia no protocolo, como protocolos condizentes com a RFC, contudo, passando conteúdo não nativo daquele protocolo.

O módulo de IPS foi ativado para monitorar somente a interface *outside* e em modo de aprendizado. Nesse modo o *firewall* gerar alarmes e detecta os ataques, mas as ações de bloqueio são removidas através do recurso *Event Action Filters*.

A estratégia de implantar o IPS em modo de aprendizado permite que os administradores da rede tratem os falso-positivos antes de efetivarem as ações de bloqueio dos eventos. Foi mantido o *Action Override HIGHRISK,* que adiciona a ação de bloquear pacotes em linha para os eventos que possuem *Risk Rating* (RR) entre 90 e 100.

O *Global Correlation* foi ativado para levar em conta a reputação do atacante no cálculo do RR. Dessa forma aumenta-se a probabilidade de bloquear um atacante com reputação negativa, de acordo com o a base de dados de reputação global mantida pela Cisco.

Para exemplificar as configurações, abaixo segue como foi configurado o *firewall* secundário do *cluster*:

1. Conectar as interfaces do ASA secundário à sua respectiva VLAN.

2. Conectar a interface management1/0 do IPS à sua respectiva VLAN.

3. Fazer a configuração inicial do IPS através da CLI.

3.1 A partir do modo privilegiado do ASA secundário, executar o comando:

```
hw-module module 1 password-reset.
```

3.2 Depois de o módulo reiniciar deve-se executar o comando:

```
session 1
```

Usuário e senha: cisco

3.3 Após o login será solicitada a alteração da senha.

4. Atualizar o *software* do IPS para a versão 7.1(6)E4.

5. Licenciar o IPS através do CSM e aplicar a atualização das assinaturas versão 6.85. O *download* das assinaturas pode ser feito diretamente do site da Cisco, primeiro é necessário criar um usuário no link https://tools.cisco.com/RPF/register/register.do.

Depois de criada a conta, deve-se associar o contrato de suporte do ASA e dos IPS à conta: http://www.cisco.com/web/Downloads/SDS/unentitled_instructions.html.

6. Atribuir as políticas compartilhadas de IPS do CSM ao novo IPS.

7. Atribuir a interface portchannel 0/0 para o vs0 sob a seção *Platform* das configurações do IPS do *firewall* secundário.

8. Espelhar o modo da detecção de anomalia (*learn* ou *detect*) do IPS1 no IPS2.

9. Atualizar o *software* do ASA para a versão 8.4.4(9).

10. Copiar para o ASA a versão 6.4.9(103) do ASDM.

11. Gerar as licenças do ASA no site https://cisco.com/go/license.

12. Aplicar as configurações de *failover* no ASA secundário.

Para configurar via ASDM, no mínimo 1GB de RAM (*Random Access Memory*) são necessários. O mesmo feito pode ser realizado por CLI (*telnet*, ssh), sem exigências de memória. As demais configurações envolvem atribuir a licença e configurar o update automático de assinaturas.

Para demais funcionalidades, Anti-X, como Anti-virus, Anti-SPAM, Anti-*Spyware*, *Anti-Phishing*, além de controle de URL (*Uniform Resource Locator*), etc. deve-se utilizar o módulo CSC-SSM, adquirido separadamente. Não é possível utilizar 2 módulos ao mesmo tempo (ex: 1 AIP-SSM e 1 CSC-SSM).

A ferramenta *packet tracer* (encontrada em *Tools* no ASDM) é muito útil para analisar o fluxo que um pacote segue, auxiliando no *troubleshooting*.

As VPNs permitem a facilidade do acesso remoto à rede corporativa, por outro lado as VPNs também apresentam um dos canais primários para ameaças remotas como *worms*, vírus e aplicativos indesejados, logo a segurança dos recursos corporativos deve ser estendida aos funcionários com acesso remoto a empresa. Através do *firewall* ASA 5585, conseguimos configurar o controle de acesso, através da inspeção e controle dos aplicativos, controle de acesso por usuário, detecção de anomalias de protocolo e *Stateful packet filtering* que trata-se de uma funcionalidade que filtra o tráfego no destino e na origem dos endereços IPs, portas, *flags*. Outra funcionalidade é a "*stateful inspection*", funcionalidade a qual realiza a inspeção de pacotes, permitindo assim o armazenamento de dados de cada conexão em uma tabela de sessão. Como essa tabela consegue armazenar os estados dos fluxos dos pacotes, é possível comparar os pacotes e determinar se esses pacotes pertencem a uma conexão já existente e se pertencem a uma fonte autorizada ou não.

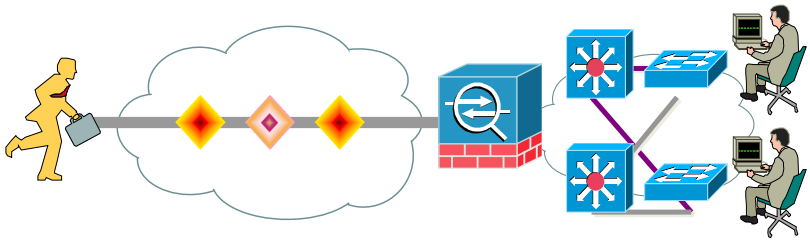

Figura – Acesso VPN permite que usuários externos acessem a rede interna

Fonte: Autoria própria

Para o monitoramento de segurança e análise de respostas, foi implantado o CS-Mars que fornece cobertura de eventos de broadcasts, correlação dos eventos e sumarização, identifica os fluxos das sessões e mapeia o caminho de ataque a topologia da rede.

Abaixo uma tela de exemplo do CS-Mars *Provides*:

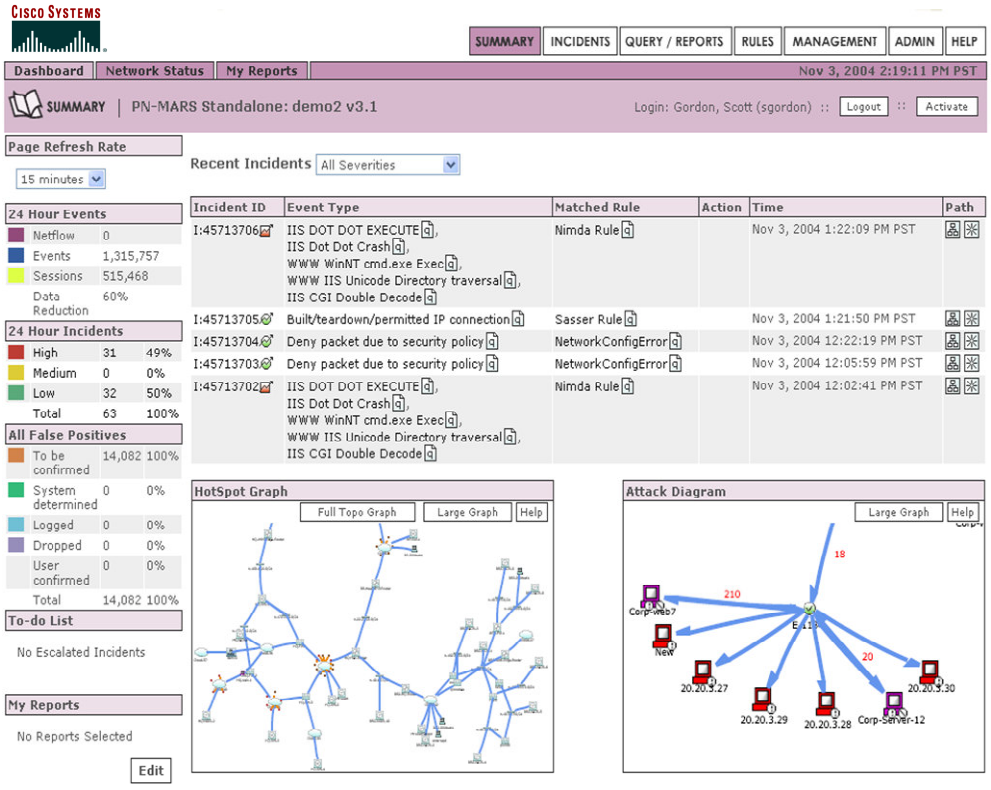

Figura exemplificando o CS-Mars Provides

Fonte: Autoria própria

Detalhes das configurações podem ser consultados no apêndice A.

4.3. EXEMPLO 3 – EMPRESA GAMA

Considerada umas das maiores empresas do ramo de produção de peças em ferro fundido, suas sedes instaladas no Sul do Brasil, a Gama sempre prezou pela alta segurança das suas informações e acessos. Diante dessa necessidade, foi realizado um projeto, para a implantação de *firewalls* na sua rede.

Na figura 15, há a topologia, onde há *firewalls* em cada localidade. São *firewalls* modelo ASA 5520 da Cisco.

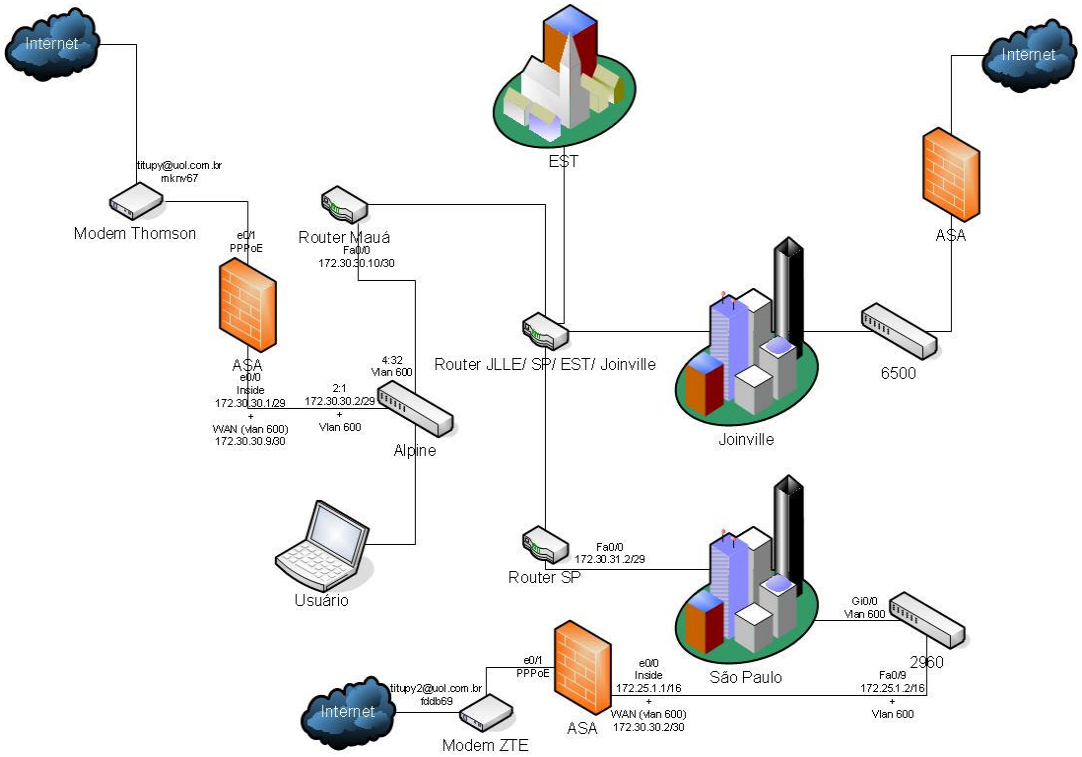

Figura 15 – Rede da empresa Gama
Fonte: Autoria própria

Os *firewalls* são os gateways dos sites remotos, operando como roteadores;

Nos sites remotos cada *firewall* possui regras de controle de acesso, permitindo ou negando o acesso entre filiais, bem como entre VLANs de uma mesma filial.

Cada ASA também está servindo de concentrador VPN para site2site e remote Access.

Isto significa que há VPN entre redes diferentes sendo fechadas nos *firewalls,* possibilitando conversação LAN com LAN via Internet (site to site). E há também

conexões remote access (via VPN Client IPsec ou AnyConnect SSL) permitindo que um usuário feche uma VPN dedicada da máquina dele para o site (*client to site*).

A VPN também funciona como um backup dos links principais da Embratel, ou seja, caso um link da Embratel falhe, o ASA detecta (através de IP SLA – *Service-Level Agreement* – monitoring) e muda sua tabela de roteamento. Com isso, a nova tabela indica que o tráfego deve seguir via VPN e uma VPN dinâmica é fechada dos sites remotos para a matriz em Joinville.

- Isto é feito via uma conexão de Internet ADSL com IP dinâmico (o site matriz não sabe qual IP cada filial terá);
- Um controle via certificados é utilizado para garantir a confiança entre os sites (e evitar que outros sites de terceiros fechem VPN de qualquer forma).

Cada ASA também possui módulo IPS inspecionando todo o tráfego (Global), com vacinas atualizadas.

Um *firewall* apenas libera ou bloqueia regras baseado em L2, L3 ou L4. Contudo, mesmo o tráfego permitido pode conter pacotes maliciosos. A função do IPS é inspecionar os pacotes permitidos, numa segunda linha de defesa.

Com este módulo IPS instalado no ASA, temos além das regras, inspeção em camada 7 dos pacotes para verificar indícios de ataques e bloquear (ou apenas logar os eventos). Os pacotes são enviados online via *backplane* interno do *firewall* para o IPS, que bloqueia ou não o pacote.

5. CONCLUSÃO

Através deste estudo pode-se demonstrar e compreender a importância e as vantagens de implementação de um *firewall,* considerado como um componente essencial dentro de um sistema de segurança de rede. No mercado podemos encontrar diversos modelos, diferenciados quanto às suas características, conjunto de regras e arquiteturas.

Entre os mais variados equipamentos comercializados, destacaram-se neste trabalho os firewalls da serie Cisco ASA 5500 devido à sua confiabilidade, sendo flexível o suficiente para atender os constantes crescimentos e alterações nas redes corporativas. Com eles, permitiu-se destacar que a complexidade de instalação de um firewall, dependerá sempre do tamanho da rede, da política de segurança, da quantidade de regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.

Desta forma, considerando-se os exemplos utilizados como referência de implantação da família Cisco ASA 5500, foi possível compreender os comandos e as regras necessárias fornecidas pelo firewall, além de observar que, um mesmo modelo pode servir para diversas topologias de rede, dependendo do ponto e como ele será instalado na rede, podendo ser configurado de uma forma genérica ou mais complexa, para se atingir os seus objetivos básicos de proteção. Dentre este, destacam-se: segurança, confidencialidade, produtividade e desempenho, abrangendo os recursos da rede e os seus usuários.

Por último, deve-se sempre avaliar a instalação correta deste componente de segurança, para não causar problemas, tais como: falhas, atrasos ou diminuição do tráfego de dados.

REFERÊNCIAS

ALECRIM, Emerson. ***Firewall*: Conceitos e Tipos**. 2004. Disponível em: <http://www.infowester.com/firewall.php>. Acesso em: 12 nov. 2012;

AWICHY, Elizabeth; CHAPMAN, D. Brent. ***Building Internet Firewalls***. O'Relly & Associates, Inc. 1995.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. ***Firewalls and Internet Security; Repelling the Wily Hacker***. Addison-Wesley, Reading, MA, 2ª ed., 2003.

CISCO SYSTEM. **Firewalls de próxima geração Cisco ASA série 5500**. Disponível em: <http://www.cisco.com/web/BR/produtos/security/asa_5500_series_next_generation_firewalls.html>. Acesso em: 05 fev. 2013.

COMPUTER COMPANY. **Segurança de perímetro – *Firewall***. Disponível em: <http://www.ccompany.com.br/firewall.htm>. Acesso em: 22 jan. 2013.

FILIPPETTI, Marco A. **CCNA 4.1: Guia Completo de Estudo**. Florianópolis: Visual Books, 2008.

FRANKLIN, Curt. **Como funcionam os roteadores**. Disponível em: <http://informatica.hsw.uol.com.br/roteadores11.htm>. Acesso em: 06 mai. 2013.

GONÇALVES, Marcus. ***Firewalls*: Guia Completo**. Rio de Janeiro: Ciência Moderna, 2000.

INTERNET SECURITY SYSTEMS. Disponível em:<http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Spoofing/default.htm>. Acesso em: 06 mai. 2013.

NAKAMURA, Emilio T.; GEUS, Paulo L. de. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

SPOHN, Marco Aurélio. **Desenvolvimento e análise de desempenho de um "Packet Session Filter**. Porto Alegre – RS: CPGCC/UFRGS. Tese de Mestrado, 1997.

TANEMBAUM, Andrew S. **Redes de Computadores**. 4ª ed. Rio de Janeiro: Elsevier, 2003.

TÉCNICAS, Associação Brasileira de Normas. **Tecnologia da Informação. Técnicas de segurança . Código de prática para a gestão da segurança da Informação** (ABNT NBR ISO/IEC 17799). 2ª Ed. Rio de Janeiro, 2005.

APÊNDICE A – Configuração de *failover* do *firewall* secundário, na empresa Beta:

```
interface GigabitEthernet0/6
no shutdown
interface GigabitEthernet0/7
no shutdown
failover lan unit primary
failover lan interface FAILOVER GigabitEthernet0/7
failover link LINK GigabitEthernet0/6
failover interface ip FAILOVER 10.22.39.253 255.255.255.252
standby 10.22.39.254
failover interface ip LINK 10.22.39.249 255.255.255.252
standby 10.22.39.250
failover
```

Abaixo, é demonstrada uma maneira de configurar uma *policy* de IPS em um sistema aleatório utilizando o ASDM.

1. Selecionar o botão configuration:

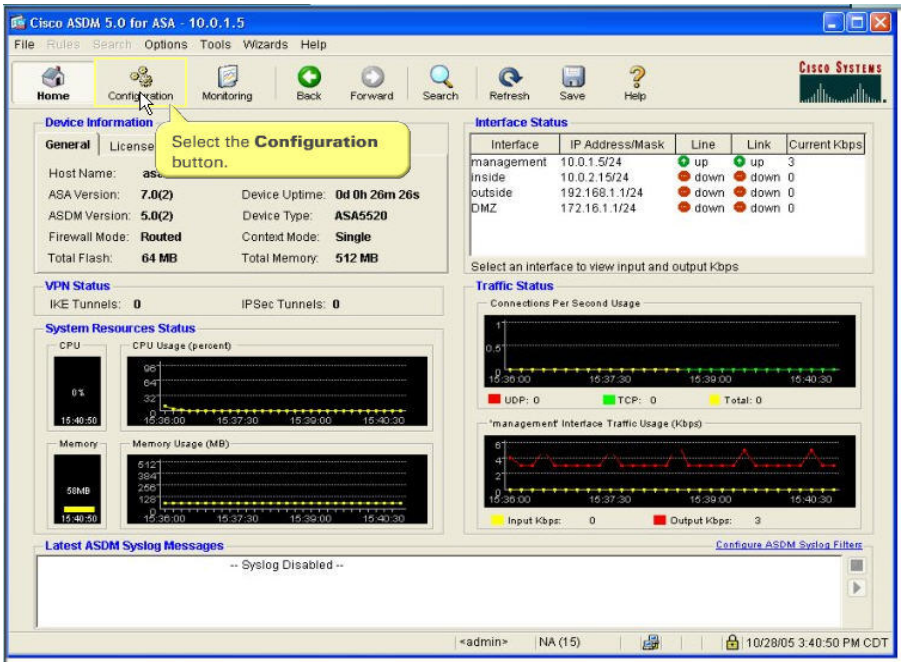

Figura 16 – Configuração uma *policy* de IPS 1
Fonte: Autoria própria

2. Selecionar a opção *Service Policy*

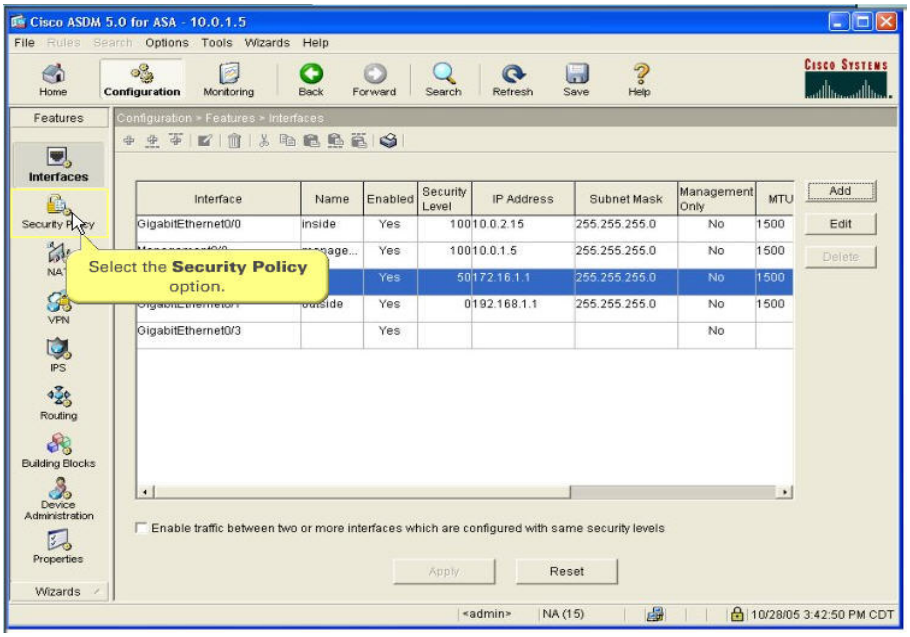

Figura 17 – Configuração uma *policy* de IPS 2
Fonte: Autoria própria

3. Selecionar o botão *Service policy rules*

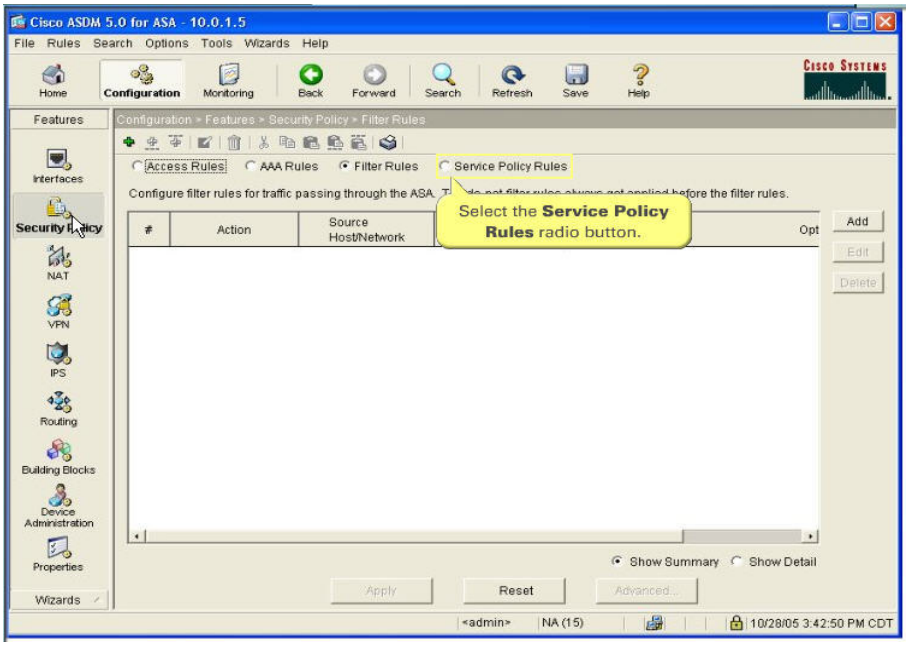

Figura 18 – Configuração uma *policy* de IPS 3
Fonte: Autoria própria

4. Selecionar o botão Add

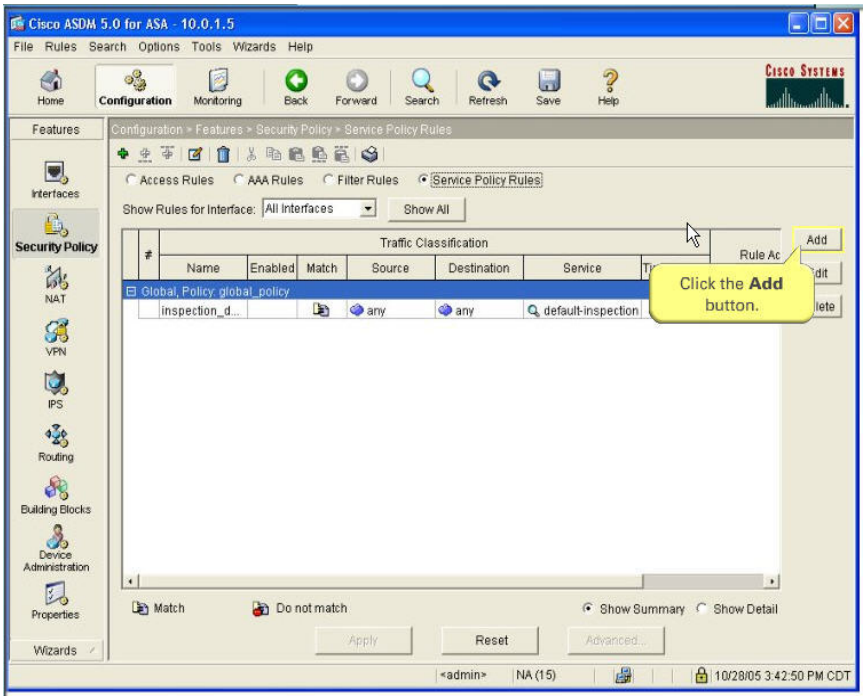

Figura 19 – Configuração uma *policy* de IPS 4
Fonte: Autoria própria

5. Selecionar a opção global (para aplicar esta *policy* em todo o tráfego) ou interface.

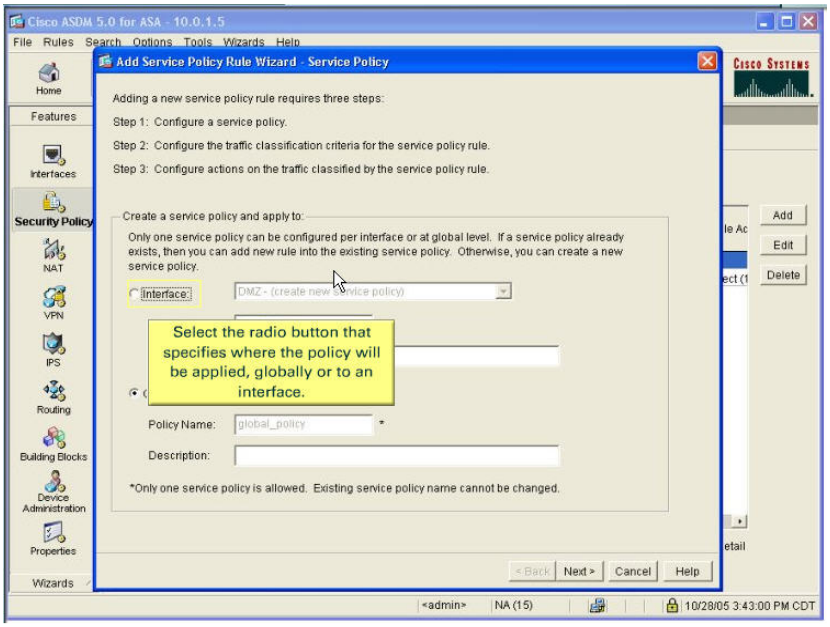

Figura 20 – Configuração uma *policy* de IPS 5
Fonte: Autoria própria

6. Neste caso foi selecionado interface.

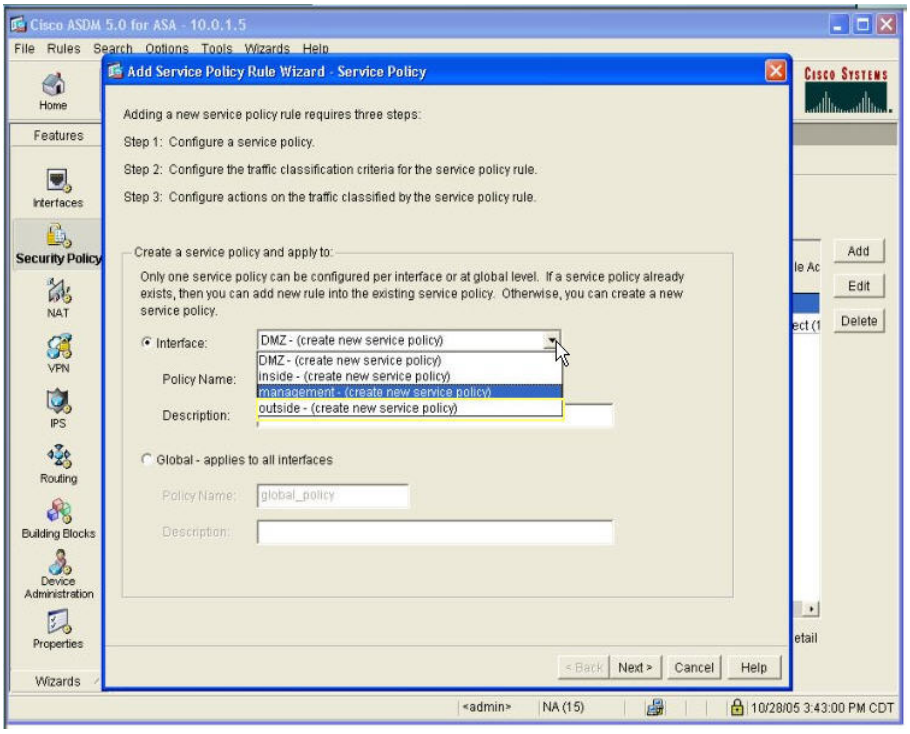

Figura 21 – Configuração uma *policy* de IPS 6
Fonte: Autoria própria

7. Definir um nome para a *policy* e clicar em Next.

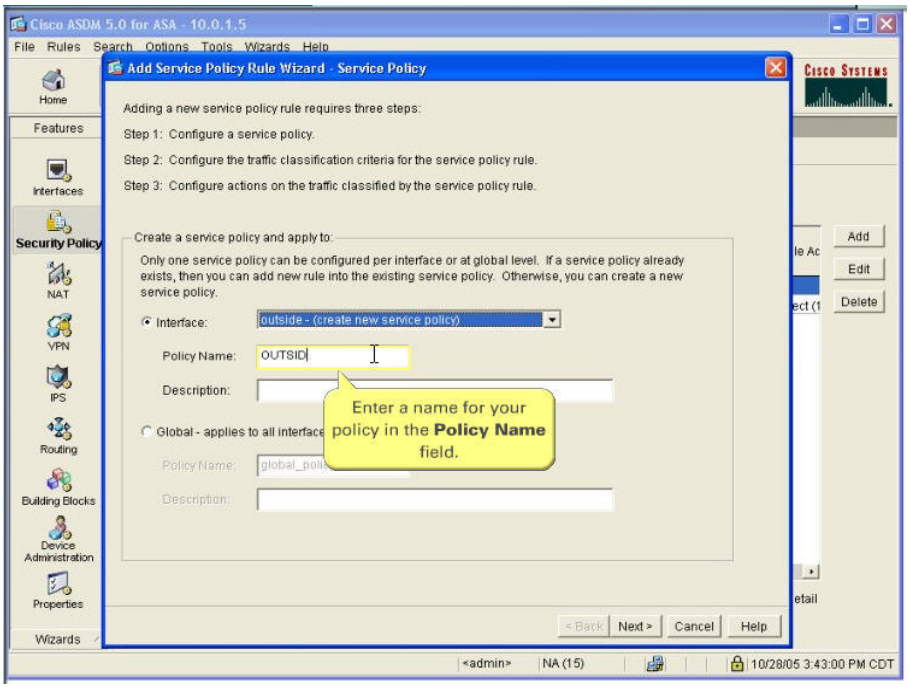

Figura 22 – Configuração uma *policy* de IPS 7
Fonte: Autoria própria

8. Selecionar o modo de classificação, neste caso por access-list. Clicar em Next.

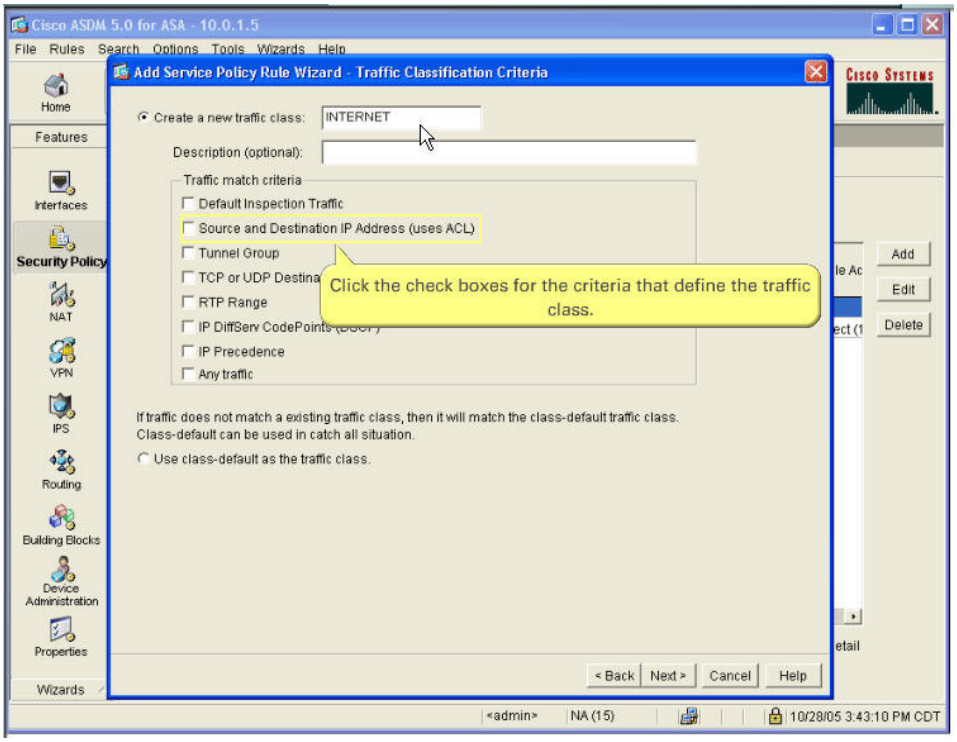

Figura 23 – Configuração uma *policy* de IPS 8
Fonte: Autoria própria

9. Definir os endereços à serem inspecionados e clicar em Next.

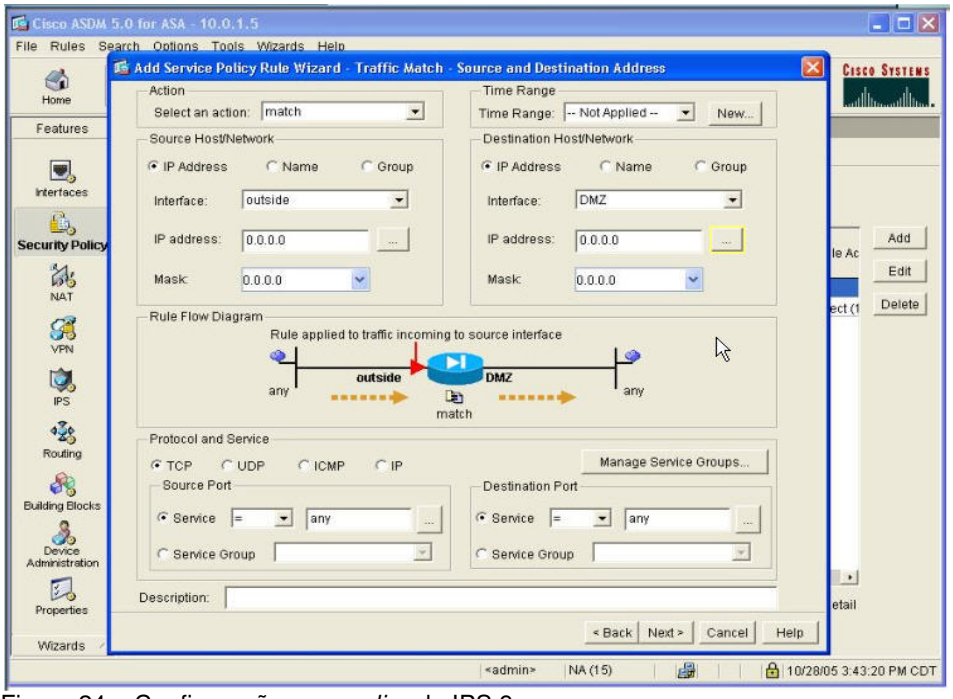

Figura 24 – Configuração uma *policy* de IPS 9
Fonte: Autoria própria

10. Selecionar *Intrusion Prevention* para criar uma *policy map*

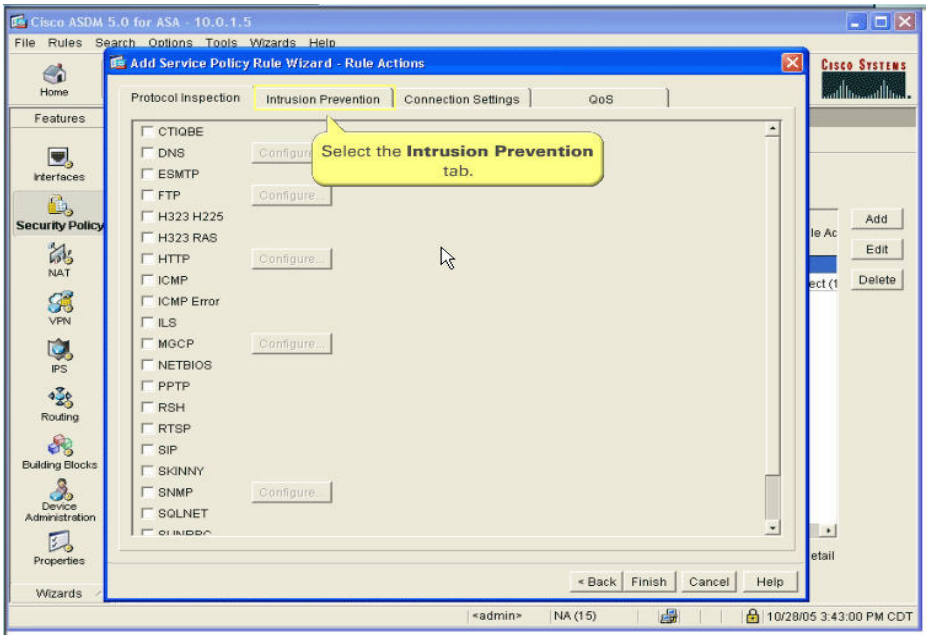

Figura 25 – Configuração uma *policy* de IPS 10
Fonte: Autoria própria

11. Habilitar a inspeção do tráfego pelo módulo de IPS, selecionando o *box Enable* IPS *for this traffic flow*

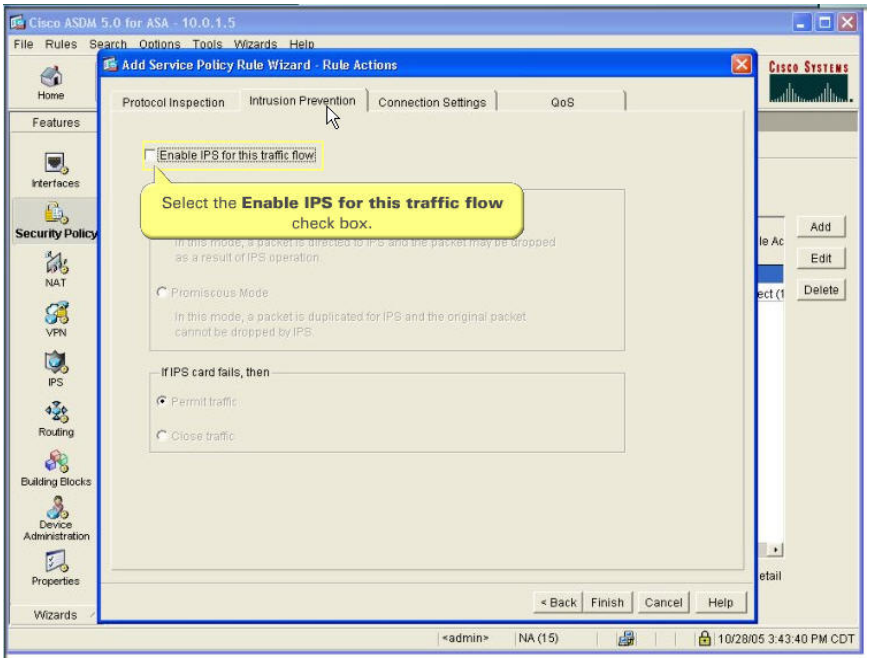

Figura 26 – Configuração uma *policy* de IPS 11
Fonte: Autoria própria

12. Selecionar o modo de operação do módulo de IPS. O modo inline é recomendado ao invés do modo promíscuo.

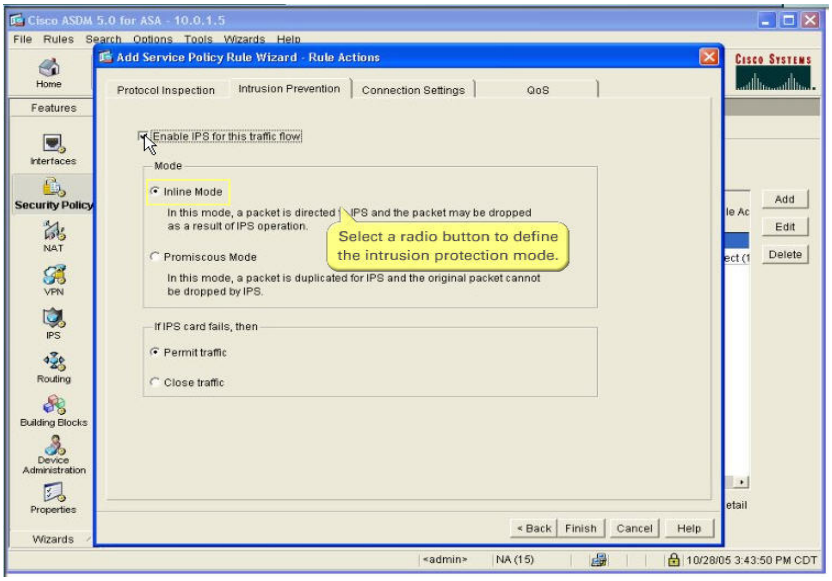

Figura 27 – Configuração uma *policy* de IPS 12
Fonte: Autoria própria

13. Configurar qual será a ação tomada, caso o módulo de IPS falhe (falha de *software* ou *hardware*). Neste caso, foi configurado para permitir que o tráfego passe sem inspeção, sendo este tráfego malicioso ou não:

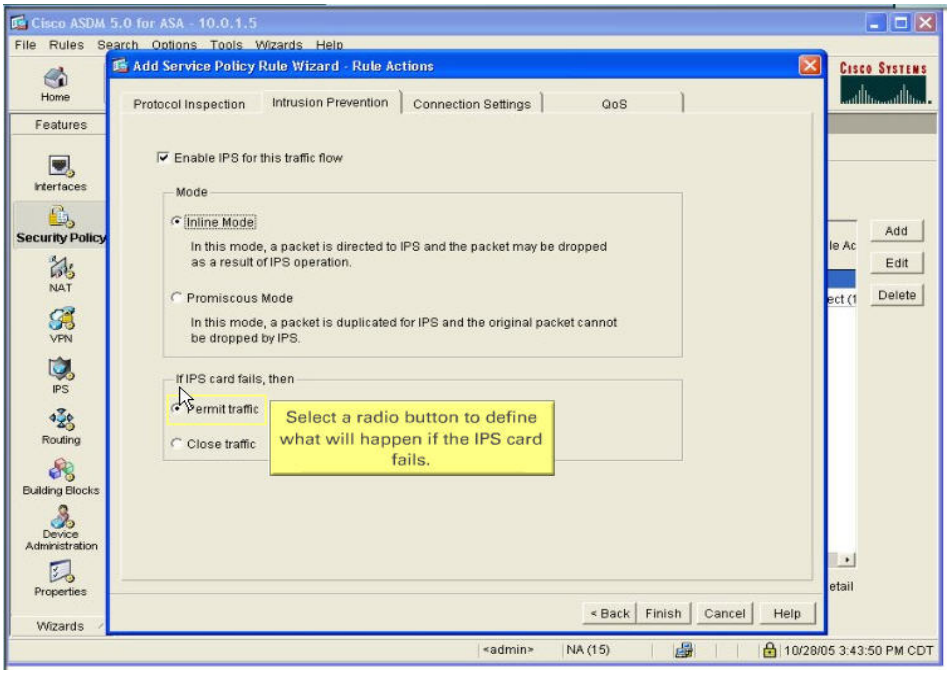

Figura 28 – Configuração uma *policy* de IPS 13
Fonte: Autoria própria

14. Finalizar a operação, clicando em "*Finish"*

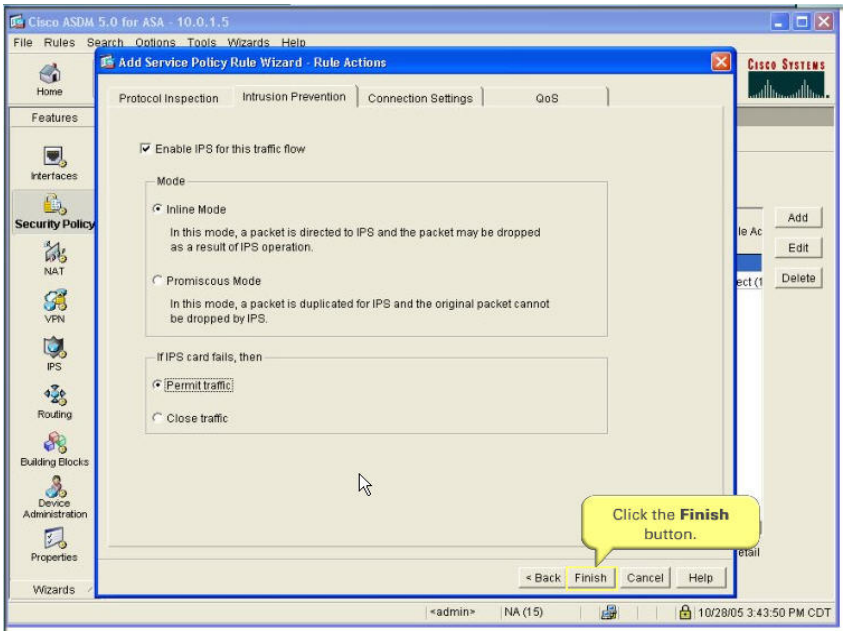

Figura 29 – Configuração uma *policy* de IPS 14
Fonte: Autoria própria

15. Observar a *policy* criada e clicar em "*Apply".*

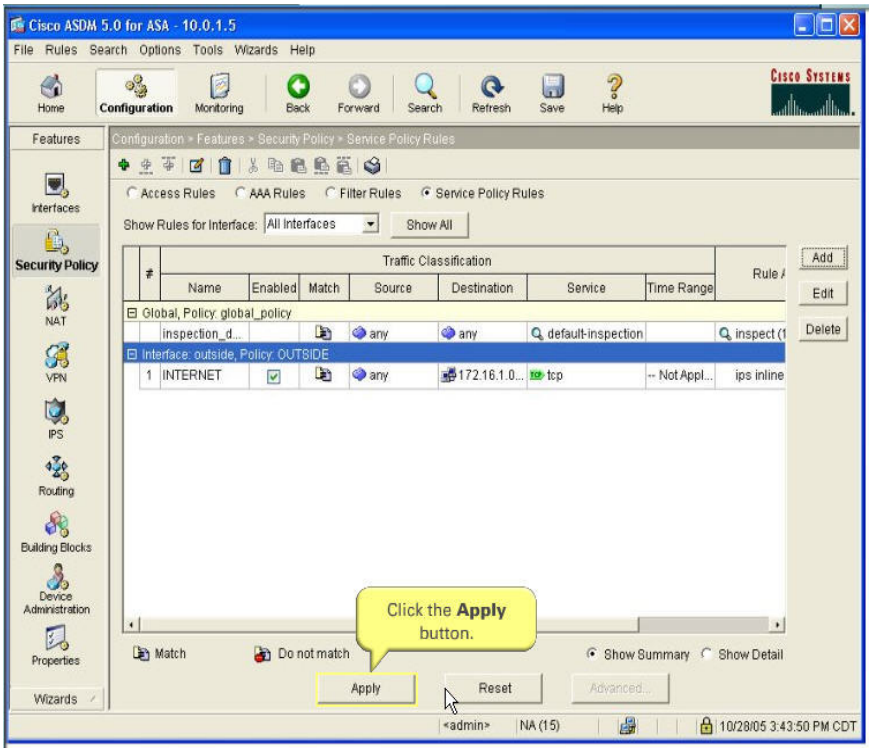

Figura 30 – Configuração uma *policy* de IPS 15
Fonte: Autoria própria

16. Prosseguir com o procedimento de “*save*”:

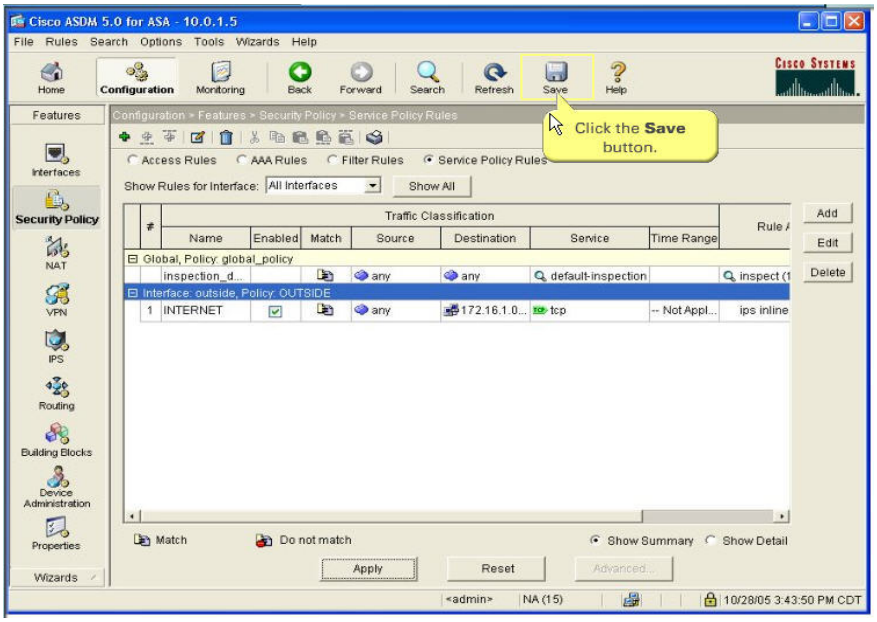

Figura 31 – Configuração uma *policy* de IPS 16
Fonte: Autoria própria

No contexto “*system”*, executar o comando show module para verificar se o módulo está corretamente inserido e reconhecido:

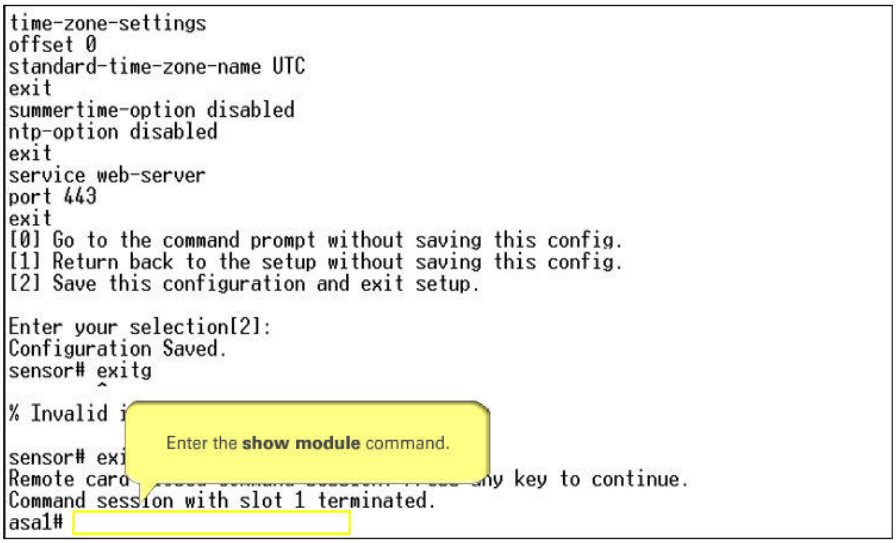

Figura 32 – Configuração uma *policy* de IPS 17
Fonte: Autoria própria

Executar o comando “*session* X” (on X é o número do *slot*) para acessar o módulo

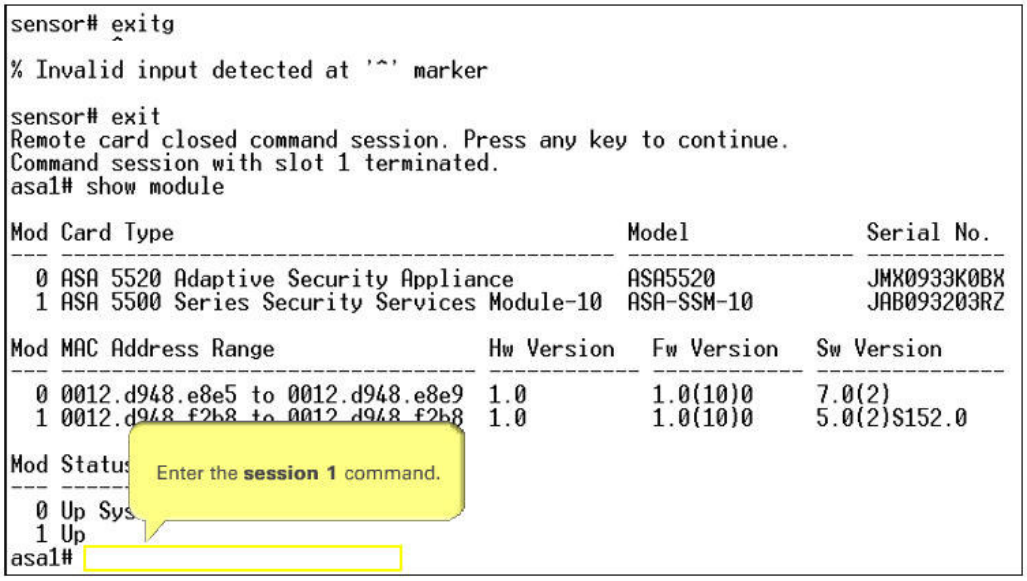

Figura 33 – Configuração uma *policy* de IPS 18
Fonte: Autoria própria

Usuário e senhas *default*: cisco

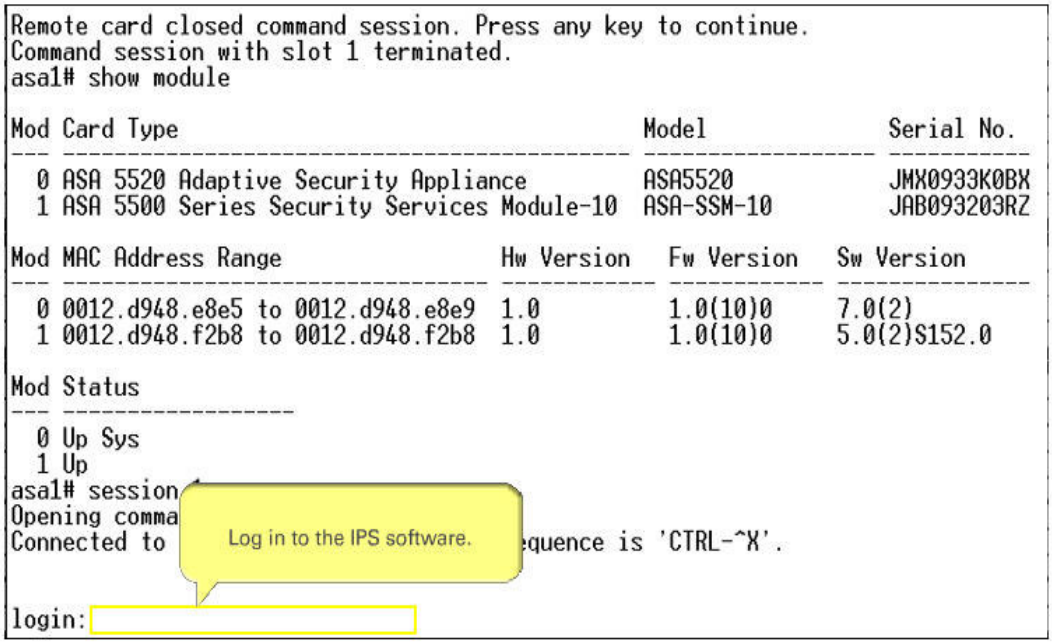

Figura 34 – Configuração uma *policy* de IPS 19
Fonte: Autoria própria

Comando “*setup*”. Trata-se de um wizard para efetuar as primeiras configurações do módulo:

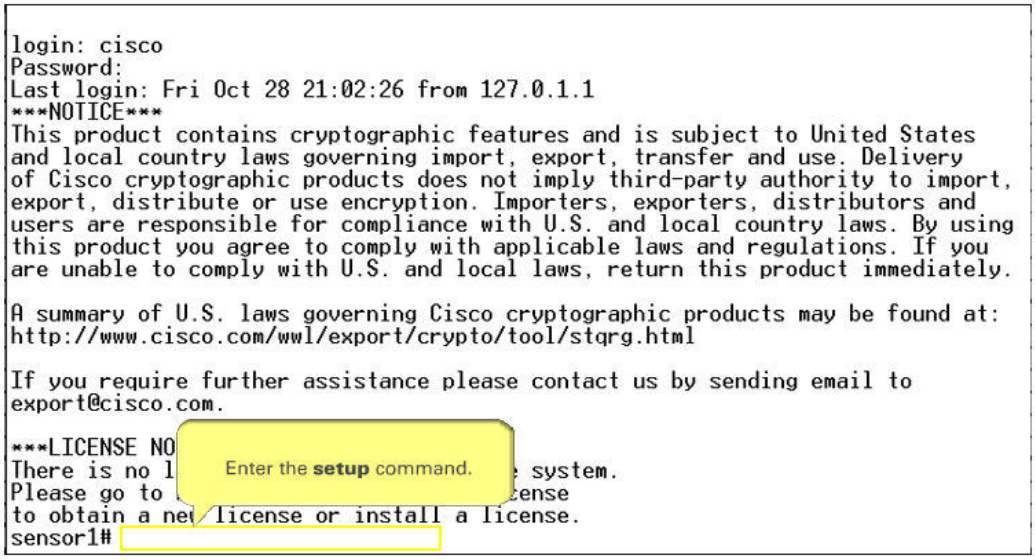

Figura 35 – Configuração uma *policy* de IPS 20
Fonte: Autoria própria

Seguindo o padrão Cisco, basta pressionar “ENTER” para seguir a resposta padrão, que se encontra entre colchetes. Caso não deseje utilizar a reposta padrão, basta digitar:

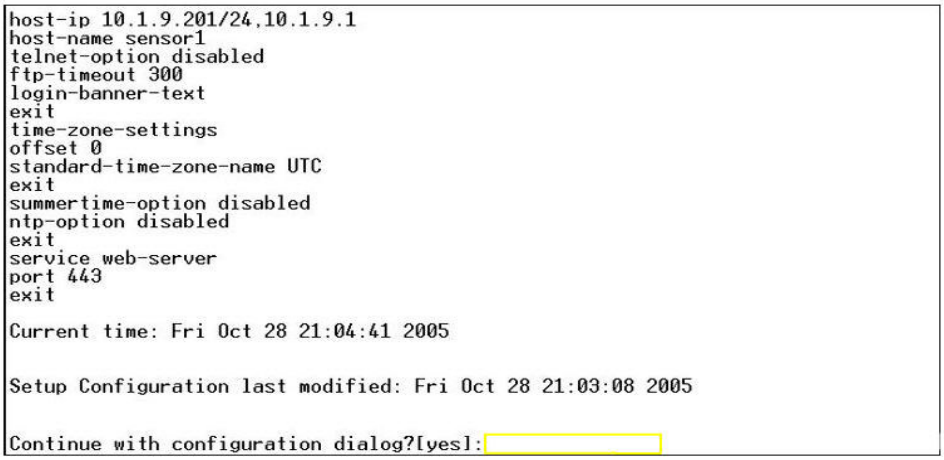

Figura 36 – Configuração uma *policy* de IPS 21
Fonte: Autoria própria

Preencher com o *hostname*:

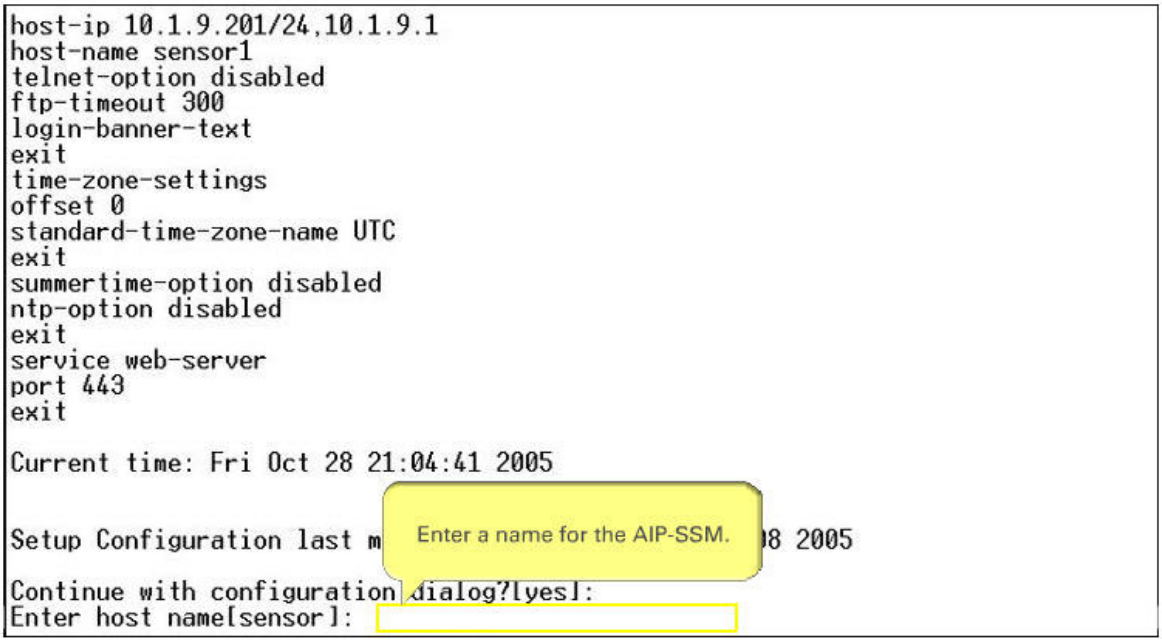

Figura 37 – Configuração uma *policy* de IPS 22
Fonte: Autoria própria

Configurações de IP (interface de gerência) e *gateway*. O formato deve ser "IP/MÁSCARA,*GATEWAY*":

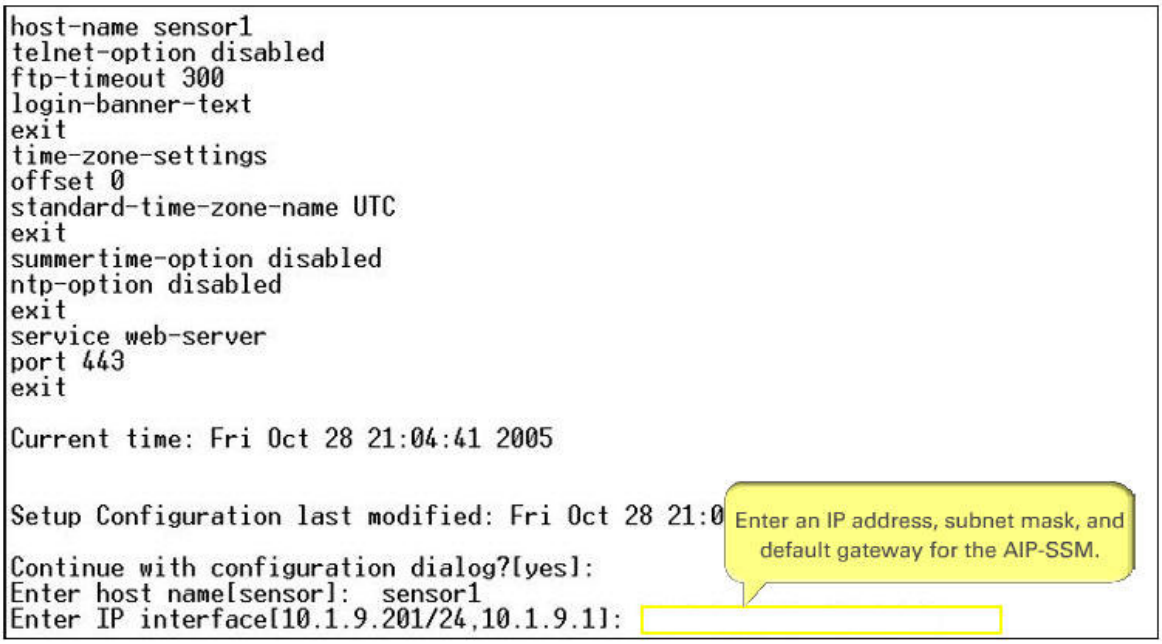

Figura 38 – Configuração uma *policy* de IPS 23
Fonte: Autoria própria

Habilitar o *telnet* ou não.

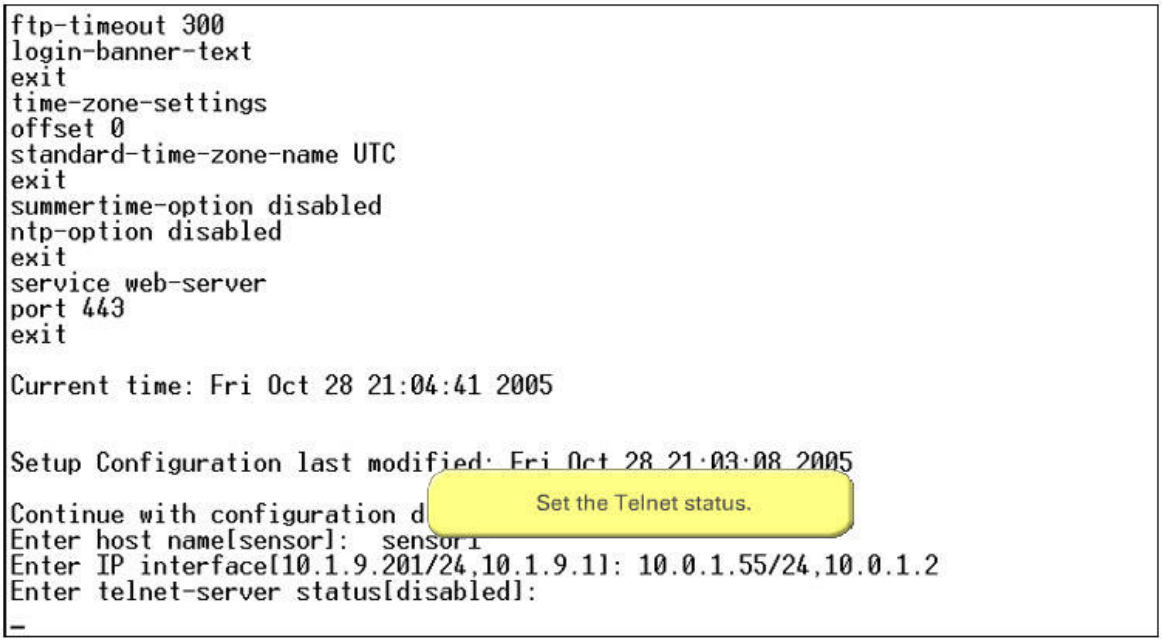

Figura 39 – Configuração uma *policy* de IPS 24
Fonte: Autoria própria

Habilitar o *webserver* ou não e setar as *access-lists* (quem poderá acessar o *webserver/telnet)*:

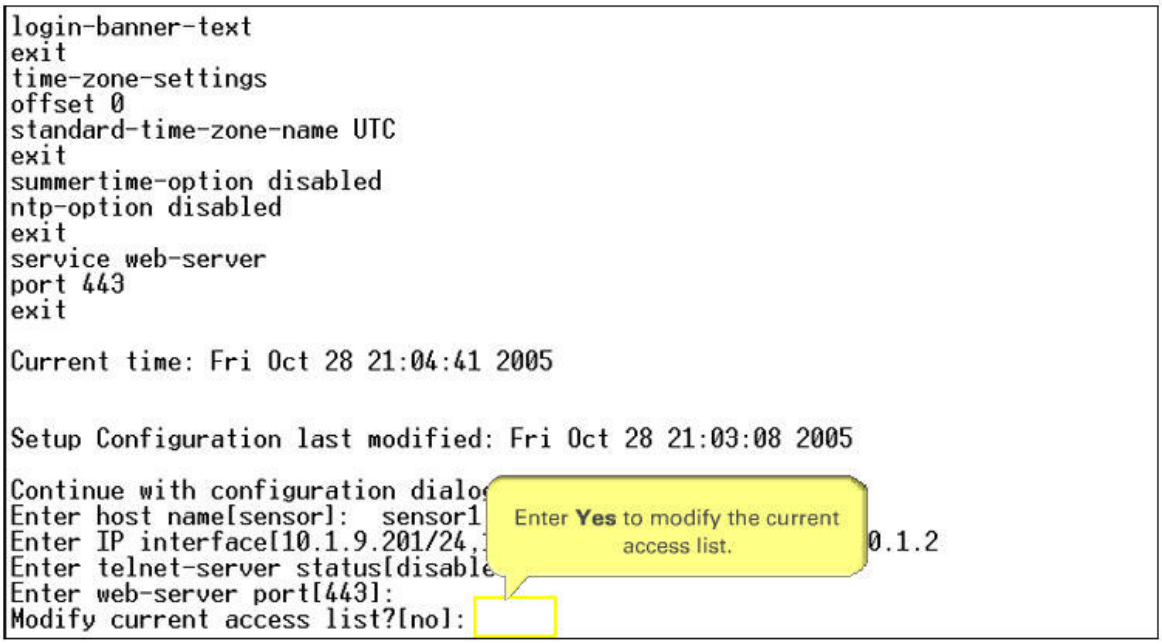

Figura 40 – Configuração uma *policy* de IPS 25
Fonte: Autoria própria

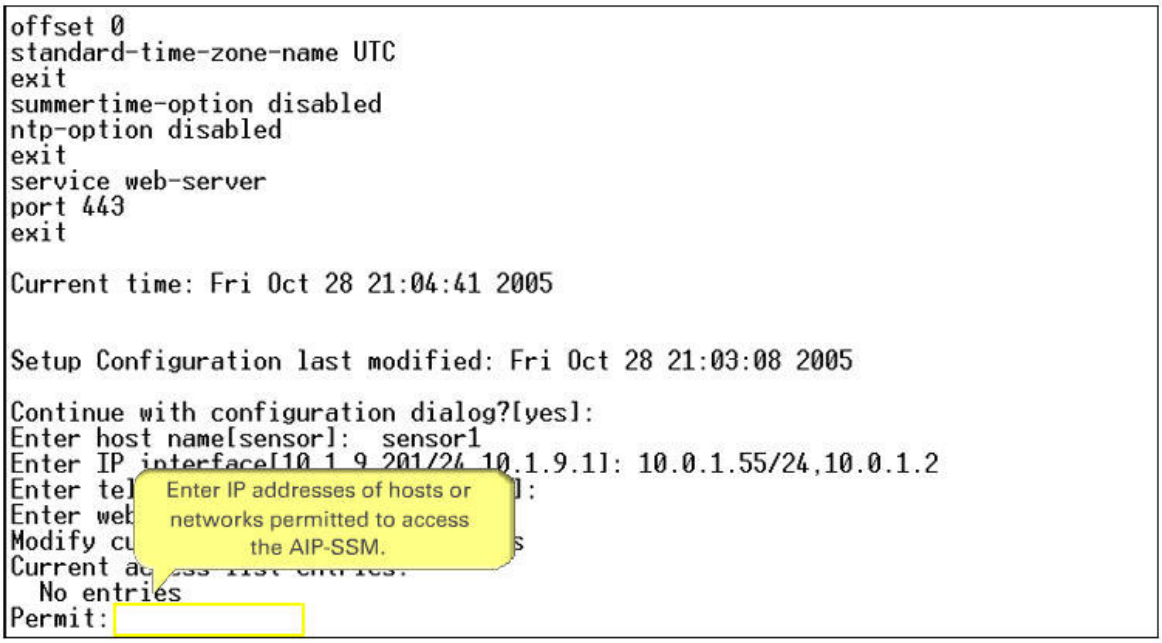

Figura 41 – Configuração uma *policy* de IPS 26
Fonte: Autoria própria

Caso não seja necessário alterar as configurações de horário, pode-se pular esta etapa. As configurações de vs0 ficarão para depois:

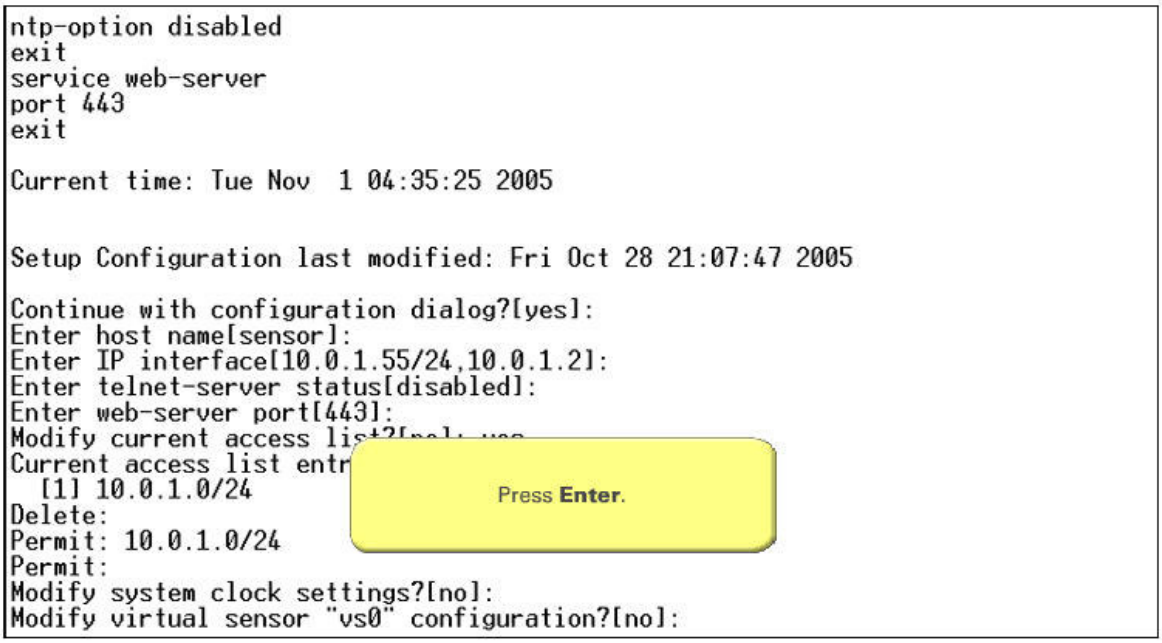

Figura 42 – Configuração uma *policy* de IPS 27
Fonte: Autoria própria

Após a exibição das configurações, digitar 2 para salvar e sair do setup. Em seguida, digitar reset e "*Yes*" para que (apenas) o módulo seja reiniciado, efetuando as configurações:

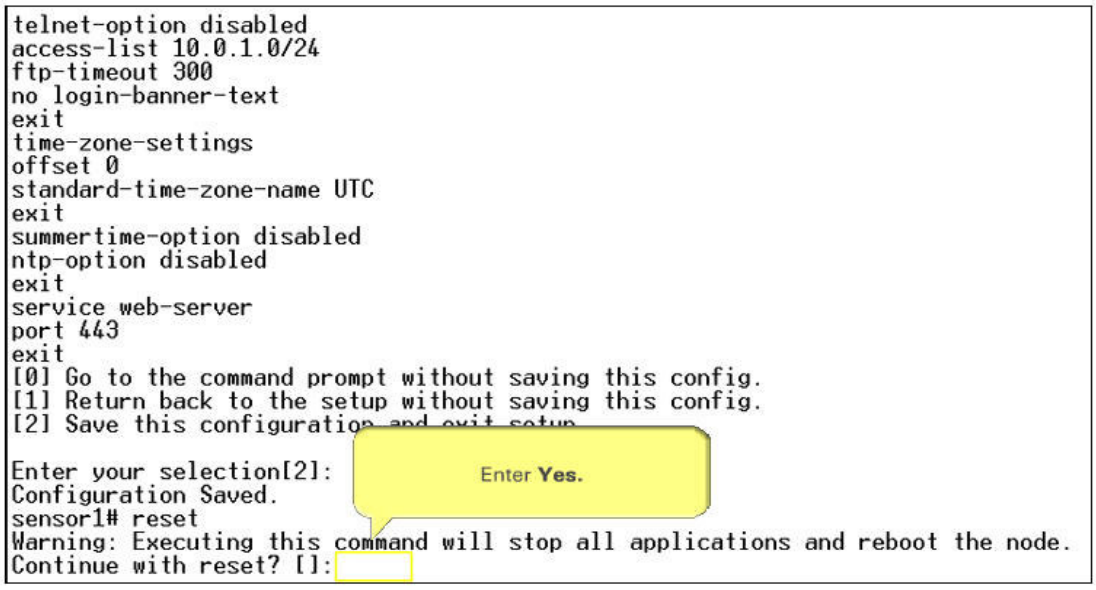

Figura 43 – Configuração uma *policy* de IPS 28
Fonte: Autoria própria