Equipamentos de Rede

Sabemos que uma rede, como todo sistema computacional é composta de *software* e *hardware*. O *software* diz respeito ao sistema operacional de rede e os protocolos que ele suporta, como o IP, TCP, UDP e etc. O *Hardware* diz respeito aos vários equipamentos, dispositivos e materiais que interligam a rede, entre eles:

- Servidor de Rede;
- Estações de trabalho;
- Servidores de Impressão;
- Pontos de Acesso;
- Impressoras de Rede;
- Sistemas de Armazenamento;
- Placas de rede;
- Infraestrutura de cabeamento;
- **Hubs;**
- **Switches;**
- **Roteadores**;
- **Firewall**;
- Modem.

Nessa unidade vamos estudar os hubs, os switches, os roteadores e o Firewall.

1. Hub

Os hubs possuem a simples função de transmitir os sinais recebidos em uma porta para as demais portas do equipamento, agindo na maioria dos casos na camada física ou no máximo na camada de enlace de dados dos modelos de referência e estão sujeitos a um alto índice de colisão.

Nos Hubs 10/100 com detecção automática, cada porta detecta e ajusta-se automaticamente a sua velocidade de porta, (*auto-sense).* Esses

equipamentos eram a maneira mais rápida e mais econômica de se montar uma rede de 10/100 Mbps alguns anos atrás.

O hub era ideal para interligar equipamentos em ambientes de escritório. Quando havia a necessidade de se utilizar mais portas, bastava conectar outro hub pela porta de *uplink*, para expandir a rede. Outra forma era usar cabos de rede *cross-over* entre duas portas de dois hubs distintos, simulando a existência de um *uplink*.

Com o barateamento dos switches e o aumento da velocidade das redes, os hubs caíram em desuso, não sendo mais recomendados para conectar estações de trabalho.

2. Switchs de Rede.

Um switch de rede é um dispositivo de alta velocidade que permite a comunicação entre estações de trabalho e servidores. Diferente do hub, que simplesmente copia o sinal que chega a uma porta para todas as outras portas, o switch de rede possui um núcleo, o *switch fabric,* que encaminha os sinais das interfaces de entrada para as interfaces de saída, criando assim circuitos independentes entre duas estações que estão se comunicando em um dado momento.

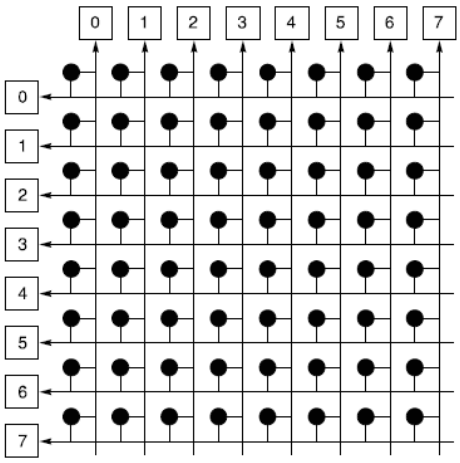

Figura 1 - Switch Fabric do tipo Cross bar.
Fonte: Patterson.

O switch também difere do hub em relação às colisões. O hub possui um único domínio de colisão representado por todas as portas, já no switch, cada porta corresponde a um domínio de colisão, assim, um switch de 24 portas

possuirá 24 domínios de colisão, o que melhora em muito o desempenho da rede. Como foi estudado na disciplina de redes, quando ocorre uma colisão, os equipamentos no mesmo domínio de colisão, entram no modo exponencial *backoff*, o que acaba diminuindo o desempenho.

Os switches de rede, geralmente trabalham na camada física e de enlace, entretanto existem switches que também trabalham na camada de rede e até na camada de transporte. Switches que trabalham na camada de enlace verificam os endereços MAC para fazer alguma função específica, como criar uma VLAN, impedir a conexão de equipamentos não autorizados, etc. Os switches que operam na camada de rede possuem protocolos de roteamento implementados em circuitos integrados especiais chamados de ASICs. Esses protocolos podem ser utilizados para ligar Vlans, por exemplo. Os switches que operam na camada de transporte fazem o roteamento levando em consideração a aplicação. Eles podem encaminhar o trafego baseado no endereço MAC, endereço IP ou nos fluxos UDP ou TCP. Esses tipos de switches também fazem a priorização do trafego, baseado na aplicação.

Vejamos algumas características de um Switch da 3COM, layer 2, figura 2 .

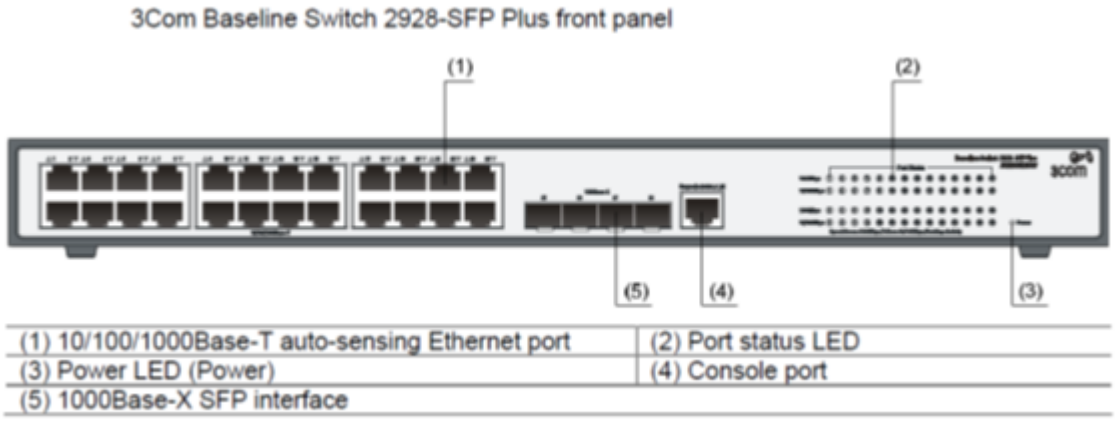

Figura 2 - Switch 3COM 2928

- Possui 24 portas 10BASE-T/100BASE-T/1000BASE-T + 4 Gigabit SFP
- Possui capacidade maxima de 56 Gbps.
- Permite a criação de VLANs.
- Possui Agregação de Link.
- Permite a priorização de voz e de trafego VOIP

- Possui o Spanning Tree Protocol.
- Permite a criação de até 32 rotas estáticas.

Quando vamos adquirir um switch de rede, precisamos ficar atentos não apenas à quantidade de portas, mas também à capacidade máxima de taxa de transmissão que ele suporta. O switch acima, possui capacidade máxima de 56 Gbps, isso significa que podemos ter um trafego *full-duplex* de 1 Gbps nas 28 portas do equipamento.

Um Switch com essa característica é chamado de nonBlocking. Isso quer dizer que a soma das velocidades das portas do switch é igual ou menor do que o backplane. Fazendo uma analogia com uma via expressa, a soma das vias de acesso é igual ou menor do que a quantidade de pistas.

Quantas pistas são necessárias para uma estrada com 24 vias de acesso de 2 faixas cada?

24 vias de acesso X 2 faixas = 48 pistas
Qual seria o backplane mínimo para um switch com 24 portas 10/100Mbps Full-duplex ser non-blocking?
24 portas 100Mbps X 2 (full-duplex) = 4,8Gbps

Throughput

O Nº máximo de pps (packet per second) que um Switch pode enviar através de todas suas portas sem perda. Usualmente baseado na distribuição perfeita do tráfego através de todas suas portas

Porta 10 Mbps – 14.880 pps

Porta 100 Mbps – 148.810 pps

Porta 1000 Mbps – 1.488.000 pps

Exemplo: Um Switch com 24 portas 10/100 Mbps e 2 portas 1000 Mbps terá seu throughput máximo calculado desta forma: (24 x 148.810) + (2 x 1.488.000) = 6.547.440 pps

Um switch de rede pode ser gerenciado ou não-gerenciado. Um switch gerenciado possui um *software* embutido que permite ao administrador de rede fazer vários tipos de controles e verificar as estatísticas do equipamento. Geralmente esses switches implementam o protocolo de gerenciamento de rede da Internet, o SNMP, simple network management protocol, que estudaremos posteriormente.

Vejamos abaixo algumas funcionalidades relacionadas aos switches.

VLAN (Virtual LAN): é uma rede virtual que segmenta o domínio de broadcast em uma LAN, ou seja, um switch de 24 portas pode se transformar em 3 switchs de 8 portas. Um exemplo de seu uso seria a segmentação entre alunos e professores de uma universidade.

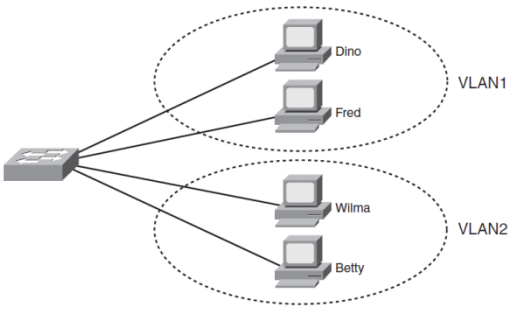

Figura 3 - VLAN

Trunk: Permite o tráfego de mais de uma VLAN em uma única interface de rede. Geralmente utilizada na conexão entre switches.

Exemplo de Segmentação de VLANs:

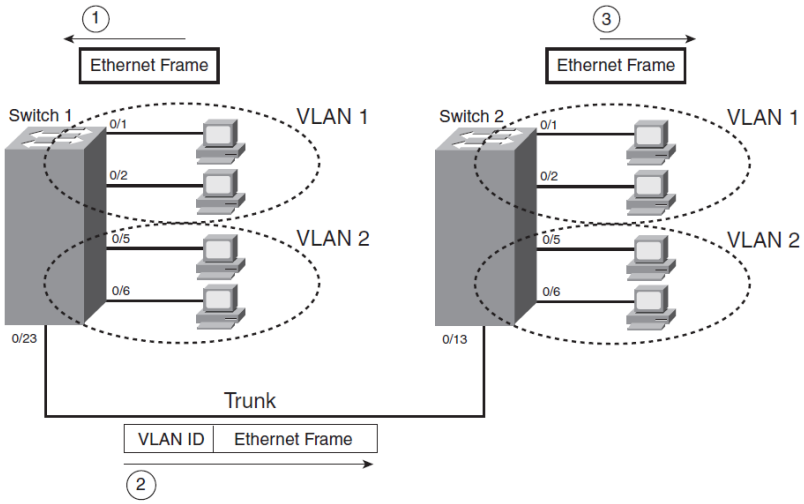

Figura 4 – Vlan com Trunk

Benefícios da Segmentação utilizando VLANS

- **Segurança**: Grupos com dados confidenciais são separados do restante da rede.
- **Redução de custo**: resultante da menor necessidade das atualizações de rede e do uso mais eficiente da largura de banda e dos uplinks existentes.
- **Desempenho:** Segregar domínios de broadcast reduz o tráfego desnecessário na rede e aumenta o desempenho.
- **Eficiência do pessoal de TI:** VLANs simplificam o gerenciamento da rede.

Métodos:

- **Estática:** Configurada manualmente na interface do Switch
- **Dinâmica:** Associação ocorre através de politicas de acesso na implementação do 802.1x
- **Vlan de Voz:** Padrão a ser utilizado pela telefonia IP.

IEEE 802.1Q

As conexões em modo trunk são utilizadas para permitir que um switch que possui várias VLANs, possa trafegar no restante da rede utilizando um único link de entrada e saída (up-link). O padrão que permite a implementação do Trunk é o IEEE 802.Q. Os switches utilizam o cabeçalho da Ethernet para

tomar as decisões de encaminhamento. Os cabeçalhos da Ethernet não possuem informações de VLAN. Quando os quadros atravessam um link trunk, um novo cabeçalho é inserido e depois retirado.

STP (Spanning Tree Protocol)

Os switches utilizados em redes locais são considerados críticos. Falhas nesses equipamentos podem acarretar indisponibilidade parcial ou total da rede, assim, adicionar redundância é fundamental. O STP permite que os switches possam ser interligados em anel gerando a redundância necessária. O *Spanning Tree Protocol* (STP) resolve os principais problemas quando links redundantes são adicionados em uma rede.

O STP constrói uma topologia em árvore, elegendo um switch como Raiz (Root), de acordo com a prioridade (**mais baixa**) dos switches em toda a rede. Após a eleição do switch Raiz as interfaces dos switches serão designadas com funções especificas, permitindo ou bloqueando o tráfego, evitando que o loop aconteça. Caso ocorra um empate na prioridade, o switch com o menor valor de MAC será eleito como raiz.

Se ligarmos switches sem STP configurado em anel ocorrem os seguintes problemas:

- Loop de rede: Quadros saltarão de um switch para outro eternamente, pois os quadros não possuem TTL (Time to Live) como no pacote IP.
- Tempestade de Broadcast: Broadcast são encaminhados para todas as portas dos Switches, gerando um loop infinito (tempestade) de Broadcasts.

Com isso, ocorre a Interrupção total da rede, devido ao excesso de tráfego causado pelos loops e tempestade de Broadcast.

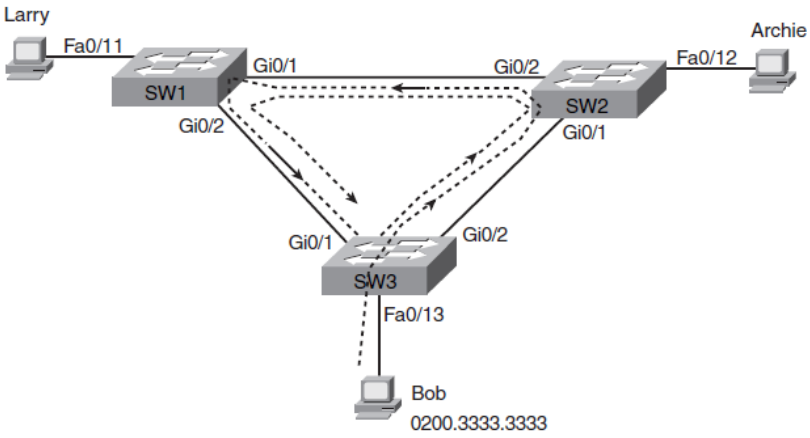

Figura 5 - Loop e tempestade de Broadcast

O Spanning Tree Protocol (STP), prevê redundância de ligação à rede permitindo que uma rede de comutação de camada 2 possa se recuperar de falhas, sem intervenção e em tempo hábil. Ele opera realizando a comunicação entre todos os switches da rede. As mensagens são trocadas a cada 2 segundos e são conhecidas como BPDU (*Bridge Protocol Data Units*).

Projeto lógico-hierárquico de Redes.

Os projetos de redes atuais estão levando em consideração que os serviços devem ficar localizados no núcleo da rede. Além disso, essas novas redes permitem um crescimento controlado e um melhor gerenciamento. Elas são implementadas em um modelo hierárquico de três camadas. A camada de acesso, camada de concentração e camada de núcleo.

Camada de Acesso: Faz a interface com dispositivos finais, como PCs, impressoras e telefones IP. Fornece um meio de conectar dispositivos à rede e controlar permissões. Os switches presentes nessa camada geralmente executam funções da camada de enlace. São switches mais simples, sem funções de outras camadas.

Camada de Agregação ou Distribuição: Agrega os dados recebidos dos switches de acesso antes de serem transmitidos para a camada Central. Controla o fluxo do tráfego da rede usando políticas e realiza funções de roteamento entre VLANs. Os switches presentes nessa camada devem possuir funções de roteamento, alto desempenho e disponibilidade.

Camada Central ou de Núcleo: É o backbone de alto desempenho da rede. Conecta através de roteamento extranets, WAN e Internet utilizando um protocolo de roteamento interior como o OSPF ou EIGRP. Os switches presentes nessa camada também devem possuir funções de roteamento, alto desempenho e disponibilidade.

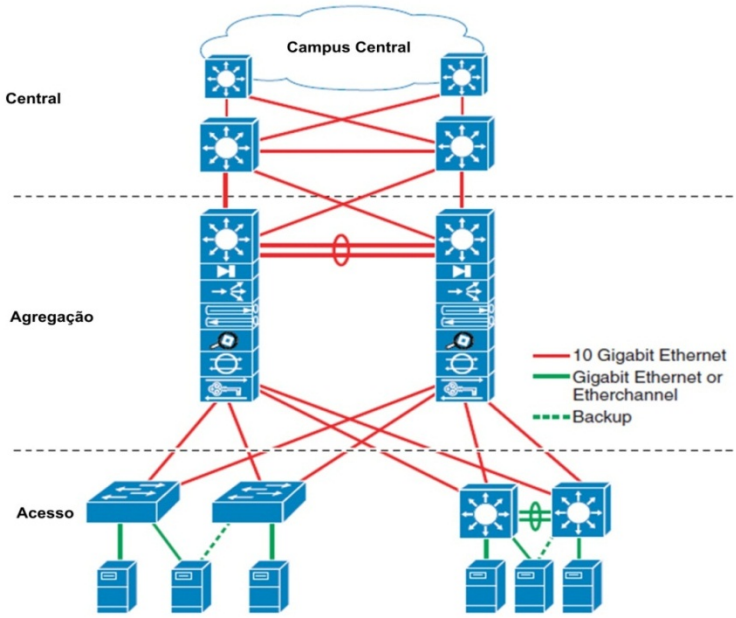

Figura 6 – Projeto de Redes em Camadas.
Fonte: Cisco Systems.

3. Roteador.

Um roteador é um equipamento que permite o roteamento entre diferentes localidades ou VLANs diferentes. Ele funciona na camada de Rede e em alguns casos até camada de aplicação. O roteador é largamente utilizado em redes de Longa Distância e na Internet. Ele faz a interligação da rede local (LAN) com a rede da operadora (WAN).

Esse equipamento funciona, para uma rede de comutação de pacotes, analisando os endereços IPs dos pacotes que chegam até ele. Após uma consulta a uma tabela de roteamento o pacote é encaminhado para uma linha de saída. Esse roteamento pode ser estático, quando as rotas são definidas manualmente, ou dinâmicos quando protocolos de roteamento modificam as tabelas de roteamento em determinados intervalos de tempo.

Na figura 7, temos o roteador da Cisco 1841 utilizado para ligar pequenas e médias empresas.

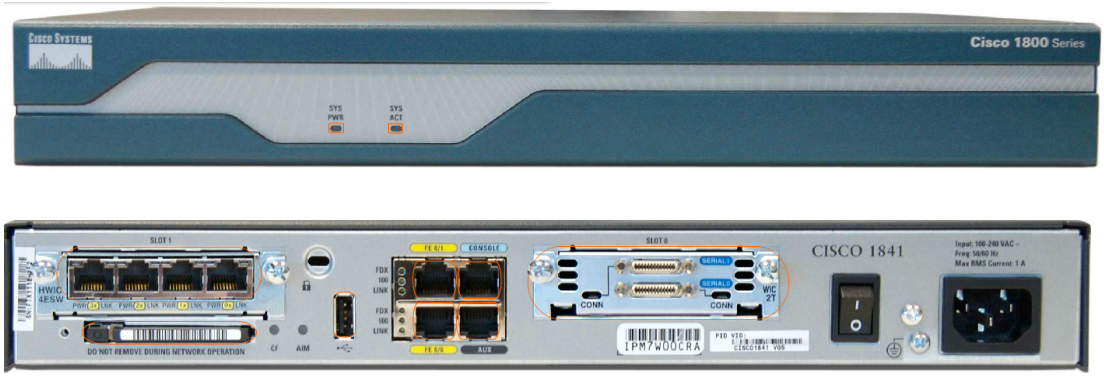

Figura 7 – Roteador Cisco 1841.
Fonte: Cisco Systems.

Quando vamos adquirir um roteador, precisamos verificar se ele já vem com as seriais. A serial é a interface que fará a ligação com o modem da operadora e pode ser visualizado na figura 7, slot 0. Nessa figura temos um slot em que foi adicionada uma placa com duas seriais. Quando vamos adquirir a interface serial, é necessário verificar que venha também com o cabo compatível para ligar a serial ao modem.

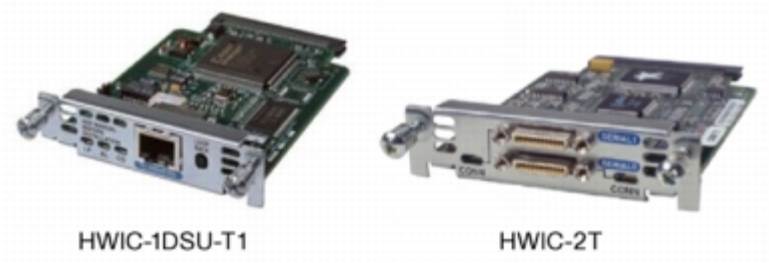

Figura 8 – Seriais para roteador 1841.
Fonte: Cisco Systems.

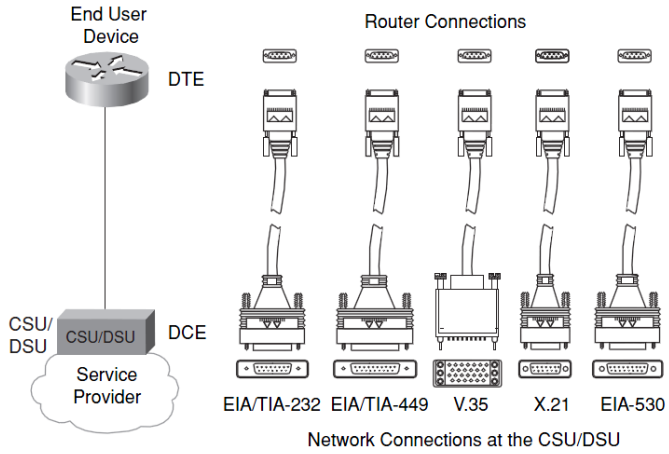

Figura 9 – Conectores dos cabos das seriais de roteadores.

Figura 10 – Roteadores de grandes provedores de internet e de médias empresas.
Fonte: Cisco Systems.

4. Firewall

Um firewall é um conjunto de componentes que envolve *hardware* e *software* que protegem tanto a rede local contra ataques provenientes de redes externas interligadas, quanto as rede externas de ataques provenientes da rede local. Na figura abaixo tem-se uma arquitetura comum relacionada a implementação de um firewall. Entre o roteador e o Firewall tem-se uma zona desmilitarizada em que são conectados os servidores que precisam responder à solicitações vindas da rede externa. Essa implementação fornece uma segurança adicional. Caso os servidores sejam invadidos, o Firewall protegerá a rede interna.

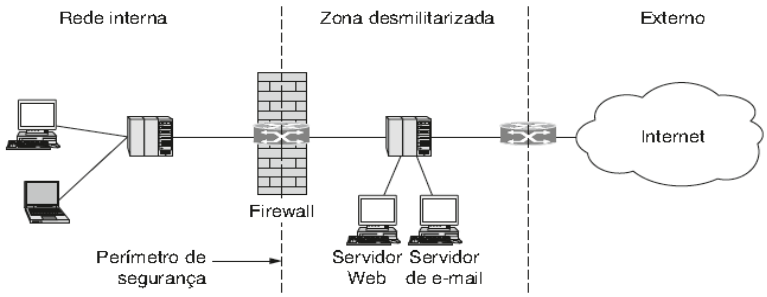

Figura 10 – Disposição de um firewall na rede

Objetivos de um Firewall:

Impedir ataques de negação de serviço:
Inundação de SYN: atacante estabelece muitas conexões TCP falsas, sem recursos deixados para conexões “reais”.

Impedir modificação/acesso ilegal de dados internos.
Ex., atacante substitui página inicial da companhia por algo diferente.

Permite apenas acesso autorizado à rede interna (conjunto de usuários/hospedeiros autenticados)

Podemos ter dois tipos de firewalls: os que fazem filtros de pacotes e os que são gateways de aplicação.

Funcionalidades dos Firewalls de Filtros de pacotes.

- Controle de Serviço: Determina os tipos de serviços da Internet que podem ser acessados: *Inbound* ou *Outbound*.
- Controle de Direção: Determina a direção na qual as requisições de serviços podem fluir: *Incoming* ou *Outgoing*.
- Controle de Usuário: Controla o acesso aos serviços de acordo com os usuários que tentam acessa-los.
- Controle de Comportamento: Controla a forma como serviços são utilizados (p. ex., filtrar e-mail)

Os firewalls de filtros de pacotes baseiam o seu funcionamento em regras de entrada e saída. Essas regras recebem o nome de ACLs (listas de controle de acesso) e podem bloquear ou liberar o trafego para endereços IP específico e/ou porta específica.

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Flag bit
Permitir	222.22/16	Fora de 222.22/16	TCP	>1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	>1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	>1023	53	_
Permitir	Fora de 222.22/16	222.22/16	UDP	53	>1023	_
Negar	Todos	Todos	Todos	Todos	Todos	Todos

Figura 11 – Exemplo de uma tabela de ACL

Fonte: Kurose, 2010.

Funcionalidades dos Firewalls Gateway de aplicações (Proxy)

- Examina o trafego de aplicações.
- Pode auditar e registrar todo tráfego de entrada.
- Faz controle de acesso por usuário.
- Faz distribuição de trafego por endereços.

Na figura 12, temos uma solução da Cisco que combina firewall, VPN, segurança de conteúdo e faz prevenção de invasões. Ele Interrompe os ataques antes que afetem a continuidade dos negócios. Soluções integradas reduzem custos e fornecem segurança para as redes.

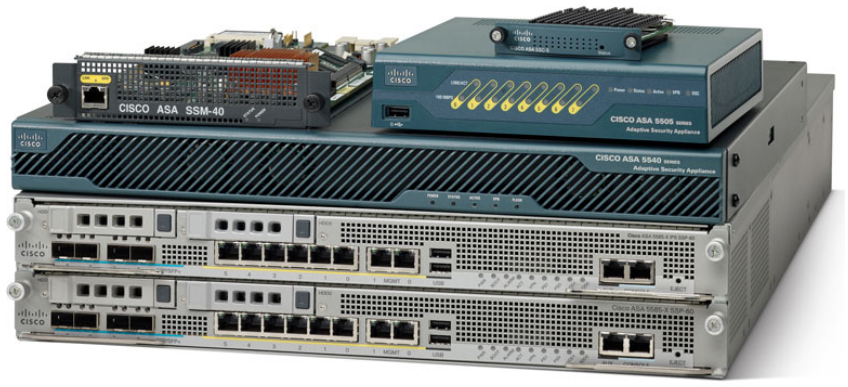

Figura 12 – Soluções de Firewall Cisco para pequenas e médias empresas.
Fonte: Cisco Systems.