A Rede de Autodefesa da Cisco

Fevereiro de 2005

Enio Alves, Gerente de Soluções
enio.alves@cisco.com
Cisco Systems

A Rede como Recurso Estratégico
"O Melhor Ataque É Uma Boa Defesa"

Cisco.com

Recursos de Redes de Informação Inteligentes

Cisco.com

RESILIENTE

- Alta disponibilidade
- Segurança em múltiplas camadas
- Serviços virtuais
- Escalonável

INTEGRADA

- Segurança, IPC, sem fio
- Direcionada para aplicativos
- Gerenciamento
- Abordagem modular

ADAPTÁVEL

- Auto-provisionamento
- Otimização automática
- Autodefesa

Problemas Atuais de Segurança de Rede

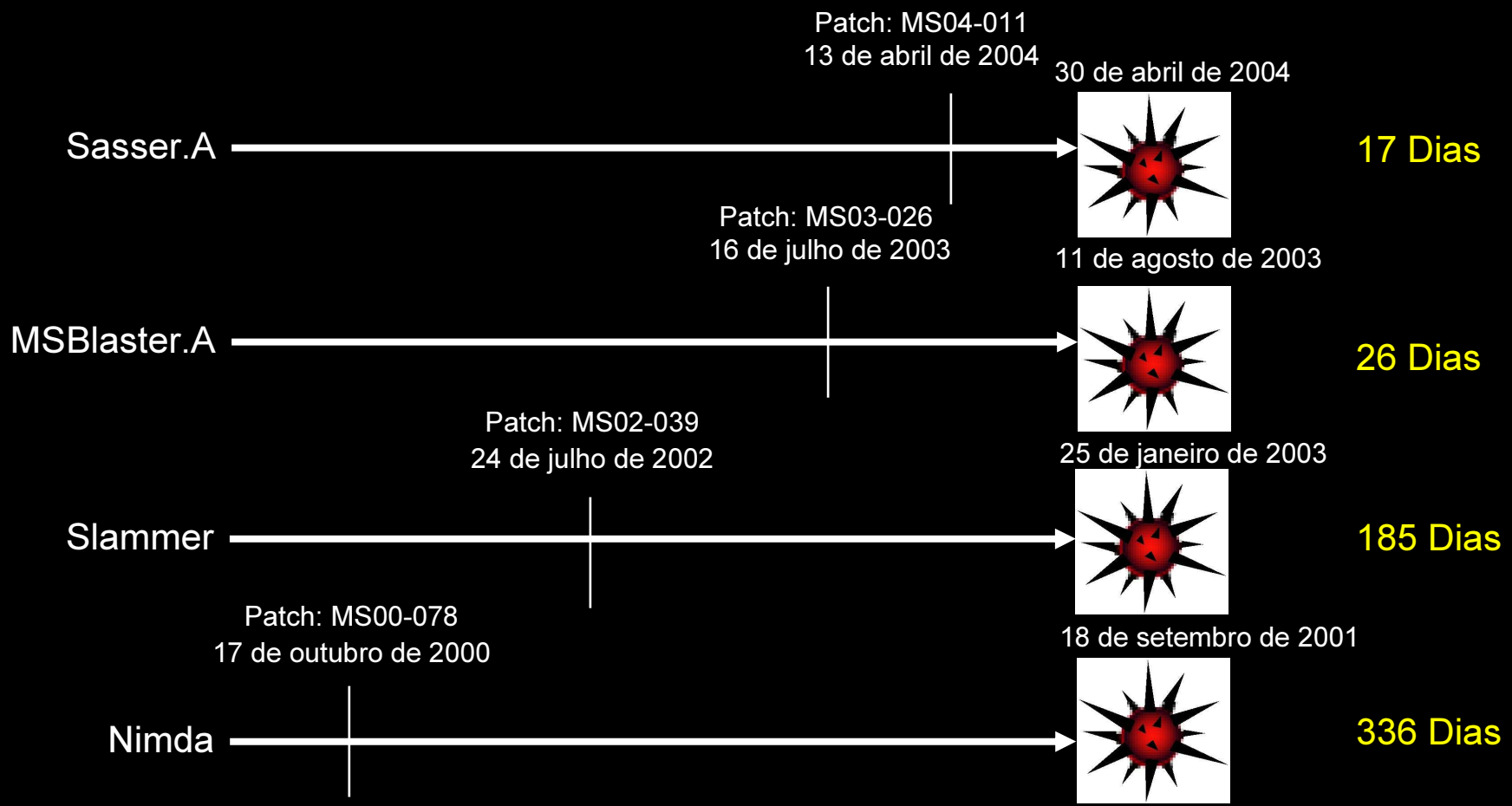
- O cenário jurídico/legislativo está mudando
- Vírus e worms continuam a interromper o trabalho das empresas
- Ataques de “Dia Zero” tornam soluções reativas pouco eficazes
- Ataques DDOS estão aumentando cada vez mais
- As tecnologias pontuais preservam o host, e não a disponibilidade da rede e a resiliência da empresa
- Servidores e desktops não compatíveis são comuns e difíceis de identificar e conter
- Localizar e isolar sistemas infectados exige muito tempo e recursos

Evolução de Desafios de Segurança

Cisco.com

Janela de Tempo da Disponibilização do Patch até o Ataque está Diminuindo

Cisco.com



Os clientes precisam de uma abordagem de sistemas inovadora para impedir e conter as infecções

Tudo é alvo de ataque
Tudo deve ser um ponto de defesa

- Roteadores são alvos
- Switches são alvos
- Hosts são alvos
- Redes são alvos
- Aplicativos são alvos
- Informações são alvos
- As ferramentas de gerenciamento são alvos

- **Tudo é alvo**
  - Alguns pontos podem ser transformados em armas
  - Novos tipos de ataques têm múltiplos vetores que não podem ser bloqueados por um único dispositivo
- **A segurança da rede é um sistema**
  - Camadas de segurança são necessárias
  - Segurança Integrada "EM TODOS OS LUGARES"

Segurança precisa estar Integrada

Portas com trancas

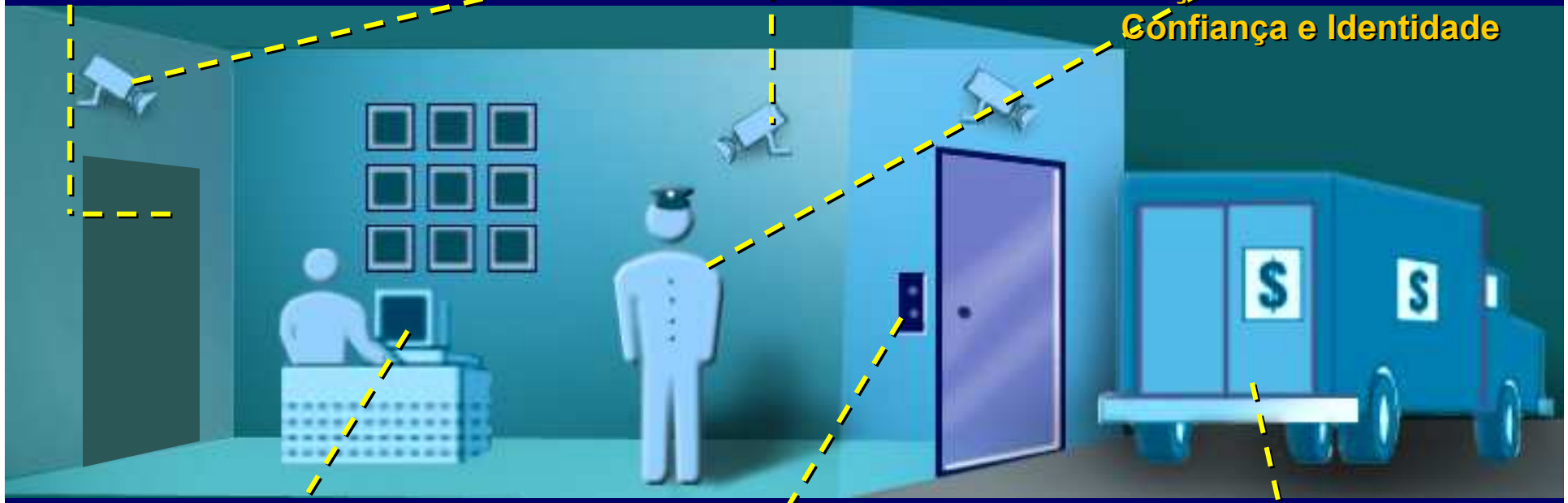
Defesa contra Ameaça

Vigilância e Alarmes

Defesa contra Ameaça

Guarda de segurança de patrulha

Proteção contra Ameaças/Gerenciamento de Confiança e Identidade



Circ. Interno de TV da Sala de Segurança

Gerenciamento de Políticas e Segurança Centralizado

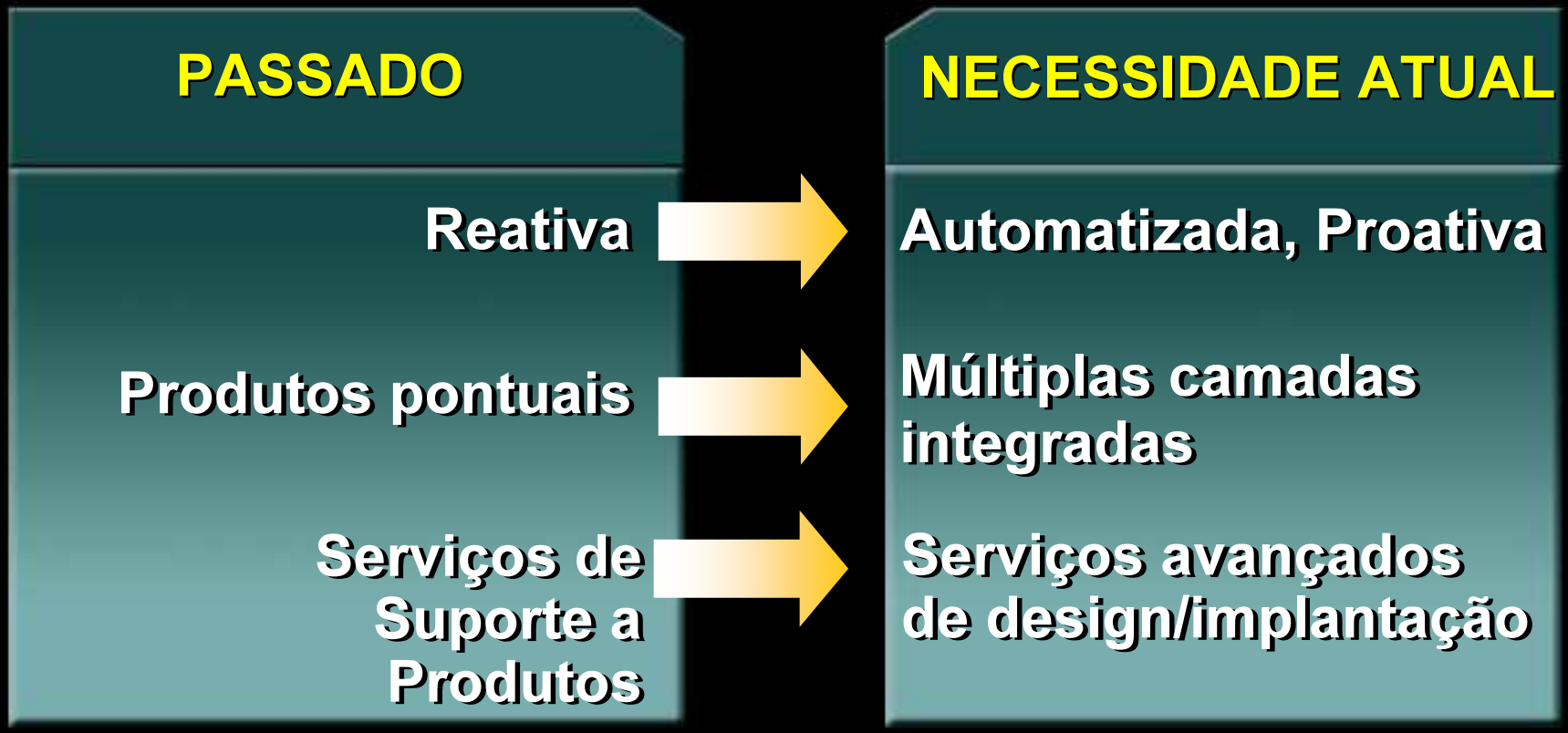
Leitores de cartão

Gerenciamento de Confiança e Identidade

Cofre e carro-forte protegidos

VPN/Conectividade segura

O Que Funcionou no Passado Não Soluciona as Novas Ameaças



Uma Abordagem de Cooperação entre Sistemas

A Visão de Segurança da Cisco

Criar Redes de Autodefesa com Recursos de Resposta Automática

- Migração da segurança para a infra-estrutura de rede
- Proteger núcleo, extremidades e ponto final da rede
- Métodos de proteção complementares com base em anomalias e assinaturas




Estratégia de Rede de Autodefesa

Cisco.com

Componentes de Segurança Integrados

Cisco.com

Privacidade

SISTEMA DE CONECTIVIDADE SEGURA

Transporte Seguro de Aplicativos através de Diversos Ambientes de Rede

Proteção

SISTEMA DE DEFESA CONTRA AMEAÇAS

Colaboração de Serviços de Segurança e Inteligência de Rede para Minimizar o Impacto de Ameaças Conhecidas e Desconhecidas

Controle

SISTEMA DE GERENCIAMENTO DE CONFIANÇA E IDENTIDADE

Gerenciamento de Identidade Contextual para Aplicação de Políticas, Direitos e Confiança da Rede

Gerenciamento e Análise

Estratégia da Cisco apresenta Camadas de Proteção para Hosts

- **Proteção de Endpoint – Cisco Security Agent**

  Minimiza a necessidades de patches e a pressão para atualização de assinatura com tecnologia de proteção baseada em comportamento

- **Controle de Admissão na Rede**

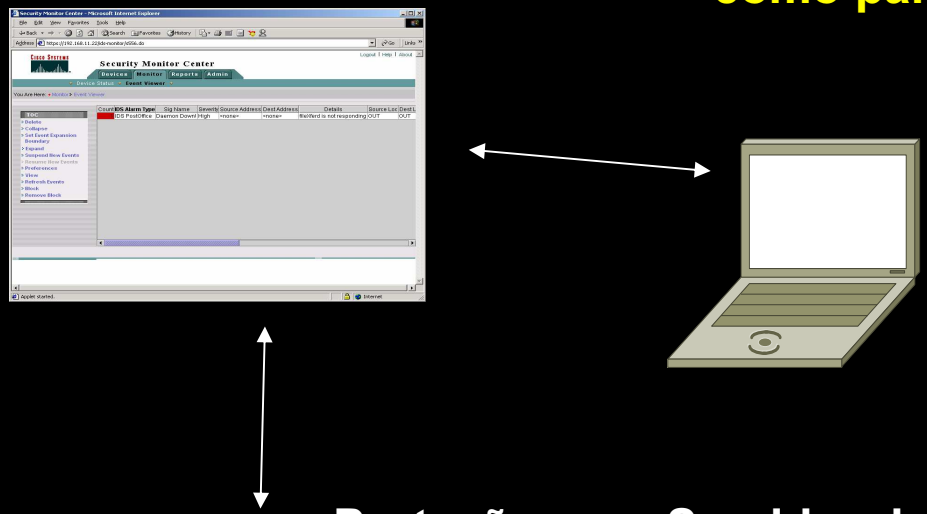
  Preserva a resiliência da empresa fazendo auditoria e forçando o cumprimento das políticas de segurança de ponto final da empresa para acessar a rede

- **Conteção da Infecção na Rede**

  Limita a gravidade das infecções reduzindo o tempo gasto identificando e isolando sistemas infectados e liberando o tráfego

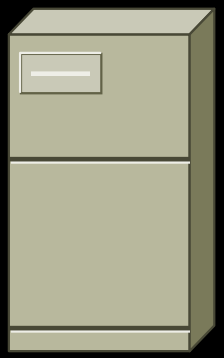
Cisco Security Agent: Proteção de Agente Único

O CSA oferece uma solução comum e consolidada tanto para os desktops como para os servidores



Proteção para Desktop do CSA:

- Firewall distribuído
- Proteção contra Vírus de Dia Zero
- Verificação de Integridade do Arquivo
- Segurança do Instant Messenger
- Segurança para outros aplicativos

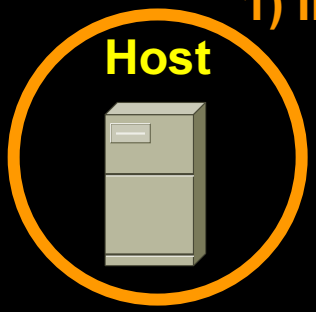


Proteção para Servidor do CSA:

- Proteção contra invasão no host
- Proteção contra estouro de buffer
- Proteção contra worm de rede
- Fortalecimento do sistema operacional
- Proteção de Servidor da Web
- Segurança para outros aplicativos

Exemplo de Sistema de Proteção contra Ameaças

Proteção do CSA contra Sasser



1) Investigar

2) Penetrar

3) Persistir

4) Paralisar

5) Propagar

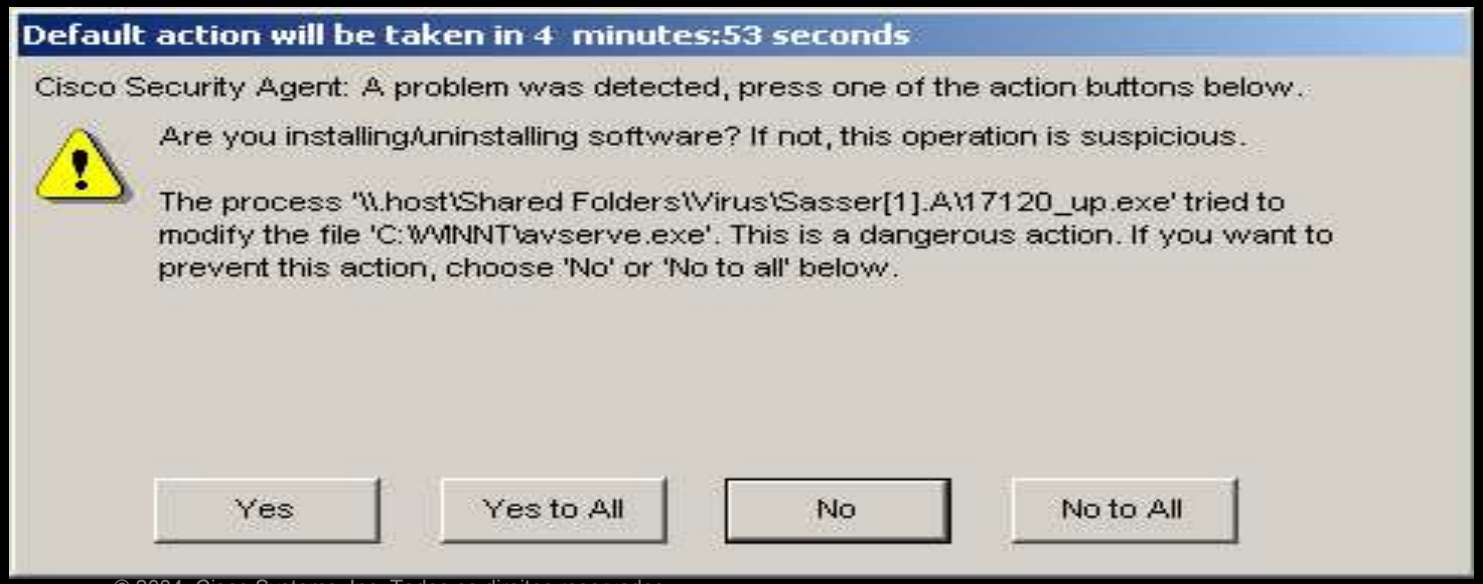
Sasser

Verifica aleatoriamente endereços IP na porta 445/tcp. Pode verificar até 1.024 endereços simultaneamente.

Cria shell remoto na porta 9996/tcp. Ele inicia um servidor de FTP para ouvir na porta 5554/tcp.

Sistema atacado conecta-se novamente ao sistema de ataque na porta 5554/tcp para recuperar cópia do worm.

Provoca falhas nos dispositivos infectados. Faz os sistemas reiniciarem continuamente.



Cisco Security Agent
Registro de Monitoração do Sasser

Cisco.com

Controle de Admissão na Rede Cisco: Primeira Solução de Segurança baseada em Confiança e Identidade

Cisco.com

IBM TREND MICRO Network ASSOCIATES symantec.

Contenção de Infecção de Rede Cisco: Segurança Proativa

Cisco.com

Cliente ativamente conectado

Cliente indica atividade inadequada

Verificação de políticas do cliente

a) Acesso desativado
b) Reparo de quarentena

5 Características de uma Rede de Autodefesa

Cisco.com

- Controle e Proteção de Endpoint
- Proteção da Infra-estrutura da rede
- Conectividade Segura e Flexível
- Inspeção e Controle de Tráfego
- Proteção Dinâmica e Cooperativa

Tecnologias da Rede de Autodefesa da Cisco

Proteção e Controle de Endpoint

Cisco.com

Recurso	*Benefícios*
Controle de Admissão na Rede	• Garante que os dispositivos estejam em conformidade com as políticas de segurança da empresa, incluindo antivírus, patches de SO
Serviços de rede baseados em identidade	• Controla Acesso à Rede e aos Serviços com base na identidade e nas credenciais do usuário
Cisco Security Agent	• Protege o host de ataques Dia Zero (Blaster, MyDoom, Slammer), bem como ataques conhecidos. Força a adoção de comportamentos adequados
SSL VPN (Twingo)	• Elimina rastros da Sessão da VPN SSL no Dispositivo
Servidor de Controle de Acesso	Autenticação, Autorização e Contabilidade para pontos finais.
Você está aí?	Console de VPN força aplicação de política em cliente VPN remoto
Extensões Compatíveis da Cisco (sem fio)	Garante compatibilidade entre clientes sem fio de outros fornecedores e dispositivos Cisco Aironet WLAN

Tecnologias da Rede de Autodefesa da Cisco

Proteção de Infra-estrutura de Rede

Cisco.com

Recurso	*Benefícios*
Proteção de Dispositivos: Política de Plano de Controle	• Reduz o sucesso de um ataque DoS supervisionando a taxa de tráfego de entrada no plano de controle
Proteção de Dispositivos: Autoproteção	• Bloqueia rapidamente os dispositivos conforme práticas recomendadas reconhecidas pela indústria (diretrizes da NSA)
Proteção de Dispositivos: Limite de Memória/CPU	• Roteador permanece operacional sob altas cargas provocadas por ataques reservando a CPU/memória
Proteção de protocolo de roteamento	• Valida pares de roteamento e origem/destino de atualizações de roteamento
Segurança de porta, farejamento de DHCP, Inspeção de ARP Dinâmica, Proteção de Origem IP	• Proteção de infra-estrutura de comutação da LAN e de identidade do usuário, integridade de endereçamento IP
SWAN: Rede sem Fio Estruturada da Cisco	• IDS de WLAN com detecção de pontos de acesso falsos, clientes desassociados e interferência de RF

Tecnologias da Rede de Autodefesa da Cisco

Conectividade Segura e Flexível

Recurso	*Benefícios*
VPN Dinâmica de Múltiplos Pontos	• Topologia de VPN flexível com configuração mínima
VLAN	• Separa domínio e tráfego de terceiros no dispositivo e na rede
GRE/IPSec Roteado	• Roteamento, suporte a aplicativos e instrumentação completos
Easy VPN	• Promove política para implantação fácil. Alta escalabilidade a baixo custo
Suíte de Segurança sem Fio da Cisco	• Proteção de WLAN com Acesso Protegido Wi-Fi (WPA), incluindo 802.1X e TKIP/AES

Tecnologias da Rede Autodefesa da Cisco

Inspeção e Controle de Tráfego

Recurso	*Benefícios*
Implantação de Firewall Flexível	• Reduz os ataques identificando fluxos de pacote suspeitos
Validação de Protocolo	• Ataques podem ser identificados e classificados por fluxos para proteger rede

Tecnologias da Rede de Autodefesa da Cisco

Proteção Dinâmica e Cooperativa

Recurso	*Benefícios*
Detecção de Anomalia na Rede (Riverhead)	• Bloqueia dinamicamente ataques Distribuídos de Negação de Serviços na rede, servidores de destino permanecem operacional
NetFlow e NBAR	• Identifica comportamentos de tráfego anomalo como DDoS e utiliza ACLs e QoS para reduzir esses ataques
Proteção contra Invasão Dinâmica	• Permite a modificação de listas de controle de acesso para deter tráfego indesejado como worms
Resposta à Ameaça	• Analisa alvo de ataque – reduz consideravelmente os alarmes falsos

Evolução da Estratégia de Segurança da Cisco

Cisco.com

Inovação de Segurança de Autodefesa

"QUALQUER UM PODE FAZER UMA PLACA DE PARE OU ATÉ UM SINAL DE TRÂNSITO – MAS É PRECISO UMA FORMA DE PENSAR INTEIRAMENTE DIFERENTE PARA CONCEBER O SISTEMA DE CONTROLE DE TRÁFEGO DE UMA CIDADE INTEIRA".

BRUCE SCHNEIER – BEYOND FEAR

É isso que a Cisco está construindo… poweredbycisco

Para mais informações Cisco

Cisco.com

- **Rede de Autodefesa da Cisco**
  http://www.cisco.com/go/selfdefend
- **Soluções de Conectividade Protegida da Cisco**
  http://www.cisco.com/com/go/security
- **Sistema de Defesa contra Ameaças da Cisco**
  http://www.cisco.com/go/tds
- **Sistemas de Confiança e Identidade da Cisco**
  http://www.cisco.com/go/nac

Para mais informações Brasil

- **Grupo de Trabalho em Segurança**
  https://www.unesp.br/gts/
- **Portal de Segurança Cisco Brasil**
  http://www.cisco.com/br/seguranca/
- **Rede Nacional de Ensino e Pesquisa**
  http://www.rnp.br